Research Program on
Digital Constitutionalism
Project Aristotle

Malaysia

Country Report

November 2021

Authors

Alicia Tan Shu Qi, SOAS Law Society
Emily England, SOAS Law Society
Frances Helena Howe, SOAS Law Society
Umran Chowdhury, SOAS Law Society

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism
Project Aristotle

Malaysia
Country Report

Authors
Alicia Tan Shu Qi, SOAS Law Society
Emily England, SOAS Law Society
Frances Helena Howe, SOAS Law Society
Umran Chowdhury, SOAS Law Society

November 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5716206

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.

A. Digital Constitutionalism and Internet Governance

Introducing Digital Constitutionalism

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

Since the birth of the Internet, John Barlow argued that it is "naturally independent of the [state's] tyrannies" and that no nation has the "moral right" or ways to enforce national laws on the Internet.[1] This lack of sovereign control caused rampant abuse of the lawless internet at the users' expense. Like how the government's use of power is curbed by laws and constitutional principles, the use of Internet shall be grounded by three traditional constitutional concepts: (a) the protection of online users; (b) intermediaries and the rule of law; and (c) the democratic legitimacy of intermediaries as rule-makers. These factors are very important to address the unique characteristics of the digital realm and the pressing issues in Malaysian society.

First, rules of online space evolve in a more democratic manner beyond the territorial boundaries of nations. Anyone who disagrees with the rules of one group can create another group in the digital realm. Such rules can be beneficial to the group's members but detrimental to others. Recently, due to the abuse of a mobile application with end-to-end encryption in Malaysia ('Telegram'), men circulated child pornography, indecent photos of women taken secretly and photoshopped pictures of women posing as sexual workers.[2] Even though there are Malaysian laws dealing with rape threats and such indecency, these rules are not enforced effectively in online spaces (as compared to the offline world) and investigations are often heavily reliant on victims to report crimes. Therefore, Digital Constitutionalism must protect online users from such adversities by adapting the respect for fundamental rights in the Malaysian constitution (enshrined in *Articles 5-13*) into the digital world.[3] A Digital Constitution should aim to maintain public order by protecting user privacy and prohibiting online sexual exploitation.

Second, the internet is formed by intermediaries such as search engines and social media providers, which exercise control over users through their infrastructure. The 'laws' binding on online users originate from the intermediary's terms of service. This allows intermediaries to block certain content or users from using their digital services. How should intermediaries be held accountable for their actions and how does the rule of law apply? Unlike the traditional Malaysian constitution based on the separation of powers, there are no other organs to form a balance of powers in the digital realm created and managed by the intermediary alone. It is argued that intermediaries should be held accountable through due process, which is "enforcing a legitimate law in a careful and accountable way... [rather than] making an arbitrary or capricious decision that can have serious consequences".[4] Therefore, intermediaries should enforce their terms of service on users and explain the reasoning of that decision to demonstrate overall openness and transparency.

Why is due process important? Intermediaries are increasingly pressured by states to regulate harmful online activity. For example, the Malaysian prime minister and lawmakers voiced the need to enact laws against online hate speech.[5] Reacting to state pressures, intermediaries choose to enforce their own terms of service in the absence of national laws and make decisions about the type of content and behaviour allowed on their platform behind closed doors. In Suzor's words, "there's no easy way to ensure... the rules are consistently enforced... in a way that is fair and free from bias".[6] Therefore, due process is crucial to legitimise the role intermediaries play in regulating the online sphere.

Third, as users consent to the intermediary's terms of service, these contracts become "constitutional documents in that they are integral to the way... shared social spaces are constituted and governed".[7] Online users have no rights to oppose the terms of the contract, except by leaving the platform altogether. In 2009, Mark Zuckerberg noted the importance of terms of service as "governing documents" and sought to make his social network more democratic by allowing users to vote on changes on the terms of service. However, this

---

[1] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 2 August 1996) <www.eff.org/cyberspace-independence> accessed 6 July 2021.

[2] Tashny Sukumaran, 'Malaysian survivors of Telegram porn scandal lead calls for change' (*Asia One*, 1 November 2020) < https://www.asiaone.com/malaysia/malaysian-survivors-telegram-porn-scandal-lead-calls-change> accessed 6 July 2021

[3] Constitution of Malaysia, arts 5-13.

[4] Nicolas Suzor, 'The Hidden Rules of the Internet' in *Lawless* (CUP 2019).

[5] Jerry Choong, 'Muhyiddin urges ASEAN to legislate against online hate speech, threats based on race, gender, sexual orientation' (*Malay Mail*, 21 Jan 2021) <https://www.malaymail.com/news/malaysia/2021/01/21/muhyiddin-urges-asean-to-legislate-against-online-hate-speech-threats-based/1942613> accessed 6 July 2021.

[6] Suzor (n 4).

[7] ibid, 'Who Makes the Rules?'.

project failed due to the sheer number of people required to vote to make a small change. Thus, to ground Digital Constitutionalism in traditional constitutional concepts, it is important to consider: can the digital realm be governed in a more democratic manner? How can Digital Constitutionalism help improve the democratic legitimacy of intermediaries, or alternatively, help improve the transparency and accountability of their decision-making processes (i.e. content moderation)? Would involving a variety of stakeholders be sufficient? There are no easy answers to such questions and these are the problems people face in the regulation of online spaces.

To conclude, the internet suffers from rampant misuse and it is crucial that Digital Constitutionalism ensures protection of online users and prevents tyranny due to the overwhelming control intermediaries have over such spaces. It is clear that many traditional constitutional concepts cannot be readily translated into digital governance without modifications. Separation of powers and democratic legitimacy (as apparent in the Malaysian organs of governance) cannot apply to intermediaries due to their unique differences. However, intermediaries can be held accountable through due process, but the question remains: is that sufficient?

2. How can we define Digital Constitutionalism?

Digital Constitutionalism is an ubiquitous phrase used in this country report, and definitely one that demands clear definition. Breaking down the phrase, 'digital' refers to information technology and 'constitutionalism' refers to the system of government that Malaysia currently has (legislature, executive and judiciary abiding by the constitution). However, when these words are interpreted separately, they do not convey the true definition of the phrase.

Digital Constitutionalism refers to a new phenomenon where traditional constitutionalism declines in the digital environment.[8] This is mainly due to the "massive reliance on algorithmic technologies to moderate content and process data", in other words, the reliance on technology producing new difficulties in governance.[9] This is apparent as discussed above, especially when the concepts of separation of powers and democratic legitimacy have little role to play in the digital sphere as compared to its role in the Malaysian constitution. The source of power intermediaries exercise over online users comes from its infrastructure. In comparison, the Malaysian government's source of power comes from the democratic electorate system and its territorial control over the lands. Therefore, in online spaces, Malaysia experiences a shift from the state's territorial sovereignty to the 'functional sovereignty' exercised by intermediaries. The regulation of online users falls on private business choices made on a global scale: "the constitutionalisation of a multiplicity of autonomous subsystems of world society".[10]

Digital Constitutionalism is also a series of disruptive changes in the way modern society is governed, impacting "the equilibrium of the constitutional ecosystem".[11] First, digital technology has enhanced the ability of individuals to exercise their fundamental rights through online communication, for example: freedom of expression, religious freedom, and freedom of assembly (contained in *Articles 10-11 of the Malaysian constitution*). Second, digital technology also threatens fundamental rights by providing a platform for hate speech, cyberbullying, child pornography and more. This abuse of digital technology necessitates content-blocking, monitoring users and collecting information related to such abusive users, which infringe rights to privacy and private life. From a Malaysian perspective, the need for a balance in the exercise of fundamental rights becomes the crux of the legal debate, especially when the exercise of freedom of speech threatens the administration of justice (discussed later in part D). Third, unlike the existing constitutional safeguards against tyranny in Malaysian constitutional law, intermediaries exercise powers on online users (only restricted by the terms of service set by themselves), lacking in accountability, transparency and balancing of powers.

Digital Constitutionalism can also refer to a set of concepts and beliefs which aim to improve the governance of the digital sphere in the face of the issues identified above. For example, legislations protecting the rights of internet users are not part of Digital Constitutionalism, but merely its output. Digital Constitutionalism is a concept that guides people to consider the protection of fundamental rights and the due process of online decision-makers, most importantly: whether online rules reflect Malaysian societal values.

[8] Edoardo Celeste, 'What is digital constitutionalism?' (*Digital Society Blog*, 31 July 2018) < https://www.hiig.de/en/what-is-digital-constitutionalism/> accessed 7 July 2021.

[9] Giovanni De Gregorio, 'The rise of digital constitutionalism in the European Union' (2021) ICON 19, 56.

[10] ibid, 57.

[11] Edoardo Celeste, 'Digital constitutionalism: a new systematic theorisation' (2019) 33 Int. Rev. Law, Comput. Technol. 76, 78.

Finally, Digital Constitutionalism also aims to adapt existing constitutional values to solve the problems in the digital realm, which is demonstrated in Part A, Question 1. Due to the lack of legal jurisdiction on the internet, Digital Constitutionalism seeks to encourage a series of actions taken in favour of preserving the key constitutional values in our society, for example: due process, balance of powers, and protection of fundamental rights. As opposed to state actors, private actors adopt legal instruments and implement actions that reflect these constitutional values.

Defining Digital Constitutionalism increases our understanding of why digital governance is important and how it can be done. As a final note, it is important that Digital Constitutionalism does not produce a set of concrete rules: the final product should be a flexible framework, guided by certain core tenets to help adapt to the fast-changing world of digital technology.

Digital Constitution

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

Before considering what the future holds, one must look at the present. The current 'Digital Constitution' we have is made up of contractual terms of service produced by private businesses. Such 'constitutional documents' are scattered across the network depending on which technological tool users opt for. Private users are not the sole group that is subject to these constitutional documents. Even state actors that make use of information technology to offer better quality public services are subject to such terms.[12] The importance of technology in both daily lives and government planning made Digital Constitution a necessity, especially when algorithmic decision-making suffers from opacity and a democratic government should be held accountable for their decisions in using technology.[13] It is argued that a Digital Constitution should follow four core tenets: (a) respect for fundamental rights and equality, (b) intermediaries and legal responsibility; (c) private companies, due process and Corporate Social Responsibility; and (d) cooperation with state actors.

A Malaysian Digital Constitution should respect fundamental liberties, which are enshrined in *Part II of the Malaysian constitution*. Malaysia has a different human rights narrative compared to the international legal discipline. This Malaysian human rights narrative was deeply entrenched in the society since Dr Mahathir's 22-year leadership as prime minister. Malaysia rejects the absolute nature of universal human rights because of their Western values, and instead adopts Asian community-based values which originated from the Confucian tradition. To the Malaysian government, the imposition of universal human rights standards on a society is a modern form of colonialism "with the potential to destroy the inherent diversity of cultures and move global society towards cultural homogenization".[14] Hence, the respect for online fundamental rights should reflect Asian societal values, avoid imposing a single human rights regime, and focus more on the rights of the community to achieve political, social and economic stability as a developing nation.[15] This Asian human rights ideology is enshrined in *Clause 8 of the Bangkok Declaration on Human Rights*, stating that although human rights are universal, their scope and application must consider "the significance of national and regional particularities and various historical, cultural and religious backgrounds". Therefore, a Malaysian Digital Constitution must reflect this human rights ideology.

Since the beginning of the Internet's birth, it was visualised to be a free space for information sharing. Businesses created neutral data-sharing platforms that do not discriminate or exclude: business practices, enabling the Internet to carry any traffic uploaded to the platform, and content. Such neutrality no longer works for the modern digital society suffering from rampant abuse. It is argued that intermediaries, especially internet service providers (ISPs) and web hosting services (WHSs), should not only be responsible for monitoring illegal content (child pornography, terrorism and criminal activities covered by law), but also other morally repugnant forms of internet speech (hate speech and bigotry).[16] As mentioned before, Malaysian leaders have expressed their political will to legislate against online hate speech. The Digital Constitution should reflect this political will and enact laws that criminalise hate speech.

[12] For example, the Malaysian government launched a project called 'Putrajaya Smart City', which aims to use information technology for better urban planning and environmental sustainability.

[13] Robert Brauneis and Ellen Goodman, 'Algorithmic Transparency for the Smart City' (2018) 20 Yale J L & Tech 103.

[14] Rohaida Nordin, 'Malaysian Perspective on Human Rights' (2010) Jurnal Undang-undang 18, 19-20.

[15] Bilahari Kausikan, 'An East Asian approach to human rights' (1995-96) 2 Buffalo Journal of International Law 147.

[16] Raphael Cohen-Almagor, 'Responsibility of Internet Service Providers and Web-Hosting Services, Part I: Rationale and Principles', in *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway* (CUP 2015).

The Malaysian Digital Constitution should encourage private companies to adopt the key principles in corporate social responsibility (CSR) to improve the due process in decision-making. Essentially, CSR mandates private businesses to have a transparent decision-making process which consults relevant stakeholders and takes into account all positive and negative implications of a decision. Private businesses should set societal rules by considering public policy, and abide by those rules. Companies should have precautionary steps before implementing a decision and liability mechanisms to redress harm.

Last but not least, one of the core tenets of a Digital Constitution should entail state cooperation on criminal matters. This can help to reduce fraud, defamation and other severe crimes such as terrorism. Malaysia has been a target for ISIS recruiters.[17] Facebook has been trying to eliminate posts relating to terrorism, but ISIS still finds ways to recruit new members.[18] A Malaysian Digital Constitution should pull the governance of digital spheres closer to the reach of nations in matters relating to severe organised crimes and public order.

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

At present, international human rights law includes several treaty provisions which support the participation of the public in a free and open digital sphere. *Article 19 of the International Covenant on Civil and Political Rights (ICCPR)* enshrines the right to hold opinions without interference; the right to freedom of expression; and the right to freedom of information, including to seek, receive and impart information through any form of media.[19] *Article 17 of the ICCPR* enshrines the right to privacy, as well as the right to protection of family, home, personal correspondence and personal reputation from arbitrary or unlawful interference.[20] The ICCPR allows derogation from many of its provisions, including *Articles 17 and 19*. Derogations are subjected to terms of proportionality and necessity, including safeguarding the public interest (i.e. the fundamental rights and freedoms of others). The right to information and the right to free expression are crucial for the digital sphere.

Malaysia is not a state party of the *ICCPR*. Malaysia does not have a federal freedom of information law. Only two states, including Selangor and Penang, have enacted legislation concerning freedom of information. *Article 10 of the Federal Constitution of Malaysia* protects freedom of expression and freedom of speech. *Article 10* also allows the Malaysian government a greater scope for derogation than the *ICCPR*, including "such restrictions as it deems necessary or expedient in the interest of the security of the Federation or any part thereof, friendly relations with other countries, public order or morality and restrictions designed to protect the privileges of Parliament or of any Legislative Assembly or to provide against contempt of court, defamation, or incitement to any offence".[21] *Article 10 (4)* also empowers the Malaysian parliament to pass any law to safeguard the provisions of *Part III of the Federal Constitution*.

A Digital Constitution "for the people" embodies effective human rights guarantees. In particular, this involves the right to receive and impart information. The right to information is considered an integral part of the right to freedom of expression. The UN Human Rights Committee in *General Comment 34* states that countries "should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto".[22] *General Comment 16* details the importance of protecting inter-personal correspondence as part of the right to privacy. The prohibition of surveillance and interception of correspondence is encouraged; unless a judicial authority provides a warrant based on reasonable grounds and the public interest. *General Comment 16* also addresses the collection of personal data, stating that "The gathering and holding of personal information on computers, data banks and other devices, whether by public

[17] See Fariza Hanis Abdul Razak, 'The Use of Facebook in ISIS Recruitment – An Exploration' (2017) 10 Journal of Media and Information Warfare 51.

[18] Gordon Corera, 'ISIS 'still evading detection on Facebook', report says' (*BBC*, 13 July 2020) <https://www.bbc.co.uk/news/technology-53389657> accessed 7 July 2021.

[19] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 19.

[20] Ibid art 17.

[21] Federal Constitution of Malaysia art 10 s 2 (a).

[22] UN Human Rights Committee General comment No. 34 (freedoms of opinion and expression) UN Doc CCPR/C/GC/34 para 15.

authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by states to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination".[23] Individuals are also entitled to protection from defamation and remedies for defamatory acts.

The interests of a democratic polity needs to be reflected in the Digital Constitution. This would entail a democratically-elected legislature which is empowered to review and scrutinise laws proposed by the government. Malaysia is a federal parliamentary democracy with periodic free and fair elections at the federal and state levels. Parliamentary committees have an important role to play in analyzing and modifying bills. A permanent parliamentary committee can be established to focus on matters relating to a Digital Constitution.

A free media is essential for a free and open digital sphere. Malaysia currently ranks 119th on the 2021 World Press Freedom Index compiled by Reporters without Borders. Malaysia has seen an 18-point fall from its earlier position in the 2020 World Press Freedom Index.[24] This fall could have been caused by the enactment of the January emergency ordinance 2021 which criminalises persons who publish fake news regarding Covid-19, raising great public concern of its potential repressive effects on free speech.[25] However, at the time of writing, this emergency ordinance, along with five other similar ordinances, have been revoked due to the end of the state-declared emergency on 1 August 2021.[26]

Representativeness of Online Platforms

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

An online platform is a public-facing internet site, a digital application or a social network site that sells advertisements directly to advertisers. These include social media sites, notable ones being Facebook, Instagram, YouTube and Snapchat. According to the Malaysian Communication Multimedia Commission (MCMC), Facebook is the leading social networking service (SNS) in Malaysia with 91.7% users, followed by YouTube (80.6%), Instagram (63.1%), Twitter (37.1%), Google Plus (24.1%), LinkedIn (10.8%), and other lesser known SNSs (0.2%).[27] The number of Facebook users in Malaysia is forecasted to reach over 25 million in 2021.[28]

Although online platforms are largely separate and private entities, their ability to be made more inclusive, representative or equal will depend on the country or state's ability to create an environment that is similar. *Article 8(1)-(2) of the Malaysian constitution* states: "all persons are equal before the law and entitled to the equal protection of the law", and no one shall be discriminated "on the ground only of religion, race, descent, place of birth or gender in any law". Following this stated standard of equality, it should be reflected on online platforms in Malaysia as well that all persons are treated equally. Specifically, demographics should not be discriminated against or excluded on online platforms on the basis of their gender, sexual orientation, race and so forth.

Taking the view that a country must first advocate the equality for this to be reflected online, Malaysia's criminalisation of homosexuality should be addressed in order to improve equality. *Sections 377A and 377B of the Malaysian Penal Code* punish persons who voluntarily have "sexual connection with another person by the introduction of the penis into the anus or mouth of the other person", with a penalty of up to

[23] UN Human Rights Committee General comment No. 16 (right to privacy, family, home and correspondence and protection of honour and reputation) Thirty-second session (1988) para 10.

[24] 'Malaysia : Back To Harassment, Intimidation And Censorship | Reporters Without Borders' (*RSF*, 2021). <https://rsf.org/en/malaysia> accessed 2 August 2021.

[25] Mohd Azizuddin Mohd Sani, 'Could Malaysia's fake news ordinance stifle public debate?' (*East Asia Forum*, 21 April 2021) < https://www.eastasiaforum.org/2021/04/21/could-malaysias-fake-news-ordinance-stifle-public-debate/ > accessed 2 August 2021

[26] Tho Xin Yi, 'Actions to revoke COVID-19 emergency laws were in line with Malaysia's laws and Constitution: PMO' (*CNA*, 29 July 2021) <https://www.channelnewsasia.com/news/asia/malaysia-muhyiddin-emergency-ordinances-in-line-constitution-15328726> accessed 2 August 2021.

[27] MCMC, *Internet Users Survey 2020* (MCMC, 2020), 49.

[28] Joschka Müller, 'Malaysia: number of Facebook users 2017-2025' (*Statista*, 7 April 2021) <https://www.statista.com/statistics/490484/number-of-malaysia-facebook-users/> accessed 1 August 2021.

twenty years imprisonment and whipping. Decriminalising homosexuality under Malaysian law can allow for a more representative and inclusive environment for the citizens both online and offline. Malaysians have been calling for the abolishment of *Sections 377A and 377B* because they are "ancient laws which seem to have outlived its useful life, open to much abuse and with much debate over its relevance".[29]

Tracing the origins of these anti-homosexual laws, the entire *Malaysian Penal Code* was modelled after the *Indian Penal Code*, and both criminal codes were the product of British colonialism (originally drafted by Thomas Babington Macaulay). The 47 countries which were colonised by the British still have laws against voluntary homosexual sex till modern day.[30] However, the constitutionality of Malaysian anti-homosexual laws are put to grave doubt when the Supreme Court of India decriminalised similar provisions in the *Indian Penal Code* and described them as "irrational, indefensible and manifestly arbitrary" in the case of *Navtej Singh Johar*.[31] Justice Chandrachud argued the state had no power to decide "the boundary of what is permissible and what is not" in determining whether a consensual sexual act is against the order of nature. Chief Justice Dipak Misra and Justice Khanwilkar held the wording of *Section 377 in the Indian Penal Code* assumes unreasonableness in the sexual acts and this "becomes a weapon in the hands of the majority to seclude, exploit and harass the LGBT community", creating an avenue for bigotry and homophobia. Finally, Justice Nariman held the provision is a violation of fundamental rights "when the state has no compelling reason to penalise same-sex couples who cause no harm to others".

Despite these archaic laws being rarely enforced in Malaysia, it was used as a political tool to defeat oppositions. Anwar Ibrahim, the former deputy prime minister, was charged with sodomy since 1998 and was convicted by the Federal Court of Malaysia in February 2015. Although he was convicted of a "victimless offence", he was disqualified from being a member of parliament.[32] Due to this political scandal, sodomy laws were brought to the public's attention and increasing number of people are calling for the repeal of these repressive laws. However, not all is lost: the Federal Court of Malaysia took a right step on 25 February 2021 when they unanimously held that the *Section 28 of the Syariah Criminal Offences (Selangor) Enactment* contravened the *Federal Constitution* because such offences fell under parliamentary powers and not under state legislature's law-making powers.[33] This author argues these sodomy laws should be repealed so as to enable a more representative and inclusive community online and offline.

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, simply put, is the use of publicly available information. OSINT is defined as "intelligence produced from publicly available information that is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement".[34] OSINT has many uses, notably to provide information for national security and intelligence. Aside from the classic examples of newspapers and televisions as sources of OSINT, the term "second-generation OSINT" has come to encompass user-generated information that is now being posted on the internet and social media platforms.[35] Refer to the figure below for more details on OSINT generations.

[29] Ng Shu Tsung, 'Abolish section 377A and 377B of the penal code' (*MalaysiaKini*, 3 October 2011) <https://www.malaysiakini.com/letters/177583> accessed 2 August 2021.

[30] Lavinia Spieß, 'A ray of hope for LGBT+ under Malaysia's homophobic legislation' (*Peace for Asia*, 9 March 2021) <https://peaceforasia.org/a-ray-of-hope-for-lgbt-under-malaysias-homophobic-legalisation/> accessed 2 August 2021.

[31] *Navtej Singh Johar & Ors. v. Union of India, & Secretary, Ministry of Law and Justice* AIR 2018 SC 4321 (Supreme Court of India).

[32] Christopher Leong, 'Press Release | Dato' Seri Anwar Ibrahim: Prosecuted or Persecuted?' (*Malaysian Bar*, 11 February 2015) <https://www.malaysianbar.org.my/article/news/press-statements/press-statements/press-release-dato-seri-anwar-ibrahim-prosecuted-or-persecuted> accessed 2 August 2021.

[33] Zheng Hong See, "The Federal Court of Malaysia held state Syariah law criminalising 'unnatural sex' void and unconstitutional" (*OxHRH Blog*, April 2021) <https://ohrh.law.ox.ac.uk/the-federal-court-of-malaysia-held-state-syariah-law-criminalising-unnatural-sex-void-and-unconstitutional/> accessed 2 August 2021.

[34] Headquarters, Department of the Army, *Open Source Intelligence* (Army Techniques Publication Washington, 2012).

[35] Heather Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (RAND Corporation, 2018).

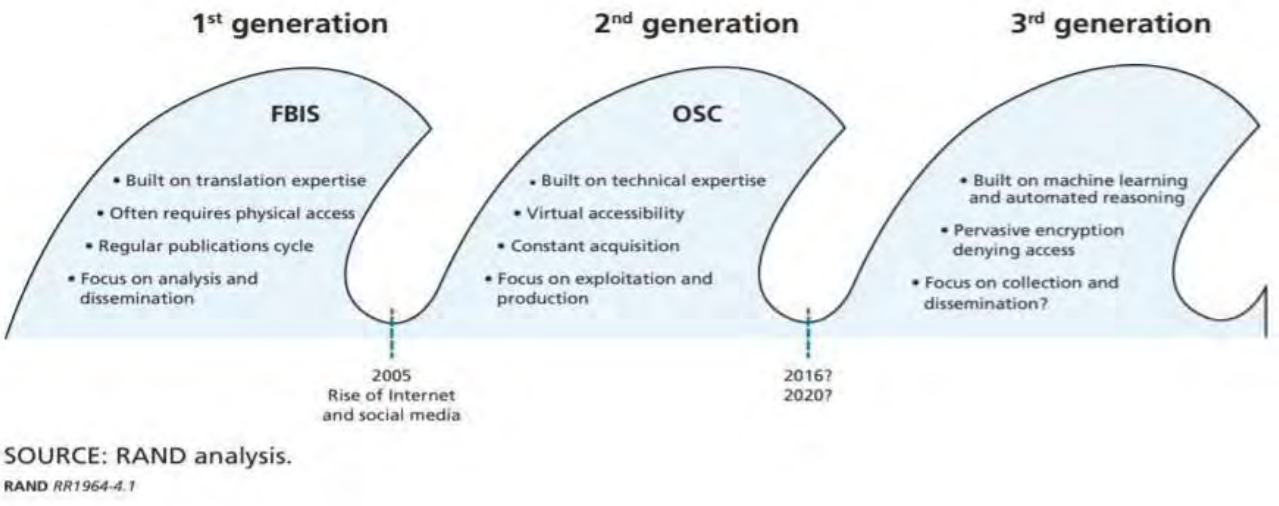

Figure: Characteristics of OSINT Generations[36]

Currently, the Open Source Competency Centre (OSCC) in Malaysia, launched in 2014, is Malaysia's first government centre using OSINT. The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) along with the public sector published a tentative plan as to how OSINT and open source software will be implemented and used by the government. The first phase took place from 2004 till 2006, which involves laying the foundation and preparing for the early adoption of OSINT. The second phase took place from 2007 till 2010, which includes an accelerated adoption of the technology. Finally, Malaysia has completed its third phase (2011-2020) which is known as 'self-reliance', and MAMPU intends to develop its own technological capabilities in system development, "focusing on the use of generic application development at the agencies in the Public Sector".[37]

This technology has been notably used by the Malaysian Internet Crime Against Children Investigation Unit (Micac) to investigate and prevent the illegal distribution and viewing of child pornography in Malaysia.[38] During the tragedy of the Malaysian Airlines Flight MH17 in 2014, a Dutch investigative-journalism company called Bellingcat, utilised OSINT to investigate and prove Russia's involvement in the crash. The aircraft was shot down whilst flying over East Ukraine. Primarily using open source intelligence, information available from social media primarily, they were able to determine that satellite footage had been doctored and linked a Buk missile launcher to the crash.[39]

As demonstrated in the past, OSINT has many investigative uses in terms of matters of national security. A report published by the RAND Corporation, particularly the cyber defence center, stated that social media is now an integral source of information that can be used for OSINT however: "OSINT is often underutilised because of the difficulties in understanding dynamic OSINT sources and methods, particularly social media platforms. It also presents new challenges, including how to protect U.S. persons, manage massive quantities of data, and leverage private-sector tools and entities to the fullest possible extent".[40]

Aside from a national security perspective, OSINT can also be used to determine the zeitgeist and popular opinion of a population. Using collocation analysis of open source data, a study conducted by Paul Baker in 2008 determined what keywords the UK public associated with the words 'refugee'. This was then

[36] ibid, 40.

[37] 'Open Source Development and Capabilities Programme (OSDeC) (*Malaysia.gov.my*). <https://www.malaysia.gov.my/portal/content/30098> accessed 2 August 2021.

[38] Emmanuel Santa Maria Chin, 'After four years, police's anti-child sexual crimes unit officially launched' (*Malay Mail*, 9 February 2018) <https://www.malaymail.com/news/malaysia/2018/02/09/after-four-years-polices-anti-child-sexual-crimes-unit-officially-launched/1574073> accessed 2 August 2021.

[39] Timmi Allen et al., 'Origin of the Separatists' Bulk: A Bellingcat Investigation' (*Bellingcat*, 8 November 2014) <https://www.bellingcat.com/news/uk-and-europe/2014/11/08/origin-of-the-separatists-buk-a-bellingcat-investigation/> accessed 2 August 2021.

[40] Williams and Blum (n 35), 10.

used to analyse and extrapolate general opinion, views and potential prejudice surrounding this word.[41] Thus, whilst OSINT is currently being actively used for security purposes particularly in the US, it still has great potential for sociological and political research. Currently, Malaysia has been utilising OSINT for certain specific purposes within the government, however it will be more beneficial to expand the uses of OSINT within the government and to utilise information on social media in particular, to their advantage.

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?

Integrative legal jurisprudence bridges the gap between the normative ideal and pragmatic side of the law by employing "analytical, empirical, and normative methods".[42] In simpler words, instead of focusing on why the law should be like this, an integrative legal scholar asks: "how do we actually do this?"[43] From the above discussion (Part A, Question 3), this author expresses her inclination towards grounding ideals (respect for fundamental rights, due process and corporate social responsibility) in contrast to setting specific legal standards. Not only does the integrative model raise complex issues, it is way too early to set concrete standards for legal areas heavily impacted by the evolution of technology. Technology collects data, processes and extracts their value, and finally predicts answers to questions. This replaces the role of humans in decision-making processes and is labelled as 'big data': the "new generation of technologies and architectures, designed to economically separate value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and analysis". As a result, traditional legal tests may rely on elements that become impossible to prove as technology continues to develop.

A simple example would be the legal test for knowledge in contemptuous publications: for traditional newspaper publications, all articles undergo the inspection and moderation of editors, making it easier for the court to find actual knowledge of the publisher in publishing the contemptuous writings. However, the same cannot be said when it comes to posting online comments – the website host does not inspect each and every comment posted due to the sheer traffic, but instead relies on peer reporting and algorithmic moderation (filtering restricted words). Therefore, the traditional test for knowledge in newspaper publications cannot be readily adapted to its digital counterpart. This problem is only solved when the court decides constructive knowledge, inferred through the extent of control intermediaries have over the online publishing of comments, shall satisfy the test for knowledge after digging through heaps of foreign case law.[44] It is doubtful that the drafters of a Digital Constitution can readily foresee the problems with adapting certain traditional legal standards to regulate their digital counterparts. Hence, a Digital Constitution should be a set of grounding ideals as opposed to an integrative model — the responsibility of adapting traditional legal standards to regulate the online sphere shall fall on the judiciary and legislature instead.

How can a Digital Constitution (consisting of grounding ideals) fulfil the specific needs of a pluralistic society? The digital space is a good illustration of legal pluralism because it is a social arena filled with co-existing and conflicting normative systems, such as: the contractual terms of service set by various online intermediaries (functional normative systems), national laws on online behaviours (official legal system), cultural and religious norms in the use of online space (Islamic laws), and trans-governmental laws (ASEAN).[45] To fulfil the needs of such a culturally, legally and socially pluralistic society, the Digital Constitution should respect the differences unique to Malaysia and its social dynamics between races. Most importantly, the Digital Constitution should provide ways to solve or negotiate claims of authority when these normative systems conflict with one another. For example, if there was a conflict between the online terms of service and a cultural norm (say, respect for Islam), the Digital Constitution should state the maintenance of racial harmony and public order is paramount in any situation and therefore cultural norms have a stronger claim of authority over private documents.

[41] Paul Baker et al , 'A Useful Methodological Synergy? Combining Critical Discourse Analysis and Corpus Linguistics to Examine Discourse of Refugees and Asylum Seekers in the UK Press' (2008) 19 Discourse & Society 273.

[42] For more information, see Matthias Klatt, 'Integrative Jurisprudence: Legal Scholarship and the Triadic Nature of Law' (2020) 33 Ratio Juris 380.

[43] Jane Allen, 'The "Doers'" Perspective: Fully Deploy the Integrative Law Model' (*ABA Groups*, 20 February 2016) <https://www.americanbar.org/groups/business_law/publications/blt/2016/02/01_allen/> accessed 19 July 2021.

[44] *Peguam Negara Malaysia v Mkini Dotcom Sdn Bhd & Another* (Case No. 08(L)-4-06/2020).

[45] For more information on legal pluralism, see Brian Tamanaha, 'Understanding Legal Pluralism: Past to Present, Local to Global' (2008) 30 Syd LR 375.

8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?

Why does competition law matter in digital services? Competition laws protect markets from big-tech domination and promote a "fair data market".[46] Digital technology can produce business models of "multi-sided markets", creating network effects and economies of scale, where costs are reduced by large amounts of output. This encourages collaborative consumption of products and peer-to-peer exchange, and thereby creating a "sharing economy".[47] To illustrate, when Grab was first introduced in Malaysia in 2012, it provided people and business organizations a platform to connect online and share goods/services. This network effect improves collaborative consumption, that is helping people find what they want to buy. In effect, this drives innovation and increases job opportunities as more freelancers earn their wages online. However, this also disrupts traditional commercial sectors (for example: taxi drivers) and causes major problems to competition and consumer welfare as Grab begins to monopolise the market.

The conventional consumer protection laws in Malaysia cannot redress the detriment consumers face in a monopoly because they are "built upon different underlying theories of harm". Although Malaysia was one of the first countries in South East Asia to enact a competition legislation on its own accord (*Malaysian Competition Act 2010*),[48] the Act faced challenges in protecting consumer welfare on digital markets. Generally, competition and antitrust laws have an economic objective: they seek to prevent abusive business practices or monopolisation of a product market to the extent that it harms consumer welfare by reducing choice and eliminating competition. The aim of the *Malaysian Competition Act 2010* is to "promote economic development by promoting and protecting the process of competition, thereby protecting the interests of consumers and to provide for matters connected therewith". Most of the substantive provisions of the Act mirror EU competition law in terms of prohibiting cartels/anti-competitive agreements (*Section 4*) and conduct amounting to an abuse of dominant position (*Section 10*). However, it is important to note that this Act does not apply to commercial activity regulated under *Communications and Multimedia Act 1998* (*Section 3*). Therefore, online intermediaries can be subject to different legislative frameworks depending on the services they provide. For example, if a company provides network facilities or applications services, their commercial activities fall within the ambit of *Communications and Multimedia Act 1998*. In contrast, if an online intermediary provides a food delivery service (say 'GrabFood'), their business activities fall under the scope of the *Malaysian Competition Act 2010*.[49]

How do competition laws of different jurisdictions prevent big-tech domination? A very good case study would be the merger review of Grab, a mobile application which offers food delivery, transport and payment services, in South East Asia. As it rapidly expands, Grab took over the assets of Uber in Cambodia, Indonesia, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam by 26 March 2018 without notifying the relevant national agencies because the takeover did not meet the mandatory notification thresholds. The Indonesian competition authority decided the transaction was a mere "asset acquisition without any transfer of control" since Uber and Grab Indonesia existed as separate entities.[50]

Singapore's Competition and Consumer Commission started an investigation of the merger on 27 March 2018 and found that the takeover greatly reduced competition in the ride-hailing sector. Further, Grab held 80% of the market share and increased prices after removing Uber from the market. In effect, this merger helped Grab impose exclusivity obligations on taxi companies and drivers, preventing new entrants from expanding in this market. The Commission required Grab to remove this exclusivity obligation, to maintain its

[46] For more information on competition law and data, see Sofia Oliveira Pais, 'Big data and big databases between privacy and competition' in Cannataci, Falce and Pollicino (eds), *Legal Challenges of Big Data* (Edward Elgar Publishing, 2020).

[47] Angayar Kanni Ramalah, 'Competition in Digital Economy: Fate of Consumer Welfare in Malaysia' (2019) 22 Malaysian Journal of Consumer and Family Economics 223.

[48] Most South East Asian countries only have competition law in its trade agreements. See Julian Nowag, 'An Introduction into Competition Law: The Substantive Provisions of the Malaysian Competition Act in Light of its European Origins' (2013) 30 Malayan Law Journal 1.

[49] For a brief summary of the Competition Act 2010, see Elaine Law Soh Ying, 'Malaysia: Overview of Competition Law in Malaysia' (*Mondaq*, 18 February 2016) < https://www.mondaq.com/antitrust-eu-competition-/467510/overview-of-competition-law-in-malaysia> accessed 20 July 2021.

[50] United Nations Conference on Trade and Development, *Competition issues in the digital economy* (Trade and Development Board, 2019).

previous pricing algorithm before the merger, to sell vehicles to other competitors, and imposed a fine of S$13 million to deter such mergers in the future.

In 2018, the Malaysian Competition Commission (MyCC) and Land Public Transport Commission closely monitored the company to ensure competition would not be disrupted. However, a year after Singapore's investigation, MyCC proposed a total of RM86 million fine on Grab for abusing its dominant position by preventing drivers from promoting services for its competitors. Grab now plans to appeal the Malaysian High Court's decision to dismiss its application for leave to commence judicial review against MyCC.[51]

The Philippines Competition Commission imposed interim measures to preserve the current market conditions, but later cleared the transaction in August 2018 after imposing pricing standards and service quality requirements. However, Grab and Uber Philippines were fined twice in the next five months for failing to comply with those requirements.

From this case study, it is clear that big-tech domination must be avoided at all costs because this risks producing a digital monopoly that increases prices and eliminates all potential competition in the future. Singapore was one of the first countries to impose extensive restrictions on Grab, which eventually led other countries to take a closer review of the market. It is clear that Grab is under the watchful supervision of each country and hopefully this deters any further anti-competitive practices on its part.

The Regional, Constitutional and Transnational Aspects of a Digital Constitution

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?

A digital ecosystem is defined as "a group of interconnected information technology resources that can function as a unit", creating value for many stakeholders.[52] The free flow of information has transformed societies, posing "unique governance challenges" such as: consumer welfare protection, online disinformation, and cybersecurity threats.[53] Most importantly, many countries (as regional actors) have taken different approaches to the protection of online privacy, and the lack of legal harmonization exposes online users to privacy risks. Regional actors and judicial cooperation play an important role in regulating the digital ecosystem. This can be demonstrated by observing and analysing the Malaysian data privacy law reform project.

The concept of data privacy is fairly new to Malaysia because the right to privacy is not a fundamental right guaranteed by the Malaysian constitution. The Malaysian *Personal Data Protection Act (PDPA) 2010* was enacted to improve consumer confidence in e-commerce due to increasing identity theft frauds in the region. Prior to this Act, data was generally protected by the confidentiality provisions in contracts or as "confidential information" in civil actions.[54] Without a doubt, the enforcement and development of data privacy laws were stumped by the lack of recognition it has within Malaysian society.[55] According to Comparitech, a British technology website, it ranked Malaysia as the fifth-worst country in protecting personal data, scoring 2.64 out of 5.[56] This is because the Malaysian *PDPA 2010* only protected against the misuse of personal data for commercial purposes, but it did not regulate issues of online privacy (e.g. geolocation and cookies) or when personal data is processed outside of Malaysia.[57]

---

[51] For more information, see CPI, 'Grab to Appeal Malaysian High Court over Antitrust Fine' (*Competition Policy International*, 11 March 2020) <https://www.competitionpolicyinternational.com/grab-to-appeal-malaysian-high-court-over-antitrust-fine/> accessed 20 July 2021.

[52] For a brief summary of digital ecosystems, see Kate Brush, 'Digital Ecosystem' (*SearchCIO*, October 2019) <https://searchcio.techtarget.com/definition/digital-ecosystem> accessed 20 July 2021.

[53] GMF, *Rebuilding Trust in the Digital Ecosystem: New Mechanisms for Accountability* (German Marshall Fund of the United States, 2021).

[54] Formiti, 'The Malaysia Personal Data Protection Act 2010 – All you need to know (Part 1)' (Lexology, 6 January 2021) <https://www.lexology.com/library/detail.aspx?g=ec5c2b84-c3aa-44d1-a61e-df0f35092c63> accessed 20 July 2021.

[55] See UNESCO, 'Rule of Law as a key concept in the digital ecosystem during Internet Governance Forum – interview 2/2' (UNESCO, 12 February 2020) <https://en.unesco.org/news/rule-law-key-concept-digital-ecosystem-during-internet-governance-forum-interview-22> accessed 20 July 2021.

[56] For the brief comments, see Paul Bischoff, 'Data privacy laws & government surveillance by country: Which countries best protect their citizens?' (Comparitech, 15 October 2019) <https://www.comparitech.com/blog/vpn-privacy/surveillance-states/> accessed 20 July 2021.

[57] Naufal Fauzi, 'Data privacy laws: Malaysia has a long way to go' (New Straits Times, 11 February 2019) <https://www.nst.com.my/opinion/columnists/2019/02/459321/data-privacy-laws-malaysia-has-long-way-go> accessed 20 July 2021.

How do national organs react to this problem? The protection of privacy is grounded in common law as the judiciary made an invasion of privacy an actionable tort in Malaysia.[58] The Department of Personal Data Protection ('DPDP') also regularly inspects businesses and recommends best practices for data protection, which are published on their website.[59] This demonstrates how national agencies and the judiciary coordinate to resolve a problem in the digital ecosystem.

Regional actors tend to play an advisory role in improving privacy protection. For example, the Personal Data Protection Commissioner issued a *Public Consultation Paper (PC01/2020)*, dated 14 February 2020, to obtain feedback on 22 proposed amendments to *PDPA 2010*. As a brief summary of the consultation project, three amendments will be analysed accordingly below.[60]

First, should direct obligations be imposed on data processors and require their registration with the Commissioner? The Software Alliance ('BSA'), a group of global software industries (such as Adobe, Amazon Web Services and Microsoft) responded to this consultation. It agreed that data users/controllers should bear the primary obligation of ensuring compliance with data protection laws. However, it stressed that the law should recognise the distinct roles data controllers and data processors play: data processors should comply with the data controllers' instructions and ensure the security of the data they hold. The law should not subject all entities to the same data protection obligations regardless of their roles in handling consumer data, because this can create new risks by requiring companies to disclose information to an unknown consumer. BSA also argues that the mandatory registration of data users would "significantly increase the regulatory burden" and that the Commissioner should adopt a "business-friendly approach and do away with all registration requirements".[61] The Asia Internet Coalition (AIC), an industry association for leading Asia-Pacific technology companies (such as Airbnb, Booking.com, LINE), also responded. AIC echoed the views of BSA that the law should recognise the different roles of data processors and controllers, adding that international practices do not oblige data processors to report a breach to a regulator or data subject, but such actions are "funnelled through the data controller, as they are the controller and owner of the data from the perspective of the data processor".[62]

Second, the paper asked whether a right to data portability should be introduced into the Act, namely to allow individuals the right to acquire and reuse data for other purposes across different networks. BSA advocates against prescriptive rules for data portability because the specific mechanisms for data transfer differ from one service provider to another and are heavily dependent on the specific infrastructure of each organization. Therefore, a prescriptive approach can be more "counter-productive" in some cases. BSA recommended taking a more flexible approach, with the adopting of transparent, industry-led international standards to facilitate data portability. AIC advocated that providing people with control over their information (access, correct, delete and download personal information) makes it easier for them to better choose among services and lowers the barriers to entry for new comparable digital services. AIC also asks the Commissioner to consider existing data portability provisions in the *European Union's General Data Protection Regulation* and *Australia's Consumer Data Rights*.

Third, inspired by the practices of EU, Philippines and North Korea, should data users report data breach incidents as a mandatory obligation, and what should be the guideline for this reporting mechanism? BSA supports the adoption of a mandatory notification for data breach incidents because this promotes trust in the digital ecosystem "by establishing expectations for data stewardship that will reduce the risk of future breaches and ensure that data subjects receive timely and meaningful information about whether their personal information has been compromised". As to the guidelines for reporting, BSA argues the notification standard shall be risk-based and data users should focus their resources on an investigation of the breach and restoring the compromised systems. Further, data subjects should receive notifications from the data user they have a direct relationship with. AIC mirrors the views of BSA, adding that data processors should be excluded from such direct obligations because they do not have the "visibility over the content of personal information controllers" and cannot differentiate between a security breach or personal data breach.

From the above case study, we saw the roles played by the judiciary, national ministries, and regional groups of private actors in bridging the gap of data protection in Malaysia. This author commends the Commissioner's initiative in forming an open dialogue with private companies and regional business

[58] *Lee Ewe Poh v Dr Lim Teik Man & Anor* [2011] 1 MLJ 835.

[59] See Jabatan Perlindungan Data Peribadi, 'Practice' (*DPDP*) < https://www.pdp.gov.my/jpdpv2/tata_amalan> accessed 20 July 2021.

[60] For the entire consultation paper, visit <https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf >.

[61] BSA, *Public Constitutional on the Review of Personal Data Protection Act 2010: Comments from BSA | The Software Alliance* (BSA, 2020).

[62] AIC, *Response to the Public Consultation Paper No. 01/2020: Review of Personal Data Protection Act 2010 (Act 709)* (AIC, 2020).

organisations to help solve a pressing issue, and that such initiatives should be encouraged and adapted to solve other problems in the global digital ecosystem.

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)?

As mentioned before in Part A, Question 3, a Digital Constitution should present a flexible and adaptive framework for the governance of the virtual world based on normative and constitutional values, for example: online protection of fundamental rights and due process. Such values should not operate as an 'anchor', but rather as a guiding beacon of light for more constitutional innovations in the future. Therefore, the digital constitution will always be in a flux. In response to the statement in question, Malaysia's traditional constitutional model has always been in a flux from the beginning of its independence. Responding timely to national threats, Malaysia created two parallel governance regimes: a government subject to the control of the elected Parliament, and the other "emergency regime" giving the government powers to override the Parliament and constitutional supremacy in a state-declared emergency. This dual regime is discussed further in Part B, Question 6.

The digital space has posed many challenges to the traditional ways of governance. At first sight, academics thought the digital revolution may induce direct democracy by letting online users vote directly on political decisions. However, this is untrue because the majority essentially relies on democracy to hold decision-makers accountable, rather than to make decisions themselves.[63] This is exemplified by Mark Zuckerberg's 2009 failed attempt to make his site more democratically legitimate: direct democracy becomes harder or impossible to achieve in digital spaces as a larger number of people is required to vote to make a small change in an intermediary's terms of service. Therefore, a Digital Constitution should address these governance challenges through constitutional innovations. For example, intermediaries can seek different forms of legitimation besides democracy, through due process and adopting corporate social responsibility.

Responding to the second part of the question, the Malaysian *PDPA 2010* does not recognise a right to be forgotten. Generally, the Malaysian judiciary recognises invasion of privacy as a tort in breach of confidence cases especially in doctor-patient relationships or defamation to another person's Facebook account.[64] Although this right is guaranteed under *Article 17 of the EU GDPR*, neither Malaysian courts nor the Commissioner of DPDP have recognised how the right to be forgotten is related to the right to privacy. However, since the legal position on digital rights is still in a flux, this author argues if the case does arise in court, the Malaysian judiciary, considering how it usually analyses foreign case laws, is likely to recognise the right to be forgotten in law. Nevertheless, the right to be forgotten should not be an absolute right, but one that is subject to the social, political and legal contexts.

11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

Although there is no single global Digital Constitution in the world for the time being, it is possible to harmonise certain aspects of national frameworks to achieve a global Digital Constitution. However, to ensure its effectiveness, it should be drafted in a flexible and adaptive manner, respecting the socio-cultural differences of each country. From a Malaysian perspective, what should a global Digital Constitution look like? In summary, a global Digital Constitution should be a simple document, which states: (a) the basic guarantees and aims; (b) the key organs; and (c) liability framework.

First, there should be a charter of rights for the users of digital technology and a set of international aims for the global Digital Constitution. Respect for sovereignty and socio-cultural differences are very important in the context of Malaysia, especially considering the Malaysian human rights narrative, as explained in Part A, Question 3. All rights for online users should be considered in the "regional and national context bearing in mind different political, economic, legal, social, cultural, historical and religious backgrounds".[65]

The global Digital Constitution should aim to resolve some of the pressing issues, such as: battling against misinformation, interstate cooperation for counter-terrorism, prohibition against excessive nudity and

[63] Daniel Valchev, 'Constitutional Dimensions of Information Revolution' in Martin Belov (eds), *The IT Revolution and its Impact on State* (Oxford Hart Publishing, 2021).

[64] Duryana Binti Mohamed, 'The Privacy Right and Right to be Forgotten: the Malaysian Perspectives" (2016) 9 Indian Journal of Science and Technology 1.

[65] ASEAN Human Rights Declaration (AHDR), art 7.

child pornography, and prohibition against online hate speech. The Malaysian government is strongly concerned about the devastating effects of misinformation, and its prevention is one of the core tenets in the *Communications and Multimedia Act (CMA) 1998*. As a countermeasure, the Malaysian Communications and Multimedia Commission (Suruhanjaya Komunikasi dan Multimedia Malaysia, 'MCMC') set up a website, 'Sebenarnya.my', allowing the public to share information on fake news. Recently, in the wake of Covid-19, the Agong (King of Malaysia) has enacted an emergency ordinance which aims to tackle false information causing public disorder in the country.

Malaysia has long expressed its commitment to prevent violent extremism through international cooperation with the United Nations (UN)[66] and by ratifying the *ASEAN Convention on Counter Terrorism*. Malaysian legal scholars define terrorism as "the use of force or terror without legal authority or a threat to use force or terror without legal authority... [which includes] any mode of attack by any person, group, or country, for whatever motive, intention, or justification, aimed against a country or her citizens or properties, be public or private properties, or against important services".[67] The internet should be a safe space – never to be abused for ulterior purposes aiming to cause havoc to a sovereign state. Therefore, the global Digital Constitution should aim to produce a reasonable framework for interstate cooperation against terrorism.

Malaysia has strict local laws against excessive nudity online and child pornography, where 1579 pornographic sites have been blocked by the MCMC in 2018. It is argued that nations tolerate different levels of nudity and the Digital Constitution should provide a flexible framework to accommodate these socio-cultural differences. Since Malaysia's official religion is Islam, as stated in *Article 3(1) of its constitution*, it has low tolerance towards sexual content and the global Digital Constitution must respect this aspect.

Most importantly, although the internet has aided the exercise of freedom of speech, it has also enabled the manifestation of hate speech. Prohibiting hate speech should be a universal aim of the global Digital Constitution because no rights should be exercised in an absolute manner that contravenes another person's human dignity.

Second, the global Digital Constitution should create and confer authority to key organs which help to administer and implement its articles. There should be a registrar for intermediaries, where all intermediaries that willingly register themselves shall adhere to the articles of the global Digital Constitution, imposing universal basic standards of protection for online users using any intermediaries' services. On the other hand, this exerts international pressure on private companies — they risk getting blocked by certain countries if they do not follow the articles of the Digital Constitution.

Further, there should be an oversight board modelled after Facebook. It should be responsible for making difficult decisions on content-blocking and connecting with national agencies that report content against local laws. Facebook's Board is made up of international individuals, controlled by the Board of Trustees — is this composition sufficiently democratic and how can this model be adapted on a global scale? What should be the approach to content-blocking: should it be strictly international or through a "country lens approach"?[68]

Finally, a global Digital Constitution should consider whether intermediaries should be subjected to different liability frameworks under national regimes, or one single supranational regime. The OECD has produced a report discussing certain key principles in influential legal instruments such as the *Digital Millennium Copyright Act (DMCA)* and *E-Commerce Directive (ECD)*.[69] Although these principles can be adopted by the global Digital Constitution, the extent to which this framework is acceptable to Malaysia and other Asian countries remains unclear.

From the problems raised above, it is still too early to give a definite answer as to whether national frameworks can be harmonised to form a global Digital Constitution. However, the homogenization of laws on an international scale must be avoided at all costs. The key to building an effective global Digital Constitution is its respect for socio-cultural and legal differences.

B. Human and Constitutionally Guaranteed Rights

[66] HE Ambassador Muhammad Shahrul Ikram Yaakob, 'Statement at the United Nations High Level Conference of Heads of Counter-Terrorism Agencies of Member States New York' (2018), para 12.

[67] Azhar Abdul Aziz, 'The Burden of Terrorism in Malaysia' (2004) Prehospital and Disaster Medicine 115, 116.

[68] See Dan Svantesson, 'Delineating the Reach of Internet Intermediaries' Content Blocking - "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?' (2014) 11 Scripted 153.

[69] See OECD, 'The Legal Responsibilities of Internet Intermediaries, their Business Practices and Self- or Regulatory Codes' in *Role of Internet Intermediaries in Advancing Public Policy Objectives* (OECD Publishing 2011).

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

To consider what rights are affected, the *Universal Declaration of Human Rights (UDHR)* is the most appropriate document. The *UDHR* is a "milestone document" detailing customary international law on fundamental human rights: "a globally agreed document that marked out all humans as being free and equal, regardless of sex, colour, creed, religion or other characteristics".[70] The *UDHR* shares considerable overlap with the Malaysian constitution as well.

To begin with, *Article 10 of the Malaysian constitution* provides that Malaysians have the freedom of speech, assembly and association. Similarly, *Article 19 of the UDHR* relates to the freedom of expression. Outlined in this clause are the rights to freedom of opinion and expression: to be able to hold opinions without interference and impart information and ideas through media regardless of frontiers or barriers.

The emergency ordinance 2021 was enacted by the Agong after declaring a state of emergency in January 2021. This act criminalises offences relating to 'fake news' specifically about the Covid-19 pandemic. This ordinance raises public concerns because it shared similarities with the previous *Anti-Fake News Act 2018* (repealed). The repealed act brought great controversy because it censored speech and prevented citizens from criticizing certain political aspects of the country. International human rights organisations have also criticised problematic aspects of the 2021 ordinance, such as: the overly vague definition of 'fake news' as any news that are wholly or partly false relating to Covid-19 or the proclamation of emergency, the disproportionate fines going up to MYR 500,000 and six years' imprisonment, and providing jurisdiction to authorities to target anyone as long as their speech concerns Malaysia. Whilst criticising the adoption of this ordinance as the wrong approach, Malaysian academics remained dubious as to whether the Malaysian government will use the powers granted by the emergency ordinance to "recklessly suppress free speech" or as a "short-term remedy for the serious issue of fake news in Malaysia".[71] However, at the time of writing, the state-declared emergency has ended on 1 August 2021 and the Malaysian government does not plan to ask for a further extension from the Agong.[72] Therefore, this ordinance has also lost its legal authority.

Article 12 of the Malaysian constitution and *Article 26 of the UDHR* relate to the right to education. *Clause 1 of this Article in UDHR* outlines that "technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit". Recently, with Covid-19 online learning has been a huge part of education. The internet has made education more accessible in a sense, however, for those without adequate or any access to the internet their access to education is thus limited. Malaysia has been described to have a digital divide, the Straits Time reported viral videos and online reports where students without internet access had to climb trees and walk long distances from their homes in order to reach a signal.[73] As a result of this predicament, the Malaysian Communications and Multimedia Commission (MCMC) has started a long-term project to provide 4G Internet access to villages in Sabah in order to bridge the digital divide. [74]

Finally, *Article 3 of the Malaysian constitution* states that everyone has the right to life, liberty and security of person. Similarly, *Article 12 of the UDHR* relates to privacy and that no one should be subjected to arbitrary interference of their privacy. Clearly, online platforms and the internet interact with this right as cybersecurity becomes an integral part of its use. In 2017, Malaysia experienced a massive data breach of information from mobile phone users. The data breach included phone numbers, ID card numbers, addresses and other data of 46. 2 million customers from around 12 Malaysian mobile phone companies.[75] MCMC started the investigation with the police to find the source of the breach. Civil society organisations had also written an open letter for the *Malaysia Personal Data Protection Act 2010* to be reviewed, calling for a

[70] 'Universal Declaration of Human Rights' (*Amnesty.my*) <https://www.amnesty.my/universal-declaration-of-human-rights/> accessed 2 August 2021.

[71] Sani (n 25).

[72] Liz Lee, A. Ananthalakshmi and Ed Davies, 'Malaysia will not extend state of emergency, says law minister' (*Reuters*, 26 July 2021) <https://www.reuters.com/world/asia-pacific/malaysia-will-not-extend-state-emergency-bernama-2021-07-26/> accessed 2 August 2021.

[73] Hazzlin Hassan, "Malaysia's digital divide makes some students trek up hills and sleep on trees for Internet access." (*The Straits Time*, 7 February 2021) <https://www.straitstimes.com/asia/se-asia/malaysias-digital-divide-makes-some-students-trek-up-hills-and-sleep-on-trees-for> accessed 30 July 2021.

[74] Paul Mu, 'MCMC has long-term plan to provide internet access to Sabah's interior districts' (*New Straits Times*, 21 July 2021) <https://www.nst.com.my/news/nation/2021/07/710423/mcmc-has-long-term-plan-provide-internet-access-sabahs-interior-districts> accessed 22 July 2021.

[75] Rozanna Latiff and Jeremy Wagstaff. "Malaysia investigating reported leak of 46 million mobile users' data." (*Reuters*, 1 November 2017 <https://www.reuters.com/article/us-malaysia-cyber-idUSKBN1D13JM> accessed 2 August 2021.

governmental policy to be introduced to all agencies handling personal data in order to ensure the security and safety of such data.[76] Due to public pressure, the Personal Data Protection Commissioner issued a public consultation paper to acquire feedback from the masses on the proposed amendments to the 2010 Act. One of the amendments involved imposing a mandatory duty of reporting on data users to report data breaches.[77]

There are many factors that prohibit the full awareness and enjoyment of human rights online. Human rights violations on the internet are increasing and National Human Rights Institutions (NHRIs) have a key role to play in order to protect and promote them. Rights on the internet are central to NHRIs' mandates.[78]

2. Who can be defined as a netizen?

'Netizen' is a term first coined by Michael Hauben in 1998 as a portmanteau of 'net' and 'citizen'. Hauben provides two understandings of this term from his perspective stating first that netizens are 'people online who actively contribute to the development of the Net' and that netizens are people who devote time and put effort into improving the digital space and community that they are in. Whilst originally denying 'lurkers' on the internet as netizens, Hauben provided a second potential perspective on netizens being anybody who uses the internet for whatever purpose be it positive or negative.[79] Considering the new formats of social media where 'liking', 'subscribing' and 'sharing' is a form of interaction with the content, even those who once were considered by Hauben a 'lurker' now can contribute to the digital sphere in more passive ways.

Instead, Hauben's perspective that a netizen should contribute to the digital world in some way, this definition can be expanded on. Similar to the term 'netizen' is that of a 'digital citizen' defined by Karen Mossberger. She defined 'digital citizen' to be a person using IT in order to engage in society, government and politics.[80] Not only this, but digital citizens have a comprehensive understanding of how to behave appropriately on the internet and so a responsible citizen will follow and understand digital safety, privacy and etiquette whilst using any IT service.[81] Although this definition provides a broader scope of what a 'netizen' or citizen on the internet may be, it is important to note that the process of being a digital citizen is also not defined as just a citizen that participates in internet activity.

If Hauben defined a netizen as someone who contributes to the digital society, the definition of 'digital citizen' has come to mean someone who contributes to society through their use of technology and the internet. Sociologist, Thomas Humphrey Marshall, has said that digital technology helps to lower barriers of entry into participation in society. In particular, digital citizenship looks at how technology and the digital sphere contributes to politics. Digital citizen participation was then defined in two stages, the first being information dissemination where citizens can be static or dynamic and the second being citizen deliberation.[82]

Both of these definitions and concepts were developed in 1998, and 2008 respectively. In 2021 alone, there were 28 million social media users in Malaysia. As the technology and its uses develop, surely the definition of a 'net citizen' or 'digital citizen' should too. Even comparing Hauben's definition with Mossberger it is clear that the definition slowly expands to encompass the ubiquity of the internet and technology. Using these definitions as a basis, a definition of 'netizen' should be created to encompass the diversity of users and participants in the digital sphere, considering both direct and indirect participation or usage.

Netizens in Malaysia have been ranked by a Microsoft survey as some of the most 'civil netizens'. This survey used a Digital Civility Index to assess the extent of negative behaviour and interactions online. Malaysia ranked fourth out of twenty-five countries for being the least negative online. Though this does not provide a Malaysian definition of netizen, it suggests that in Malaysia, netizens are closer to Hauben's definition in

[76] Civil society organisations, 'After data leaks, Personal Data Protection Act needs review' (*Malaysia Kini*, 6 February 2018) < https://www.malaysiakini.com/letters/411314> accessed 2 August 2021.

[77] For more information on the consultation, see Part A Question 9.

[78] Association for Progressive Communications, "Human rights and the internet: The key role of national human rights institutions in protecting human rights in the digital age" (*Association for Progressive Communications*, 21 June 2017) <https://www.apc.org/en/pubs/human-rights-and-internet-key-role-national-human-rights-institutions-protecting-human-rights> Accessed 30 July 2021.

[79] Michael Hauben and Ronda Hauben, '*Netizens: On the History and Impact of Usenet and the Internet*' (*First Monday*, 1998) <https://firstmonday.org/ojs/index.php/fm/article/view/606/527> Accessed 2 August 2021.

[80] Caroline Tolbert, Karen Mossberger and Ramona McNeal, *Digital Citizenship: The Internet, Society, and Participation* (MIT Press, 2008).

[81] Ershi Qi, Jiang Shen and Runliang Dou, *The 19th International Conference on Industrial Engineering and Engineering* (Springer Berlin Heidelberg, 2013), 742.

[82] Marc Holzer, James Melitski, Seung-Yong Rho and Richard Schwester, *Restoring Trust in Government: The Potential of Digital Citizen Participation* (IBM Center for the Business of Government, 2004).

which users intend to create a better digital space and make positive contributions.[83] Further, the term 'netizen' is largely used when referring to citizens expressing their views, political and social, through the internet. An example on Free Malaysia Today, following the prime minister's announcement of the new cabinet, articles titled 'Netizens blast Ismail over 'same old same old' Cabinet' have been published. Throughout the article 'netizens' are referred to and their indignation over the retained cabinet members.[84] Alternating between the terms 'user' and 'netizen', the Malaysian media frequently uses netizen in the sense of digital citizen participation. Consequently, a combined definition of Hauben and Mossberger may be considered when contextualising a 'netizen' in Malaysia.

3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?

As discussed above, Hauben defines a netizen as either a person who actively contributes to the online community in a positive way, or someone who actively uses the internet whether for bad or good. In basic terms then, a netizen, according to the second definition, could be a 'bad actor'. However, the definition of 'bad actor' differs depending on the discrepancies and laws of each nation.

A 'bad actor' can be briefly defined as a person that exerts a negative effect on the digital space that they interact in. There could be a number of reasons for which their activity is considered negative. Generally speaking, bad actors could first be considered merely as those who commit a cybercrime or illegally in accordance with national and international legislations relating to the Internet. In Malaysia, there are several key legislations regulating the online space: *Copyright (Amendment) Act 1997*, *Computer Crimes Act 1997*, *Digital Signature Act 1997*, *Telemedicine Act 1997*, and most importantly the *Communications and Multimedia Act 1998*. A good example of a bad actor is a person who spreads disinformation about the pandemic in Malaysia. In accordance with the emergency ordinance 2021, anyone publishing fake news about Covid-19 will be criminalised (this takes effect till 1 August 2021).

As for international laws, Malaysia follows the standards of ASEAN (Association of Southeast Asian Nations). On 6 December 2018, ASEAN issued a joint media statement from its 18th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings (TELMIN), detailing its goal to "propel ASEAN towards a digitally-enabled economy that is secure, sustainable, and transformative; and to enable an innovative, inclusive and integrated ASEAN Community".[85] This statement endorsed the *ASEAN Framework on Digital Data Governance*, which aims to facilitate the legal harmonisation of data regulations between ASEAN member states, enhance data management and "promote intra-ASEAN flows of data".[86] This framework lays down an important principle on "data security", which states any data storage centres or platforms which handle data should take appropriate measures to protect the "confidentiality, integrity and availability of any data in their possession, or control against risks such as loss or unauthorised access", as well as redressing data breaches efficiently by "containing the breach and implementing mitigating measures to rectify the breach".[87] Therefore, according to this framework, if an online intermediary which controls, processes or stores data fails to follow national standards on data security and remedy data breaches, they can also be 'bad actors'.

Asides from the national or international laws and standards that are set surrounding the digital sphere and the appropriate way to act, each individual social media platform and or application usually has its own set of terms and conditions, regulations and rules that it enforces. The majority of online platforms have terms of service/terms of use and or community standards or guidelines. These community guidelines do not necessarily reflect the country's legal system, but there is often considerable overlap. These are referred to as 'private codes of conduct' provided by individual online platforms, usually with the consequence of content removal or membership revocation. The most common ways in which these standards are regulated are: the removal of content after users report it as inappropriate, the use of filters blocking certain words from being

[83] Yeoh, Angelin. "Microsoft survey finds Malaysian netizens among the 'most civil' online." *The Star*, 2020, https://www.thestar.com.my/tech/tech-news/2020/02/13/microsoft-survey-finds-malaysian-netizens-among-the-most-civil-online. Accessed 4th Oct 2021.

[84] Jaya, Petaling. "Netizens blast Ismail over 'same old, same old' Cabinet." *Free Malaysia Today*, 2021, https://www.freemalaysiatoday.com/category/nation/2021/08/27/netizens-blast-ismail-over-same-old-same-old-cabinet/?__cf_chl_jschl_tk__=pmd_f9mXPKzSXQHwJA5oBcysrkepBLq9T4dwhtWoPv6YAsg-1633326729-0-gqNtZGzNAnujcnBszQjR. Accessed 4th Oct 2021.

[85] ASEAN, *Joint Media Statement* (ASEAN, 2018).

[86] ASEAN Telecommunications and Information Technology Ministers (TELMIN), *Framework on Digital Data Governance* (2017).

[87] ibid, para 13.

posted or tagged, and AI tools-based machine learning models. Private codes of conduct thus create another standard in which a netizen may be considered a 'bad actor' online.

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)?

It is very important to create and sustain an open and inclusive digital ecosystem that contributes to the public's social and economic wellbeing. As a multicultural country, Malaysia is made up of 67.4% Bumiputera, 24.6% Chinese, 7.3% Indians, and other ethnicities (0.7%).[88]

First, one of the major problems minorities experience in digital ecosystems is the "digital divide". This refers to the gap between groups of people who can effectively use technology such as computers, mobile phones and the Internet for communication and disseminating information.[89] Malaysia should tackle the digital divide to prevent long-term social, political and economic repercussions because minorities can be the future workforce, driving the nation forward. As a developing country, Malaysia has prioritised internet connectivity for all as one of its primary goals to better connect its citizens to economic opportunities, market, information and local social services. According to the 2020 report by MCMC, 88.7% of the total population use the Internet. Majority of those who do not use the Internet are 50 and above (70.8%), and they are either too old to learn about the Internet, a lack of interest, or they have no device. Considering these statistics and the Covid situation in particular, the MCMC proposed to the government that Internet access is no longer a privilege but a basic necessity, and that Malaysia is quite fortunate to have good Internet infrastructure comparable to most developed countries.[90] Without resting on its laurels, MCMC continues to draw up long-term plans to provide 4G Internet access to indigenous tribal villages in the main Peninsula[91] and to disadvantaged communities in the interior districts of Sabah.[92] The MCMC Chairman, Dr Fadhlullah Suhaimi Abdul Malek, also echoed this view by proposing to the government that internet service should be a basic built-in utility (instead of building external telecommunication towers) in the residential neighbourhood, and this can help expedite the process of transitioning to 5G technology.[93] Minority groups (indigenous people and other disadvantaged groups) should be capable of using, contributing to and benefiting from the digital ecosystem through unrestricted Internet access. This helps to transform the existing "manual economy" to a "digitalised economy" that is more resilient against the pandemic. Due to increased Internet use, the Malaysian government could introduce its own contact-tracing application (MySejahtera) which not only collected important location data on the transmission of the virus, but also helped to direct people to local health screening and vaccination facilities.

Second, Malaysia should increase the equitable participation of all minorities by teaching online users ways to respond or report hate speech. Even though most websites targeted at Malaysians contain terms of service, algorithmic moderation and peer-reporting systems that prevent the use of certain vulgar and culturally sensitive words, it is argued that this is insufficient. Hate speech should be criminalised in Malaysia and online users should have an efficient way of reporting the incident to the respective authorities. Further, there should be collaboration between the governments, private actors and society in countering "malign influences in digital ecosystems".[94]

Third, Malaysia should provide ways for minorities to contribute to the digital economy. USAID, an international development agency stationed in the US, suggested that private sectors should provide

[88] Department of Statistics Malaysia, 'Population Distribution and Basic Demographic Characteristic Report 2010' (DSM, 07 May 2015) <https://www.dosm.gov.my/v1/index.php?r=column/ctheme&menu_id=L0pheU43NWJwRWVSZklWdzQ4TlhUUT09&bul_id=MDMxdHZjWTk1SjFzTzNkRXYzcVZjdz09> accessed 22 July 2021.

[89] See Michael Boone, M LaVelle Hendricks, Rusty Valler, 'Closing the Digital Divide and its Impact on Minorities' (2014) 3 The Global eLearning Journal 1.

[90] MCMC (n 27), 120.

[91] Bernama, 'MCMC to improve Internet access under Jendela' (The Star, 4 March 2021) <https://www.thestar.com.my/tech/tech-news/2021/03/04/mcmc-to-improve-internet-access-under-jendela> accessed 22 July 2021.

[92] Paul Mu, 'MCMC has long-term plan to provide internet access to Sabah's interior districts' (New Straits Times, 21 July 2021) <https://www.nst.com.my/news/nation/2021/07/710423/mcmc-has-long-term-plan-provide-internet-access-sabahs-interior-districts> accessed 22 July 2021.

[93] Bernama, 'MCMC suggests state govts count internet access as basic utility in residential areas' (Malay Mail, 6 October 2020) <https://www.malaymail.com/news/malaysia/2020/10/06/mcmc-suggests-state-govts-count-internet-access-as-basic-utility-in-residen/1910001> accessed 22 July 2021.

[94] USAID, *Digital Strategy 2020-2024* (USAID, 2020), 38.

information on international best practices for digital infrastructure and training to local innovators, especially targeted at minority groups. In a similar initiative, the Malaysia Innovation Policy Council is a national think tank aimed at upgrading local policies and regulations to drive innovation by collecting and assessing the viability of digital technology initiatives from the public. This council is composed of the Industry Coordination Committee which facilitates and advises industries for digital technology initiatives, and the Intervention Committee responsible for setting up task force teams from relevant ministries, agencies and stakeholders to find solutions.[95]

To summarise, there are three ways in which Malaysia can embed approaches which are responsive to the needs of minorities: first, bridging the digital divide by providing Internet access; second, increasing the participation of minorities by tackling hate speech; and third, finding ways for minorities to contribute to the digital economy.

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?

Consent is not legally defined in Malaysian data protection laws but efforts have been made to address this issue. So far, the MCMC is more concerned with parental supervision over children's exposure to the Internet than with identifying a certain age as to when children can validly consent to digital services. This author argues that the age to be able to give informed consent in digital space should be the same as the minor's age for entering into contracts.

Section 6(1)(a) of the Malaysian Personal Data Protection Act (PDPA) 2010 stated that sensitive personal data cannot be processed without the explicit consent of a data subject. However, the legislation provides numerous exceptions to the processing of data without consent. For example: when data processing is necessary for contractual performance to which the data subject is a party, taking steps to collect information before entering into a contract, complying with legal obligations to which the data subject is subjected to, to protect the data subject's "vital interests", for justice administration or exercise of functions conferred on a person under law (*Section 6(2)*). Further, personal data can only be processed for activities directly related to the lawful purpose and is not excessive (*Section 6(3)*). There are also additional circumstances in which sensitive personal data can be processed under *Section 40(1)*: for medical purposes, purposes of obtaining legal advice or for legal proceedings, and when the data subject deliberately made personal data public. Noting that the requirement for consent is incidental to the purpose and limits of data processing, the Commissioner sought feedback to redraft *Section 6* to add clarity to the concept in a recent *Public Consultation Paper (01/2020)*. Should consent be defined in one specific provision and should there be a default definition of consent?[96]

BSA argues that the concept of consent shall focus on the objective of obtaining consent, and not the means of acquiring it. The act should recognise the validity of an informed/accessible opt-out option and implied consent as part of international best practices. The Act should refrain from mandating consent to be acquired multiple times unless material changes occur to the processing of data. BSA argues consent should be implied when consumers reasonably expect personal data to be collected and processed. Examples include accessing public transport services using electronic fare cards.[97]

AIC argues against a narrow definition of consent and that the act should recognise data processing for "legitimate business purposes that are consistent with the context of the transaction or expectations of consumers". AIC states that a further clarification on the meaning of consent can be included in the same section or a separate subsection. More importantly, AIC asks the commissioner to consider when new consent is required, the definition of deemed consent, and when deemed consent may be insufficient. AIC echoes BSA's views that consent should not be required multiple times in the absence of material changes because this can be "time-consuming, disruptive and result in 'consent fatigue'". For example, in Europe, the majority of Internet users blindly ignore or accept messages requesting consent to cookies. AIC also argues that the new act should include certain circumstances that allow the processing of personal data without actively obtaining consent, supplemented with guidelines and scenarios illustrating when it is appropriate to do so. Finally, AIC advocates against imposing restrictions on the organisations' "legitimate cybersecurity efforts;

[95] For more information, see MDEC, 'MDEC is introducing the Malaysia Innovation Policy Council (MIPC)' (MDEC, 30 April 2019) <https://mdec.my/news/mdec-is-introducing-the-malaysia-innovation-policy-council-mipc/> accessed 22 July 2021.

[96] KKMM, *PC 01/2020 - Review of Personal Data Protection Act 2010* (KKMM, 2020), 6.

[97] BSA (n 61), 5.

implementation of measures to detect or prevent fraud or identity theft; the ability to protect confidential information; or the exercise or defence of legal claims".[98]

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?

As a start, the Malaysian constitution confers powers to maintain public order in *Articles 149-151*. It is argued that public order should be defined with a non-exhaustive list of circumstances, adaptable to the current situation. Disorder in the offline world should definitely influence the definition and management of public order online, especially during a period of political, economic and health instability to preserve the wellbeing of the people.

From a Malaysian perspective, public order is defined in a flexible manner, adaptable to any changes in reality. To illustrate, the Agong characterised the Covid-19 pandemic as a danger to public order, declaring a state of emergency even though a health crisis is not explicitly listed in *Article 149(1)(a)-(f) of the constitution* as a situation of disorder. This is because Covid-19 falls within the definition provided in *Article 150(1)*, referring to any circumstances endangering national security, economic life and public order as perceived by the Agong. In the event of danger to public order, the legislature can make valid laws that disregard fundamental rights guaranteed under the constitution (liberty of the person, prohibition of banishment and freedom of movement, freedom of speech, assembly and association, and rights to property). Any amendments to such emergency laws do not need to pass through the two Houses of Parliament (*Article 149(1)*). The Agong can adopt emergency ordinances which have the same effect as an Act of Parliament (in the event that Parliament is suspended) (*Article 150(2b)-(2c)*). The Malaysian government also has powers to declare a state of emergency when public order is endangered. This in effect grants the executive many powers, including: the suspension of Parliament and elections, imposing curfews and movement restriction orders.[99]

These constitutional provisions aiming to resolve emergencies are known colloquially as 'emergency laws'. In effect, they produce two parallel legal regimes of governance in Malaysia: a cabinet answerable to an elected Parliament under normal circumstances, and the "emergency regime" which confers powers on the Government to take action without parliamentary authorisation. These emergency powers override the guarantees of the constitution, "graphically illustrat[ing] the import of a continuous state of emergency in the country".[100] Declaring a state of emergency raises political, legal and social problems because it undermines constitutional supremacy (*Keluhuran Perlembagaan*) as stated under the National Principles of Malaysia (*Rukun Negara*). However, the subjugation of constitutional supremacy is not without cause — Malaysian laws and politics are strongly influenced by its unique historical experience characterised by the numerous political and ethnic conflicts before and after its independence. In summary, there have been a total of six declarations of emergency: the 1948 battle against the Malayan Communist Party, the Indonesian conflict in 1964, the 1966 constitutional impasse at Sarawak, the ethnic conflict causing grave injuries in 1969, the worsening relations between Central and Kelantan in 1977, and finally the rise of the new Prime Minister (Muhyiddin) and Covid-19 in 2021. It is apparent that emergency laws are a useful political and legal tool "with an authoritarian pedigree", especially for the purposes of maintaining political stability in times of crises.[101] Without the flexibility and political strength bestowed upon the governing party, Malaysia would have been defenceless before these national threats and the multicultural nation would have never existed.

The protective spirit of emergency laws have permeated through time and adapted its application to modern technology. Hence, situations of disorder in the offline world do influence the management of public order online in Malaysia. This is evidenced by the variety of powers police officers have over the online world for the purposes of criminal investigation. For example: policemen can gain access to classified data stored in a computer for police investigation purposes (*Section 116B*, *Criminal Procedure Code*) and intercept communications to find evidence for terrorism and corruption with the Public Prosecutor's authorisation (*Section 116C of the Criminal Procedure Code*; *Section 6*, *Security Offences (Special Measures) Act 2012*; *Section*

[98] AIC (n 62), 8-10.

[99] For a brief summary, see Nadirah Rodzi, 'Malaysia's state of emergency: What you need to know' (The Straits Times, 12 Jan 2021) <https://www.straitstimes.com/asia/se-asia/malaysias-state-of-emergency-what-you-need-to-know> accessed 9 July 2021.

[100] Cyrus Das, *Emergency Powers and Parliamentary Government in Malaysia: Constitutionalism in a New Democracy* (Brunel University, 1994).

[101] Mohd Rizal Yaakop, 'The Emergency Law in Malaysia – Political Security or Liability?' (2010) Universiti Kebangsaan Malaysia 1.

43, *Malaysian Anti-Corruption Commission Act 2009*). In the event that the offline world suffers from severe concerns of national security, or when a state of emergency is declared, *Section 266 of the CMA 1998* grants special powers over the digital realm. These powers include: suspending licence, taking temporary control over network facilities, withdrawing the use of network facilities, preventing certain communications and taking possession of customer equipment.

To conclude, public order should be defined in a flexible manner to give maximum power and flexibility for the nation to defend itself. Situations in the offline world should affect the maintenance of public order online, exemplified by the powers granted to the government in the event of a state-declared emergency.

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?

The state is and should be allowed to impose Internet shutdowns, slowdowns and communication throttles during a state of emergency, but this must not jeopardise the citizens' ability to make distress calls for help (*Section 266, CMA 1998*). Although such a power exists, it has never been used for the purposes of public order and hopefully nothing in the future will transpire to necessitate the imposition of Internet shutdowns.

Considering instances of Internet shutdowns from foreign jurisdictions, governments often impose Internet shutdowns to affect the architecture of the Internet and the dissemination of information. This should be differentiated from online censorship, which targets certain content; whereas Internet shutdowns treat all traffic as immoral or illegal content. It is important to recognise that the Internet is the source of information and relevant (though not a necessity) to the exercise of democratic rights such as the freedom of expression and assembly. Hence, the effects of Internet shutdowns in the digital world must not be ignored. How do states justify Internet shutdowns? Most authoritarian governments argue the imposition of communication throttles are essential to "pursue legitimate interests, such as national security", and they rarely implement shutdowns in a legal and transparent manner. [102] Fortunately, in Malaysia, when a state of emergency is declared to justify the use of emergency powers, the Agong produces an emergency ordinance which explains the reason for such actions, backed with evidence. In addition, the Malaysian constitution and laws do provide legal justifications for the use of such powers. Therefore, Internet shutdowns are imposed through a legal and transparent process.

What is the socio-legal rationale for Internet shutdowns? Sometimes, social media becomes a tool for disseminating false information and indirectly contributes to the escalation of violent unrest in certain countries.[103] From a Malaysian perspective, the socio-legal rationale for imposing Internet shutdowns would definitely be the maintenance of public order, when influenced by the severe political instability in the offline world. Technically, the right to Internet access is not recognised by the United Nations as a human right. Many human rights activists argue that the right to access the Internet is essential for people to exercise their rights of freedom of expression. The United Nations had expressed similar sentiments: measures that "intentionally prevent or disrupt access to or dissemination of information online" raise human rights concerns.[104] However, it is critical to remember that digital technology is more of a tool to enable the freedom of expression – much like a telephone, but access to it is not a human right.[105] From the Malaysian perspective of human rights, the rights to freedom of expression, assembly and association can be suspended in a state of emergency, as stated in the constitution. This is also in line with the *ASEAN Human Rights Declaration (AHDR)*, because human rights and fundamental freedoms must be exercised in a manner that "meet[s] the just requirements of national security, public order, public health, public safety, public morality, as well as the general welfare of the peoples in a democratic society" (*Article 8*).

To summarise, the key focus should be on the legitimate purpose of imposing Internet shutdowns, and whether the process is legal and transparent. Malaysia should have the power to impose such restrictions in the event that the Internet becomes a tool abused by harmful actors to destroy the peaceful foundations of the nation.

Social Media Councils

[102] Giovanni de Gregorio and Nicole Stremlau, 'Internet Shutdowns and the Limits of Law' (2020) 14 International Journal of Communication 4224.
[103] ibid, 4229.
[104] Human Rights Council, 2016, res. 32/13, para. 10.
[105] Gregorio and Stremlau (n 102), 4226.

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?

This issue focuses on the proposal by Article 19 (A19) to have social media councils which are independent from the intermediaries to protect the right to freedom of expression.[106] It is argued that the Social Media Council (SCM) model can only work in Malaysia if stakeholders respect and reflect the nation's socio-cultural differences and interests. Therefore, it cannot be reinterpreted on a larger scale for the purpose of monitoring human rights. Unfortunately, the SCM is not the right model for Malaysia.

The crux of the problem SCM aims to tackle is the modern context of digital dominance by private companies — they exert substantial influence over critical public debates and the rights of freedom of expression should be protected in this context. An SCM is defined as a "multi-stakeholder accountability mechanism", providing a transparent and accountable forum in addressing issues of content moderation, following the standards of international human rights.[107] As mentioned repeatedly, Malaysia does not adhere to the international narrative of human rights strictly, but rather focuses on promoting community-based values. For example, to protect the wider community, rights of freedom of expression, assembly and association can be suspended. Further, Malaysia has its own organisation responsible for monitoring and reporting immoral and illegal content (MCMC). From the beginning itself, it is hard to see how an SCM can contribute to the Malaysian digital social fabric.

First, the SCM model proposes a "voluntary accountability mechanism" that pulls the control of social platforms and content moderation away from the rightful sovereign control of the state. A19 believes many state laws on the Internet grants "disproportionate censorship powers to the state, whether through prison terms, fines or content blocking powers, chilling free expression, or to outsource regulation to private companies with no proper integration of international standards". In terms of policy, this statement does not take into account the historical development of Malaysia as a developing nation and its multiracial/multi-religion/political struggles as a newly set up democracy. It is the emphasis on community welfare over individual rights, and social/economic rights over civil/political rights that helped Malaysia develop into today's peaceful and multiracial society. In terms of law, Malaysia does not adhere strictly to the international human rights discipline, but rather adopts the *AHDR* narrative of human rights. Further, the exercise of the right to freedom of expression is subject to the political and social context of Malaysia, in particular: the maintenance of public order. Therefore, A19's proposals: (1) to have an SCM and/or independent judicial body which externally evaluate the social media's decision in content-blocking (due to violation with local laws); [108] or (2) to have multiple stakeholders that are independent from the government as advisors, do not address the legal and policy considerations Malaysia faces.

Second, the direct application of international standards as binding law or a code will not work in the context of Malaysia. A more viable option can be a code of Malaysian societal values binding on social media — but this is already being implemented by MCMC (a national body with jurisdiction over Malaysia), and there is no need for another SCM serving a similar function. Further, Malaysia has its own advisory and appeals mechanism for content moderation.

It is clear that the SCM is not the right fit for Malaysia due to its adherence to international human rights. However, this model raises some important questions: is it possible to have an ASEAN-based SCM that exercises control over all member states, and is this desirable considering the differences between each Asian state?

C. Privacy, Information Security, and Personal Data

Personal and Non-Personal Data

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

Personal data identifies a natural person whereas non-personal data does not identify the individual. Personal data can include the name, date of birth, gender, domicile, sexuality, ethnic origin, educational background, health issues and opinions of an individual.

[106] For more information, see Article 19, 'Social Media Councils: Consultation' (Article 19, 11 June 2019) <https://www.article19.org/resources/social-media-councils-consultation> accessed 9 July 2021.

[107] Article 19, *The Social Media Councils: Consultation Paper* (2019), 3.

[108] ibid, 8.

Under Malaysian law, the *Personal Data Protection Act (PDPA) 2010* enshrines safeguards to protect data used in commercial transactions.[109] The *PDPA* was influenced by the *European Union Data Protection Directive 95/46/EC*.[110] It incorporates six principles of data protection.

The six principles include the general principle of consent which requires the individual to agree to the collection and processing of data; the notice and choice principle which informs the individual about the nature and purpose of collecting personal data; the disclosure principle which requires personal data to be disclosed only with consent that is obtained either at the time of disclosure or at the time of data collection; the security of the stored data and prevention of misuse, modification, unauthorised or accidental access, loss, theft, alteration, disclosure or destruction of data through adequate security measures; the retention principle which requires that data be deleted when it is no longer required; the data integrity principle concerning the accuracy of data; and the access principle which gives an individual the right to access and rectify inaccurate data.[111]

The *PDPA* only covers personal data in commercial transactions with the exception of data processed by credit reporting agencies. The Registrar Office of Credit Reporting Agencies under the Ministry of Finance is responsible for regulatory oversight of credit reporting agencies. The *Credit Reporting Agencies Act 2010* was also adopted by parliament.

The Department of Personal Data Protection (PDP) is responsible for enforcing the *PDPA*. The Commissioner of the PDP has to deal with disputes over personal data protection. The Commissioner is advised by the Personal Data Protection Advisory Committee, which is appointed by the Ministry of Communications and Multimedia. The decisions of the commissioner can be appealed at an Appeal Tribunal of the department. These decisions may include decisions concerning registration of data users (businesses which collect and store data); the registration of a code of practice; enforcement notices; and investigations of complaints under the *PDPA*. If a data user is not satisfied with a decision of the appeals process, the data user can then approach the High Courts of Malaysia for judicial review.

The Malaysian *PDPA* mirrors elements of the *GDPR* and the *UK's Data Protection Act*. The Office of the Commissioner can undertake inspection visits after serving a notice on a data processor. Many of the disputes since the *PDPA* was adopted have concerned data processing without a certificate of registration. In February 2020, the commissioner invited the views of the public regarding the improvement of the *PDPA*.[112]

The *PDPA* covers the sectors of banking and financial institutions, insurance, communications, utilities, health, tourism and hospitality, education, real estate, direct selling, services (e.g., legal, accountancy, business consultancy, engineering, architecture, recruitment companies, retail and wholesale), transportation, brokerage and moneylending.

The *PDPA* statute does not clearly define consent. The *Personal Data Protection Regulations 2013* mandates that consent must be recorded by the data user. The codes of practice, which exist for the utilities, financial, aviation and insurance sectors, include specific provisions for obtaining consent. The code of practice for the electricity sector mandates that consent must be recorded either in the form of a signature or a clickable box.

The *PDPA* does not cover personal data collected by the Malaysian government. This leaves the door open to surveillance activity. The Malaysian government can justify surveillance on grounds of national security and threats to public order.

Non-personal data may include public data (i.e. generic or anonymous data of land records, vehicle registration and public health information); community datasets (i.e. data collected by local government and utility services to understand community issues); datasets collected by the private sector in the telecoms, e-commerce and ride-sharing industries; and data collected privately through the application of algorithms and proprietary knowledge. The protection of non-personal data from abuse or misuse is ambiguous in Malaysian law and this will be discussed in detail at Part C, Question 2.

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

Non-personal data is data that does not contain any personal information, such as: a person's name, their date of birth or age. Data will be considered non-personal as long as there is no information that could

[109] Personal Data Protection Act 2010.

[110] Shanthi Kandiah, "The Privacy, Data Protection and Cybersecurity Law Review: Malaysia." (*The Law Reviews*, 21 October 2020) <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/Malaysia> Accessed 28 July 2021.

[111] Personal Data Protection Act 2010 s6, 7, 8, 9, 10, 11, 12.

[112] Kandiah (n 110). For more information on the public consultation, see Part A, Question 9.

identify a natural person. This kind of data can be split into three categories: public, private and community non-personal data. Regulation of data in Malaysia is governed by the *Personal Data Protection Act 2010 (PDPA)*. However, this act relates to personal data and not non-personal data. The future proposed amendments to the act by the Department of Personal Data Protection continue to focus on the storage and processing of personal data. Currently, there is little information or legislation regarding non-personal data in Malaysia.

Beyond Malaysia, the EU and specifically the *General Data Protection Regulation (GDPR)* provides principles as to how personal data should be processed, regulated and handled, but at the same time remains silent on the regulation of non-personal data. The *EU Regulation on a framework for the free flow of non-personal data* in the EU is the sole European legal instrument detailing the regulation of non-personal data.[113] Allowing the free flow of non-personal data raises important ethical and legal concerns. Most notably, the definition of non-personal data is "data other than personal data" as defined in the *GDPR*.[114] The differentiation between personal and non-personal data is not as clear-cut as the laws stipulate. Academics argued it has become increasingly "burdensome" to differentiate the two due to technical and legal factors: there is no single legal test for whether a data is personal or non-personal, and the growing sophistication of data analysis algorithmic systems make it easier to re-identify what seems to be non-personal data as personal data ("link datasets and infer personal information from ostensibly non-personal data").[115] This creates the danger of enabling the free flow of personal data (though seemingly non-personal to the layman's eyes) throughout the European Union and possibly risking critical data breaches. Although problems have yet to surface since the 2018 Regulation, this author remains wary of the vague distinction between personal and non-personal data.

Aside from some of these ethical considerations, there are economic considerations related to non-personal data. *GDPR* and the EU advocate that there should be freedom of movement of non-personal data within the European community. Making the data publicly available allows all businesses to store and process data anywhere in the EU, reducing the costs and barriers to data processing and storage because businesses no longer have to comply with data localisation requirements (such as having a data centre in an EU member state to store and process data).[116] Non-personal data can aid small businesses in their advertising, targeting their market and designing products thus only allowing certain businesses to have access to non-personal data can provide them with an unfair advantage within the market.

As a summary, Malaysia has to balance numerous ethical, legal and economic considerations in the regulation of non-personal data, namely: preventing the free flow of personal data, risking large scale data breaches and helping businesses grow by reducing barriers and costs to storing/processing non-personal data. Currently, Malaysia is still in the process of reforming its personal data protection laws, therefore the regulation of non-personal data should not be the prime focus of the legislature for the time being until the basic data protection laws have established their legal authority in the legal system.

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?

End-to-end encryption is a crucial tool for the protection of privacy for internet users. End-to-end encryption allows for the communication between two parties to exist without interference from a third-party or even the host platform. This technology ensures that only parties to a conversation can access all content being shared, accordingly applications that provide end-to-end encryption are utilised by civilians as well as those in society with a need to communicate sensitive information privately like the medical and media industries. End-to-end encryption is vital to ensure a democratic society free from state interference in private communication. The privacy of end-to-end encryptions should be sacrosanct. Traceability can potentially infringe the right to privacy. There has to be legal safeguards to ensure that traceability is not authorised arbitrarily or for a gross misuse of power.

Notwithstanding the importance of privacy, a backdoor to end-to-end encryption has proven useful for law enforcement purposes, including to counter online harm. In Malaysia, end-to-end encryption has been

[113] Council Regulation (EC) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59.

[114] ibid, Art 3(1).

[115] Michèle Finck and Frank Pallas, 'They who must not be identified – distinguishing personal and non-personal data under the GDPR' (2020) 10 International Data Privacy Law 11.

[116] 'Free flow of non-personal data' (*European Commission*) <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data> accessed 2 August 2021.

viewed as an obstacle to crime prevention. The *Security Offences (Special Measures) Act 2012* confers powers on the Public Prosecutor to authorise any police officer the power "to intercept any message transmitted or received by any communication"[117] in relation to national security offences. The Act also allows authorised intercepted messages to be used as evidence in court.[118] However, the *Security Offences (Special Measures) Act* does not detail whether these intercepts can be made when communications are encrypted. Therefore, it cannot be said that the act provides a legal backdoor to encryption or seeks to provide a backdoor to encryption but rather that communication that is not encrypted can and will be intercepted when they indicate a perceived threat to Malaysian security.

Section 233 of the Communication and Multimedia Act 1998 criminalises any "communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person."[119] The section also sanctions individuals who "initiate(s) a communication using any application service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number of electronic addresses."[120] As this section applies to "any application service" it could be interpreted to include platforms that use end-to-end encryption. This interpretation of the *Communication and Multimedia Act* is aided by the inclusion that parties involved need not be identifiable. Thus, this act may indicate the existence of a backdoor to end-to-end encryption in Malaysian law when the substance of communications is annoying, abusive, threatening or harasses another individual. This gives a broader scope of power compared to the power to intervene in encrypted messages put forward by the EU which suggests a backdoor can only be used in grave situations such as threats to public security or to aid in the prevention of child exploitation.[121]

However, traceable technology can be used to target a wide segment of the population on politically-motivated or discriminatory grounds. Malaysia is a suspected recipient of cyberespionage technology from Circle, a company which sells spyware to governments only.[122] Circle is part of the NSO Group which has developed Pegasus, a software that hacks into WhatsApp accounts. The authors of Citizen Lab claimed the Royal Malaysian Police can monitor private messages on platforms like Facebook and WhatsApp with the help of the Malaysian Communications and Multimedia Commission (MCMC). Nevertheless, it is important to note that this claim is only substantiated with photos of the Circles device found in Pixcell Mazda Farmer, whose operator's identity cannot be verified. Although Inspector General of Police has cited the need to monitor online hate speech to justify its monitoring of social media and instant messaging platforms, NGO Empower argues "it remains unclear how the police and Malaysian Communications and Multimedia Commission (MCMC) intend to 'monitor' the expressions and activities of social media and instant messaging users in Malaysia, and how the data collected will be used". Empower also added that "Facebook alone has 14 million users in the country. Questions as to the scale and scope of the monitoring, the methods (cyber-stalking, communication interception, malware etc), the storage and protection of data collected must be answered to the satisfaction of the people of Malaysia".[123]

From a commercial angle, businesses are increasingly adopting encrypted systems for internal messaging purposes. Using end-to-end encryption ensures a strong level of security for messages. Businesses are using a multitude of applications for end-to-end encryption in their communications. In line with the right of a data subject to access and rectify personal data, the *GDPR* in the EU now allows "Subject Access Request".[124] This means a business has to decrypt encrypted data in the event of a request from the data subject. Therefore, a data subject's right to access its own encrypted data should be one of the instances

---

[117] Security Offences (Special Measures) Act 2012, s6(b).

[118] ibid, s24.

[119] Communication and Multimedia Act 1998, s233(1)(a).

[120] ibid, s233(1)(b).

[121] 'End-to-End Encryption With Backdoor – These Are The EU's Plans' (*Boxcryptor*, 2 March 2021) <https://www.boxcryptor.com/en/blog/post/e2ee-weakening-eu/?utm_medium=post&utm_source=newsletter&utm_campaign=en.newsletter.b2bb2c.awareness.politics&utm_content=e2ee.weakening> accessed 8 August 2021.

[122] Citizen Lab. "Uncovering the Clients of Cyberespionage Firm Circles." citizenlab.ca, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/. Accessed 29 July 2021.

[123] 'The PDRM Will Read Your WhatsApp Messages, Leading To Accusations of Privacy Invasion | Coconuts KL' (*Coconuts*, 12 January 2016) <https://coconuts.co/kl/news/pdrm-will-read-your-whatsapp-messages-leading-accusations-privacy-invasion/> accessed 8 August 2021.

[124] PrivSec Report, 'The EU GDPR Data Encryption And Decryption' (*GRC World Forums*, 2021) <https://www.grcworldforums.com/gdpr/the-eu-gdpr-data-encryption-and-decryption/156.article> accessed 8 August 2021.

where a backdoor to end-to-end encryption can be legally allowed in Malaysian law. Businesses have to adopt the most secure systems of end-to-end encryption. Under the Mobile Device Management (MDS) systems, businesses can easily gain access to an employee's device. This may spark concern from employees who may be unwilling to share data that is unrelated to the business. The escrow approach involves storing all encryption and decryption keys in a single location. However, the confidentiality of access to these keys needs to be ensured. A pragmatic approach involves the Key Management Server (KMS) under which keys are issued to a data subject by an IT department in a business upon a Subject Access Request.

From an international perspective, *Article 17 of the International Covenant on Civil and Political Rights (ICCPR)* protects the right to privacy, stating that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[125] The UN Human Rights Committee in its *General Comment 16* regarding the interpretation of *Article 17 of the ICCPR* states that "Compliance with Article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".[126] *General Comment 16* stresses that any interference with the right to privacy has to be in keeping with the rights and freedoms outlined in the *ICCPR*.

On the other side of the spectrum, the European Union has shone a light on the incompatibility between end-to-end encryption and ensuring public security. Indeed, in the draft council resolution on encryption entitled *Security Through Encryption and Security Despite Encryption* published 16 November 2020, the EU recognised that "the digitalisation of modern societies brings with it certain vulnerabilities and the potential for exploitation for criminal purposes".[127] Indeed, many law enforcement organisations depend on information gathered over the internet to prevent or investigate criminal behaviour.

Although Malaysia has never ratified the ICCPR and its constitution states the right to privacy can be set aside in situations of public disorder, end-to-end encryption still forms a vital security guarantee for personal correspondence via electronic means. Therefore, traceability should not be the norm. Exceptions should be authorised after a due process review, i.e., warrant based on reasonable grounds of public interest. Any authorised interference should be proportional and necessary to the extent required for the public interest and to protect the human rights and civil liberties of others.

As a summary, a legal backdoor to end-to-end encryption can be potentially beneficial and detrimental at the same time. From a national security perspective, such backdoors are incredibly helpful for criminal investigations and maintaining public order in the online space by preventing terrorist activity and transfer of obscene communication. However, this can also be misused for politically-motivated purposes if there is no proper safeguard. From a commercial perspective, businesses should be allowed to provide data subjects access to their own data and be careful in handling their employees' privacy. To avoid abusing such a promising tool, due process and legal authorisation should be the primary focus in enabling legal backdoors to end-to-end encryption.

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?

The importance of compliance with complex data protection at times of crisis should not be overstated. Regulatory sandboxes should definitely play a role during events of crises: where data protection and privacy laws are relaxed with the aim of finding solutions or creating products which solve the current dilemma. A regulatory sandbox is a framework designed to "allow small scale, live testing of innovations by

[125] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.

[126] UN Human Rights Committee General comment No. 16 (right to privacy, family, home and correspondence and protection of honour and reputation) Thirty-second session (1988) para 10.

[127] European Council, 'Draft Council Resolution on Encryption Security through encryption and security despite encryption' (*Council of the European Union*, 16 November 2020) <https://data.consilium.europa.eu/doc/document/ST-12863-2020-INIT/en/pdf> accessed 8 August 2021.

private firms in a controlled environment... under the regulator's supervision",[128] in the temporary absence of legal control.[129]

The objective of the regulatory sandbox should be tailored to solve the crisis. For example, if the crisis is a resurgence of the COVID-19 pandemic, the objective of the sandbox will be monitoring and containing the spread of COVID-19. Sometimes, the objective of a sandbox should not focus solely on whether the product can be launched, but from a regulator's angle — should existing laws on data protection or privacy be relaxed and/or reformed to better meet the demands of similar crises?[130]

The eligibility criteria for innovators to participate in the sandbox depends largely on whether the regulator has the exclusive authority in a certain field. When entities apply to be part of the sandbox, the product or service provided must aim to solve the crisis, but it is disruptive to the current regulations, though with clearly defined parameters and risk management.[131] The duration of the sandbox shall be tailored to meet the needs of the crises with an option for time extension, granted at the regulator's will. The applicant shall notify the regulator and request for the extension before the project expires.

There are two approaches in setting up regulatory sandboxes: thematic or multi-industry. Central Bank Malaysia (Bank Negara Malaysia, 'BNM'), Securities Commission (Suruhanjaya Sekuriti, 'SC') and Ministry of Transport (Kementerian Pengangkutan Malaysia, 'MOT') have set up thematic regulatory sandboxes with specific themes, aimed at a single industry. The latest multi-industry regulatory sandbox in Malaysia is the National Technology and Innovation Sandbox (Sandbox Inovasi & Teknologi Nasional, 'NTIS'), which aims to facilitate technological innovations that can solve the economic challenges caused by the COVID-19 pandemic.

It is argued that a crisis-oriented regulatory sandbox is more likely to be multi-industry than thematic. However, multi-industry sandboxes face particular challenges, especially when the 'owner' of the regulatory sandbox does not have the authority to relax certain regulations. Hence, the owner of the sandbox must engage the appropriate national agencies before developing a regulatory framework to fit the innovation. This can be done by setting an open and collaborative platform between various ministries to cater for the discussion and establish a "cross-functional group consisting of representatives having multiple expertise from different regulators".[132]

What does the regulatory framework of a crisis-oriented sandbox look like? For starters, one may consider the framework set up by the Information Commissioners' Office (ICO) which aims to soften laws. Participants in the regulatory sandbox receive a statement of 'comfort from enforcement', which essentially states that "any inadvertent contravention to the data protection legislation as a result of product or service development, whilst participating in the sandbox, will not immediately lead to regulatory action."[133] Malaysia has its own data protection laws, contained in the *Personal Data Protection Act (PDPA) 2010*. *Section 46 of the Act* allows ministers (upon the recommendation of the Personal Data Protection Commissioner and by order published in the Gazette) to exempt certain people from the application of the act. This provision can form the basis of the regulator's power to relax regulations for innovators who use personal data in this sandbox.

What principles shall ground the operation of this regulatory sandbox? Safeguards shall be built into the sandbox to protect the rights of data subjects, such as: the need to disclose and inform consumers the type of data being collected. Failure to abide by such safeguards may terminate the entity's right to participate in the sandbox. The safeguards shall be based on the seven principles of data protection as established by the Department of Personal Data Protection (*Jabatan Perlindungan Data Peribadi*, 'DPDP')[134] and the ASEAN Framework on Digital Data Governance (adopted by the ministers on 6 December 2018).[135] In summary, both the principles of data protection by DPDP and ASEAN prohibit unauthorised processing of personal data without the consent of consumers and the storage of personal data beyond a certain time limit. These principles also mandate the data to be constantly updated for its intended use to prevent misleading

[128] Ivo Jenik and Kate Lauer, *Regulatory Sandboxes and Financial Inclusion* (CGAP, 2017), 1.

[129] Mohamad Izahar Mohamad Izham and Amiza Ahmad Murad, 'Cultivating Innovation through Regulatory Sandboxes' (2020) ASEAN Insiders 1, 2.

[130] Mueller, *FinTech: Considerations on How to Enable a 21st Century Financial Services Ecosystem* (Milken Institute, 2017).

[131] See Izham and Murad, 4.

[132] GSMA, *Proposal for TELSOM/ATRC: Advancing the ASEAN-GSMA Policy Dialogue on Cross Border Data Flows* (2019), 5

[133] ICO, 'What will happen if our application to the Sandbox is successful?' (ICO) <https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/what-will-happen-if-our-application-to-the-sandbox-is-successful/> accessed 12 July 2021.

[134] Department of Personal Data Protection, 'Principles of Data Protection' (Official Portal of Department of Personal Data Protection) <https://www.pdp.gov.my/jpdpv2/public/principles-of-data-protection/?lang=en> accessed 12 July 2021.

[135] TELMIN (n 76).

information and ensure that access to such data is "adequate, relevant and transparent".[136] All entities participating in the project shall provide a clear 'Sandbox Plan' and abide by the obligations to ensure the project proceeds efficiently.

To conclude, a crisis-oriented sandbox is a very useful tool for Malaysia to disregard certain legal bars temporarily for a greater cause. However, at the same time, such sandboxes shall provide safeguards for data subjects and rules to prevent its abuse.

Intelligence Agency

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

The Malaysian External Intelligence Organisation (MEIO) operates at a high level of secrecy. Unfortunately, there is virtually no reliable source of information on the Internet in terms of its operation and it has very limited media presence. Its most recent media appearance is that its former head, Datuk Hasanah Abdul Hamid, sent a letter requesting help from the American intelligence agency (CIA) to turn the votes of Malaysia's General Election 2014 in favour of the notorious Prime Minister Najib Razak.[137] Hasanah was later charged with criminal breach of trust for misappropriating USD $12.1 million in public funds. The High Court granted Hasanah a discharge not amounting to acquittal on 12 April 2021 because the deputy public prosecutor exercised his discretion under *Article 145(3) of the Federal Constitution*, and she will be charged on a later date.[138]

D. Intermediary Regulation

Online Harms and Netizens

1. How do we define online harms?

Although 'online harms' is not defined in Malaysian laws, it is a phrase used in a UK government initiative, the *Online Harms White Paper* which aims to define and identify online harms and provide solutions and suggestions to minimise and eradicate them.[139] This UK initiative could serve as a guideline to incorporate into, or create laws and regulations relating to online harms in Malaysia. Online harms, as one would imagine are online activities of a 'harmful' nature and when the repercussions of online activity bleeds into a person's personal life and privacy, causing adverse effects on society. An initial list of online harms has been created by the white paper based on an assessment of frequency and severity or impact on individuals and society. These harms have been split into three categories, harms with a clear definition, harms with a less clear definition and underage exposure to legal content. This is a table of online harms provided by the white paper[140]:

Harms with a clear definition	**Harms with a less clear definition**	**Underage exposure to legal content**
Child sexual exploitation and abuse	Cyberbullying and trolling	Children accessing pornography
Terrorist content and activity	Extremist content and activity	Children accessing inappropriate material (including under 13s using social media and under 18s using dating apps; excessive screen time)
Modern slavery	Coercive behaviour	

[136] ibid, 4.

[137] The Straits Times, 'Malaysian spy agency has over 1,000 personnel worldwide' (*The Straits Times*, 1 August 2018) <https://www.straitstimes.com/asia/se-asia/malaysian-spy-agency-has-over-1000-personnel-worldwide> accessed 12 July 2021.

[138] MalaysiaKini, 'Ex-spy chief's case dropped' (MalaysiaKini, 12 April 2021) <https://www.malaysiakini.com/newsletter/570480> accessed 3 October 2021.

[139] Department for Digital, Culture, Media & Sport, "Consultation Outcome: White Paper Online Harms." (*Gov.uk*, 15 December 2020) <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#fn:8> accessed 30 July 2021.

[140] Ibid.

Extreme pornography	Intimidation	
Harassment and cyberstalking	Disinformation	
Hate crime	Violent content	
Encouraging or assisting suicide	Advocacy of self-harm	
Incitement of violence	Promoting Female Genital Mutilation (FGM)	
Sale of illegal goods/services, such as drugs and weapons		
Content illegally uploaded from prisons		
Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18)		

Table: Categories of Online Harms

Further, the provided definition of online harms is behaviour online which may hurt physically or emotionally. It could be harmful information that is posted online or information that is sent to a person. Aside from the harms outlined above, online platform algorithms have been suggested as contributing to harmful activity as well. Algorithms may prevent a user from seeing alternative information on social media, may only show one side of an argument and generally create a barrier from the user being able to access accurate and accredited information. [141]

Illegal activity that can constitute 'online harms' in Malaysia include: online defamation, sedition, posting child pornography, cyber-stalking, content uploading without permission, 'fraping' (hijacking a person's Facebook account and changing their status), and posting corporate secrets online.[142] To illustrate the legal aspects of an 'online harm', three elements have to be proved for online defamation to be established in Malaysia: defamatory words, the statement refers to a person being defamed and it is published by a third party. *Section 114A of the Evidence Act 1950* inserts an evidentiary presumption on people who are presumed to have published a defamatory statement unless the contrary is proved: any person whose name, photo or pseudonym appears on the publication showing himself as the owner, editor or someone who facilitated the publishing; a person subscribing to the network service; or someone who controls the computer from which the publication originates. The High Court in the *Kopitiam* case held that it is empowered to direct the administrators of the website (as persons holding relevant data) to disclose data to the alleged victim of defamation in order to fairly dispose of his defamatory action against an article posted in that website.[143]

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?

Online platforms generally have their own codes of conduct known as private codes of conduct. Malaysian legislation does not specifically outline legal standards of online social media platforms. However, there are regulations with online shopping platforms or e-commerce. Online businesses are all required to register with the Ministry of Domestic Trade and Consumer Affairs (MDTCA) and when foreign participation

[141] Ibid.

[142] Hariati Azizan, 'Are you guilty of cyber crime?' (*Malaysian Bar*, 29 January 2012) <https://www.malaysianbar.org.my/article/news/legal-and-general-news/legal-news/are-you-guilty-of-cyber-crime> accessed 2 August 2021.

[143] *Kopitiam Asia Pacific Sdn Bhd v Modern Outlook Sdn Bhd & Ors* [2019] 10 MLJ 243.

is involved, the domestic trade division of the MDTCA must be engaged. Additionally, legislation governing e-commerce in Malaysia include: the *Electronic Commerce Act 2006; Consumer Protection Act 1999; Consumer Protection Regulations 2012; Contracts Act 1950; and Sale of Goods Act 1957*. E-commerce online platforms will also be subject to legislation relating to online activity as well. [144]

With regard to regulation of online social network platforms, the EU has the most comprehensive approach for tackling illegal content online.[145] The majority of online platforms have their own individual terms of service or use and community standards or guidelines. These do not necessarily reflect a legal system however there tends to be overlap between the two. These codes of conduct provided by individual online platforms often aim to remove vulgar content and keep their platforms accountable. The common ways to achieve this include: the flagging of content through a peer reporting system, algorithmic filters regulating content and cancelling the act of posting certain words, and other AI machine-learning models. However, AI and digital measures taken by online platforms are not sufficient at regulating content and it is almost inevitable that pre- and post-human moderation is necessary in order to properly ensure accuracy. The *Malaysiakini* case illustrates the failure of AI to capture comments which were contemptuous to the administration of justice.[146]

The majority of online platforms that were interviewed by the EU policy department reported using mechanisms based on flagging tools whilst only one mentioned using an email alias as a direct reporting channel for users. Different flagging tools include a dedicated button or link on the platform, a simple flagging tool that appears next to the content and a dedicated on-platform support inbox that can be used to share information about the status of the report. Categories for flagging content usually include nudity or sexual content, hate speech, threatening or violent content and/or bullying. Users can select which category they believe the content violates.[147]

Common problems that are faced by online platforms in keeping the platform accountable include that there are often unsubstantiated or unreliable claims made by users. In this case, content cannot be removed or regulated until or if further information is not provided to the regulators. When the content is found to be incompatible with community guidelines it will be taken down and in countries such as Germany, if the content is found to be incompatible with local laws then it will be flagged and unavailable in the country and taken down to be published in the platform's transparency report. Many NGOs, industries and hotlines reporting illegal content often state that the measures taken by online platforms in regulating their content is not sufficiently effective. Mechanisms providing a flagging or 'notice-and-takedown' system are not always user-friendly and this can create problems and inefficiencies.

The EU's solutions and suggestions on creating guidelines and moderating their content involves creating a harmonised and transparent 'notice-and action' process that is also user-friendly and accessible. Networks of fact-checkers and hotlines across the EU should also be strengthened. In terms of fundamental rights, private codes of conduct should consistently interpret their regulations with surrounding rules, for example, in the EU private codes of conduct should be assimilated to be compatible with existing EU regulations.

Given the amount of online content, public authorities should be properly equipped to ensure the effectiveness of content moderation and they may need to be complemented by private bodies that are charged with regulating content and enforcing the private community guidelines. Additionally, more inclusive legislation should be created relating to regulating content and a clear codified framework for obligations and liabilities should be created to guide online platforms in their regulation. Currently, legislation mainly distributes the responsibility of online platform accountability solely onto the platforms themselves, and so platforms can benefit from a codified and accessible legislative framework.[148]

To summarise, online community guidelines should be drafted in such a way which accords with national laws, and if applicable, supranational standards. Online platforms should be held accountable to the extent their functional capacity allows. Public authorities should cooperate with online intermediaries to form a codified and accessible legislative framework that governs intermediary liability to maintain a proper check-

[144] Shazana Abdul Hapiz, 'Legal Aspects Of E-Commerce In Malaysia' (*Conventus Law*, 26 August 2020) <https://www.conventuslaw.com/report/legal-aspects-of-e-commerce-in-malaysia/> Accessed 26 July 2021.

[145] Alexandre de Streel et al, *Online Platforms' Moderation of Illegal Content Online: Law Practices and Options for Reform* (European Parliament, 2020).

[146] See the *Malaysiakini* case in Part D, Question 8.

[147] de Streel (n 145).

[148] Ibid.

and-balance. Finally, online fact-checkers and hotlines should be used as alternative mechanisms to help maintain the standards of online behaviour.

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

From the so-called 'early days of the Internet', developed nations believed intermediaries should be free from governmental pressure and be allowed to self-govern themselves. However, as we know it, this led to its rampant abuse. It is argued that online platforms should not be completely immune from liability for third-party content in certain situations. One of the main challenges in the digital sphere is the violation of intellectual property rights (IPR). Copyright holders increasingly hold intermediaries liable for copyright infringements committed by their subscribers in order to prevent infringements and recover their economic losses.[149] In one of the first cases concerning an intermediary's liability for third-party copyright infringement, the District Court of Northern California held that even though the intermediary is not directly liable for the acts of its online users, it can be contributorily liable if the intermediary knew or should have known of the infringement. This liability was imposed because intermediaries are the 'gatekeepers' that are best placed to monitor the activities of online users and prevent copyright infringements.[150]

This situation continued until the enactment of *Digital Millennium Copyright Act 2000* and the *E-commerce Directive*, which created 'safe harbour' provisions for intermediaries. Basically, the law gives some level of immunity to intermediaries if they comply with a mandatory obligation to remove infringing content once they receive a notice from the copyright holders. Under the *E-commerce directive of the European Union*, an intermediary is not liable for third party infringements if the intermediary is providing a hosting service, facilitating data or is not provided sufficient notice of any wrongdoing.[151] However, the intermediary should terminate or prevent infringements when requested by the court or administrative authority in the respective member states. This is known as the 'notice and takedown' approach, which is also adopted in English laws concerning the liability of intermediaries for online copyright infringements. A seminal European case demonstrates an example of the limited immunity intermediaries are given in the context of copyright infringements. The court in *L'Oreal v Ebay* provides a test for intermediary liability: firstly, an intermediary needs to be made aware of a trademark infringement; secondly, a court will decide whether to grant an injunction if doing so would be proportionate as an effective remedy; thirdly, an injunction can be an effective remedy even if access to a website is merely made difficult instead of impossible.[152] This case provides website-blocking injunctions as a remedy for copyright holders.

In a complex UK Supreme Court case, *Cartier International AG v. British Telecommunications and Others*[153] concerned whether the internet service providers (ISPs) are liable to pay for the full costs of complying with the website-blocking order (to block access to websites and selling counterfeit copies of the goods and block links which enable access to those websites) sought by Cartier. Although generally copyright holders bear the costs of obtaining such orders and the ISPs bear the costs of implementing these orders, [154] judges considered the provisions and recitals of the *E-Commerce Directive* and held that the underlying rationale for an ISP's immunity from liability came from the fact that they have little or no control over the content they transmit or store since they are a "mere conduit".[155] Therefore, since these website-blocking injunctions were "wholly directed to the protection of the [copyright holder's] legal rights", and the "entire benefit… inures to the rights-holder", there is no reason why ISPs as a network provider (which is "abused by others") is not legally entitled to seek indemnifications from the copyright holders besides the infringers.[156] As a result, intermediaries enjoy limited immunity for copyright infringements under EU and English law, which duly reflects the general spirit of intermediary legal liability in Malaysia. Malaysian courts tend to use European jurisprudence as persuasive authority in their judgments in order to align with international legal standards.

[149] Ida Shafinaz bt Mohamed Kamil and Dr Ida Madieha bt Abdul Ghani Azmi, 'Gatekeepers Liability for Internet Intermediaries in Malaysia: Way Forward' (2020) 21 International Journal of Business, Economics and Law 23.

[150] *Religious Technology Center v. Netcom On-Line Communications Services, Inc*. (907 F. Supp. 1361 (N.D. Cal. 1995).

[151] Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1, arts 12-15 (E-Commerce directive).

[152] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* [2011] I-06011.

[153] [2018] UKSC 28.

[154] *Twentieth Century Fox Film Corporation v British Telecommunications Plc* [2011] EWHC 2714.

[155] *Cartier* (n 153), para 30.

[156] ibid, para 35.

Under Malaysian law, an intermediary service provider is not liable for transmitting, caching and storing copyright infringing materials provided the intermediary does not initiate the acts, modify or select the content, has no "actual knowledge" or unaware "of the facts or circumstances from which the infringing activity is apparent", and does not receive any financial benefit "directly attributable to the infringement of the copyright".[157] Intermediaries are obliged to remove infringing content once the copyright holder notifies the service provider, and it will not be liable in removing such content in good faith.[158] These provisions bear a remarkable resemblance with the *E-Commerce Directive*. If the person knowingly makes a false notification of copyright infringement, he/she will be fined for a maximum of MYR 100,000 and/or imprisonment for a maximum term of five years, and liable to compensate for losses.[159]

Apart from the specific provisions targeted at copyright infringements above, Malaysia also has other laws and guidelines of broader scope applying to all illegal content. For example, *Section 263 of the Malaysian Communications and Multimedia Act 1998* states "a licensee shall use his best endeavour to prevent the network facilities that he owns or provides... from being used in, or in relation to, the commission of any offence under any law of Malaysia". The *Communications and Multimedia Content Code*, which is a set of industry guidelines, also recommends intermediaries to block a subscriber's access to 'Online prohibited Content', to remove such content from its platform, and to not knowingly provide access to such content.[160] Although the list of 'Online prohibited Content' does not explicitly refer to copyright infringements, Malaysian scholars argued that its definition is wide enough to cover all illegal content including copyright infringements.[161] Other than these obligations, an intermediary service provider is not obliged to actively monitor its website or domains for infringing content due to the concept of 'Innocent Carrier'. This means all intermediaries which have no control or knowledge over infringing content are deemed as an innocent carrier, which is not held responsible for any infringements.[162] From the above observations, it is clear that Malaysian law does not hold online intermediaries liable for third-party content which infringes copyright unless it is established that they have 'control' and 'knowledge' of those illegal materials. This approach differs from the EU and English approach, which is more centred on the interpretation of the provisions in the *E-Commerce Directive*.

In common law jurisdictions, intermediaries can be held liable for third-party defamatory content. For example, in *Tamiz v. Google*,[163] the case before the English Court of Appeal concerned whether Google, as the online intermediary, is entitled to an 'unassailable defence' provided in *Section 1(1) of the English Defamation Act 1996* — this defence is given to a person who is not the author, editor, or publisher of the content, has taken reasonable care in the publication and does not know or reasonably should have known that the statement is defamatory. The English Court of Appeal ruled that Google lost this defence because a reasonable time has elapsed between the time of notification of the defamatory content and the eventual takedown.[164] Holding intermediaries liable for third-party defamatory or contemptuous comments became the central issue in the *MalaysiaKini* case, when an intermediary was held liable for the failure to remove a contemptuous comment against the administration of justice.[165] This case is discussed in further detail in Part D, Question 8. Interestingly, the judge in the *MalaysiaKini* case referred to European jurisprudence (*Delfi AS v Estonia*) as guidance in deciding the case before them.

Intermediaries often argue against liability for third-party, user-generated content because it is virtually impossible to monitor every content posted by online users due to the sheer traffic its platform gets on a daily basis. It is argued that online platforms should not be completely immune from liability from third-party content provided certain exceptions are met. These exceptions should be either listed clearly in legislation or developed on a case-by-case basis with clear ambits.

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

User-generated content falls within the right to freedom of expression, which is guaranteed by *Article 10 of the Federal Constitution of Malaysia*. A three-step test exists in international law to justify derogations on

[157] Malaysia Copyright Act 1987 (amended by the Copyright (Amendment) Act 2012), s43C-E.

[158] ibid, s43H(1) and s43F(1).

[159] ibid, s43I(1).

[160] Malaysian Communications and Multimedia Content Code, Part 5, paras 7.1-10.2.

[161] Kamil and Azmi (n 149), 29.

[162] Content Code, Part 5, para 2.1.

[163] [2013] EWCA Civ 68.

[164] See 'Tamiz v Google Inc' (*5RB Barristers*) <https://www.5rb.com/case/tamiz-v-google-inc-ca/> accessed 12 August 2021.

[165] See Part D, Question 8.

free expression.[166] This test follows the principles of *Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR)*. Firstly, derogations must be provided under law. Secondly, the purpose of any derogation has to protect civil liberties and human rights. Derogation is allowed for the purposes of safeguarding national security, public order, and public health and morals. Thirdly, any derogation must be justified as proportionate and necessary.

The *Communications and Multimedia Act 1998* is relevant for the functioning of intermediaries in Malaysia. According to *Section 211 of this Act*, "No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person".[167] A violation of *Section 211* can result in imprisonment for one year and a fine ranging up to MYR 50,000.[168]

In line with the need for a content code outlined in *Section 213 of the Communications and Multimedia Act 1998*, the *Malaysian Communications and Multimedia Content Code* was adopted as a set of industry guidelines for intermediaries. The code prohibits indecent content defined as nudity and sex and obscene content defined as pornography. The code demands careful editorial judgment over the portrayal of any violence. The code prohibits "hate propaganda, which advocates or promotes genocide or hatred against an identifiable group".[169] The code includes hate speech in its definition of "bad language", stating "hate speech refers to any portrayal (words, speech or pictures, etc.), which denigrates, defames, or otherwise devalues a person or group on the basis of race, ethnicity, religion, nationality, gender, sexual orientation, or disability and is prohibited. In particular: descriptions of any of these groups or their members involving the use of strong language, crude language, explicit sexual references or obscene gestures, are considered hate speech".[170] One provision of the code promotes family values.[171] While false content is prohibited, an exception is explicitly provided for satire and cultural fiction.[172]

Malaysia has a history of racial disturbances. The code prohibits the spread of "false information with regards to outbreak of racial disturbances in a specific part of the country".[173] For policing and counter-terrorism purposes, the code prohibits "making available instructions and guidance on bomb-making, illegal drug production or counterfeit products".[174]

The code is ambiguous in some of its provisions. For example, prohibiting the circulation of "information with regards to the outbreak of a deadly or contagious diseases"[175] appears detrimental to the public interest. The Covid-19 pandemic has proven the role that intermediaries play in facilitating public awareness during a health emergency.

Refugees and undocumented migrants have been the target of online hate speech in Malaysia. Parliamentary discussions have called on the government to introduce a stronger hate speech law in response to xenophobia against refugees and migrants in digital media.[176] Malaysia is not a state party of the *Convention on the Elimination of All Forms of Racial Discrimination (CERD)*. The principles of *CERD* are part of customary international law. The *CERD* requires a condemnation of xenophobic propaganda. Therefore, any xenophobic propaganda may readily fall within the parameters of problematic user-generated content.

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

The term 'fake news' was popularised by former US President Donald Trump, yet the concept has existed for centuries. Fake news refers to when misinformation is published as though it is fact. In the now repealed *Anti-Fake News Act 2018*, the Malaysian Government defined fake news as "any news, information, data and reports, which is or are wholly or partly false…".[177] The term is often used in a political context to

[166] 'Briefing Paper: Blasphemy Provisions In Malaysian Law' (*Article19.org*, 2021) <https://www.article19.org/wp-content/uploads/2021/01/2021.01.20-Malaysia-blasphemy-briefing-paper-final.pdf> accessed 12 August 2021.
[167] Communications and Multimedia Act s211 (1).
[168] Ibid s211 (2).
[169] The Malaysian Communications and Multimedia Code Part 2 (5.2).
[170] Ibid Part 2 (6.0) (iii).
[171] Ibid Part 2 (9.0).
[172] Ibid Part 2 (7.3).
[173] Ibid Part 2 (5.3) (ii).
[174] Ibid Part 2 (5.3) (i).
[175] Ibid Part 2 (5.3) (iv),
[176] Reuters Staff, 'Malaysian Lawmaker Calls For Hate Speech Law After Reuters' Rohingya Report' (*U.S.*, 2021) <https://www.reuters.com/article/uk-facebook-malaysia-rohingya-idUKKBN2840N0> accessed 12 August 2021.
[177] Anti-Fake News Act 2018, s2.

refer to information which damages the reputation of individuals or information which can impact voter activity. The term can also refer to conspiracy-related propaganda such as the spread of misinformation pertaining to COVID-19.

In response, the online platform Instagram has published their *COVID-19 and Vaccine Policy Updates and Protections* which outline community guidelines in order to remove content that "contributes to the risk of real-world harm" including "misinformation that contributes to the risk of imminent violence or physical harm."[178] Under the policy, this content will be removed. Examples of misinformation provided in the policy include "claims that no one has died from COVID-19, claims that the mortality rate of COVID-19 is the same or lower than the seasonal influenza, claims that getting a flu shot or flu vaccine is more likely to kill you than COVID-19" and "claims that the number of COVID-19 caused deaths are much lower than the official figure". Instagram have also introduced "information labels" that appear on content that contains any reference to the pandemic. These labels, which users can click on, direct individuals to verified information provided by health experts like those from the World Health Organisation.[179]

The *Anti-Fake News Act 2018* made it an offence in Malaysia to "maliciously" create, circulate or disseminate fake news. Indeed, anyone found to have committed such an offence would have faced up to six years in prison as well as facing a fine of up to five hundred ringgit.[180] The act sought to address the dissemination of false information without relying on online platforms to moderate such content themselves. Online platforms as distributors, circulators and disseminators of fake news could have been found in breach of the act when proven that they did so "maliciously." *Section 7* also provided orders for the removal of publications containing fake news.[181] After public dissent and the accession of a new political party, the act has since been repealed by the *Anti-Fake News (Repeal) Bill 2019* on 9 October 2019 which included an explanatory statement citing a change in government policy as why the act was being repealed and that fake news was already dealt with under existing legislation.[182] Despite this, in March 2021 the Malaysian government enacted the *Emergency (Essential Powers) (No. 2) Ordinance 2021* which again criminalises the sharing of fake news in relation to the COVID-19 pandemic.[183] The ordinance was enacted without parliamentary approval as parliament has been suspended due to the COVID-19 state of emergency declared in Malaysia. At the time of writing, this emergency ordinance has been revoked after the end of the state-declared emergency on 1 August 2021.

The benefits of moderating fake news on online platforms are clear. The spread of misinformation can severely impact an individual's engagement in politics and can impact their health choices (such as choosing to avoid getting a COVID-19 vaccination) to name two outcomes. On the reverse side, Richard Priday highlights the detrimental effects of moderating fake news on online platforms: "with the potential ability to imprison, bankrupt or put journalists out of business for publishing poorly defined misinformation, there is enormous scope for abuse, of which the worst case scenario would be outright government censorship, impinging on human rights and making people's lives worse." Indeed, Priday quotes Oxford Internet Institute researcher, Yin Yin Lu who affirms that "not reporting something is as dangerous as reporting something that is false."[184] Indeed, whilst the legislation enacted by the Malaysian government to moderate fake news may be beneficial to many citizens, some spectators like the organisation Article 19, assert that legislation like this severely threatens freedom of speech. In relation to the *Anti-Fake News Act 2018* in Malaysia, Human Rights Watch criticised the act as one which primarily operated to stifle dissent against public bodies instead of operating with the primary goal of tackling harmful misinformation.[185] Even Malaysian academics remained dubious as to whether the powers of the emergency ordinance would be used disproportionately to silence

---

[178] 'COVID-19 and Vaccine Policy Updates Updates and Protections' (*help.instagram.com*) <https://help.instagram.com/697825587576762> accessed 11 August 2021.

[179] 'Helping People Stay Safe and Informed about COVID-19 Vaccines' (*about.instagram.com*, 16 March 2021) <https://about.instagram.com/blog/announcements/continuing-to-keep-people-safe-and-informed-about-covid-19> accessed 11 August 2021.

[180] Ibid, s4.

[181] Ibid, s7.

[182] Anti-Fake News (Repeal) Bill 2019.

[183] Emergency (Essential Powers) (No.2) Ordinance 2021.

[184] Richard Priday, 'Fake news laws are threatening free speech on a global scale' (*WIRED*, 5 April 2018). <https://www.wired.co.uk/article/malaysia-fake-news-law-uk-india-free-speech> accessed 11 August 2021.

[185] Rozanna Latiff, 'Malaysia parliament scraps law penalizing fake news' (*Reuters*, 9 October 2019) <https://www.reuters.com/article/us-malaysia-politics-fakenews-idUSKBN1WO1H6> accessed 11 August 2021.

debates and criticisms against the government as its 2018 predecessor, beyond its legitimate purpose to control emerging fake news regarding the Covid-19 situation in Malaysia.[186]

Therefore, the practices put in place by online platforms and by the Malaysian Government to moderate fake news can be beneficial but a balance must be struck between the right of citizens to freedom of speech, expression and publication.

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 are laws which state that a person or entity is not held liable provided certain conditions are met.[187] In the context of online intermediaries, examples of 'safe harbour provisions' can be found in *Articles 12-15 of the E-Commerce Directive*. These provisions state all intermediary service providers are not liable for illegal information that is transmitted, cached, stored or hosted unless they initiated the transmission, selected or modified the content and have actual knowledge of the illegal activity. Finally, *Article 15* prevents a general obligation on intermediaries to monitor third-party content provided they remove the illegal content once notified.

However, intermediaries often face a challenge in upholding digital governance while at the same time ensuring the rights of users. In Wikimedia Commons, the importance of intellectual property means that uploads can be swiftly deleted if there is suspicion about its copyright status. Facebook requires that violations of intellectual property be reported in order for content to be removed. Reporting violations contrasts with a general obligation to unilaterally take action regarding third party content. User reports of violations should be subjected to adequate review and actions taken should be proportionate and necessary so that decisions of content removal are not made arbitrarily to the extent that freedom of speech is curtailed unreasonably.

The granting of safe harbours can either facilitate the exercise of fundamental rights or curtail them. For example, providing safe harbours is crucial to the provision of freedom of speech. If online platforms are held liable to all content posted by users and face legal consequences for such content, online platforms may not continue to provide platforms for all to continue to facilitate freedom of expression without interference. Indeed, many jurisdictions such as Malaysia, provide for "notice and takedown procedures" that work as automatic censures of user content.[188] In Malaysia, the rules regarding safe-harbour protections for online platforms in relation to copyright infringing third-party content are contained in the *Malaysian Copyright (Amendment) Act 2012*. Internet intermediaries will not be liable for copyright infringement provided they meet the conditions of the safe harbour provisions in *Sections 43C-43I of the Act*.[189]

Despite this, in 2020, criminal proceedings were brought against the website Malaysiakini for comments made by third parties.[190] The Court found that Malaysiakini was the publisher of the content posted by readers despite not having knowledge of the content posted.[191] Council for Malaysiakini cited *Section 3(3) of the Communications and Multimedia Act 1988* that the censure of the internet is not permitted by law.[192] In response, the court found that the rights of users to freedom of expression which is provided for in *Article 10 of the Federal Constitution*, must be interpreted in accordance with other existing legislations with the objective to monitor internet usage[193]. The minority judgement asserted that: "The repercussions of extending the law of contempt from actual knowledge to constructive knowledge is that there would be a chilling effect on

[186] Sani (n 25).

[187] 'What is a Safe Harbor?' (*Winston & Strawn LLP*) <https://www.winston.com/en/legal-glossary/safe-harbor.html> accessed 13 August 2021.

[188]Kamil and Azmi, 'Theory, 'Gatekeepers Liability for Internet Intermediaries in Malaysia: Way Forward' (2020) 21 International Journal of Business, Economics and Law 23, 28.

[189] Copyright (Amendment) Act 2010, s 43C-43I.

[190] *Peguam Negara Malaysia v Mkini Dotcom Sdn Bhd & Another* (Case No.08(L)-4-06/2020). See Udbhav Tiwari, 'Criminal proceedings against Malaysiakini will harm free expression in Malaysia' (*Mozilla*, 8 July 2020) <https://blog.mozilla.org/netpolicy/2020/07/08/criminal-proceedings-against-malaysiakini-will-harm-free-expression-in-malaysia/> accessed 13 August 2021.

[191] Christopher Ong & Lee Ong, 'The Malaysiakini Case: Liability of Online Intermediary Platforms as the Presumed Publisher for Third-Party Content - A further Analysis' (*Lexology*, 16 March 2021) <https://www.lexology.com/library/detail.aspx?g=35e86231-1660-45a4-a54c-343544d898e4> accessed 13 August 2021.

[192] Communications and Multimedia Act 19998, Section 3(3).

[193] Christopher Ong & Lee Ong, 'The Malaysiakini Case: Liability of Online Intermediary Platforms as the Presumed Publisher for Third-Party Content - A further Analysis' (*Lexology*, 16 March 2021) <https://www.lexology.com/library/detail.aspx?g=35e86231-1660-45a4-a54c-343544d898e4> accessed 13 August 2021.

freedom of expression in the media in that even articles or statements expressing valid criticism may be excised or precluded from being published online. There is a grave likelihood that user comments would simply be disabled. That would be detrimental and anathema to *Article 10 of the Federal Constitution*."[194] The proceedings resulted in the website having to pay MYR500,000.[195] Accordingly, whilst safe-harbour provisions protect intermediaries from harm, the Malaysian judiciary is free to limit the operation of safe harbours in exceptional circumstances. The limitation of safe-harbour provisions can be detrimental especially when intermediaries choose to censor themselves and their subscribers in fear of legal repercussions.

However, the *MalaysiaKini* case has to be assessed in light of the Malaysian context. Aside from the *Personal Data Protection Act 2010*, there is little legislation in Malaysia concerning the right to privacy. The *Federal Constitution of Malaysia* does not enshrine the right to privacy. Under *Article 10(2) of the constitution*, the right to freedom of speech, expression, assembly and association is subjected to restrictions deemed "necessary or expedient" in the interests of public order, morality and the security of the Federation.[196] The rights to freedom of expression and privacy are civil and political rights which are given less emphasis in Malaysia as a developing country, focusing on Asian values of togetherness and racial harmony.

On another side of the spectrum, granting safe-harbour protections may come at the cost of the fundamental right of citizens to privacy by enabling intermediaries to gain access to users' private information. In Malaysia, police officers can gain access to classified data stored in a computer for police investigation purposes (*Section 116B*, *Criminal Procedure Code*) and intercept communications to find evidence for terrorism and corruption with the Public Prosecutor's authorisation (*Section 116C of the Criminal Procedure Code*; *Section 6*, *Security Offences (Special Measures) Act 2012*; *Section 43*, *Malaysian Anti-Corruption Commission Act 2009*). Imagine there is a suspected group of terrorists organising their activities using WhatsApp, and the Malaysian Public Prosecutor has requested for WhatsApp's cooperation in decrypting the messages (which are protected with end-to-end encryption) to which WhatsApp quickly agreed. However, at the end of the day, the messages had nothing to do with terrorist activity but merely a group of teenagers pranking each other. In this case, WhatsApp can be granted a safe harbour because it cooperated with the official investigation of the Malaysian police. But this safe harbour comes at the cost of those teenagers' rights to privacy and family life.

The question here is: how should safe-harbours protecting and enabling intermediaries to cooperate with governments in grave situations of public disorder and the privacy of users be balanced? It is argued that in such cases, the burden should be on the intermediary to first prove they have received sufficient information from the relevant department and official authorisation from the governmental authority before agreeing to cooperate. If the intermediary has proven this to be the case, the burden should shift to the police and/or governmental authority that their decision to infringe user privacy is proportionate and necessary. Taking a step back, currently in Malaysia there are no active safe-harbour provisions that come at the cost of fundamental rights. But this is a rather important question to ponder upon if it became necessary to provide safe harbours that infringe fundamental rights.

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?

From the Malaysian experience, without a legal impetus, the global intermediary ecosystem would not have shifted from a 'post-hoc' lens to a proactive approach in understanding and regulating technology. On 19 February 2021, a case concerning the liability of online intermediaries reached the Federal Court of Malaysia.[197] After the outcome of this decision, online intermediaries must be more proactive in regulating their respective online services to avoid legal liability.

In that case, Malaysiakini.com published two articles on 9 June 2020: the first one concerned the acquittal of a notorious minister who had 46 charges of corruption and money laundering, and the second one stating the Chief Justice announced for all courts to be fully operational from 1 July 2020. Many anonymous third-party users posted contemptuous comments against the judiciary for acquitting the notorious minister. One week later, the Honourable Attorney-General of Malaysia commenced actions against Malaysiakini for publishing the comments. To establish the case, the AG invoked *Section 114A of the Evidence Act (EA) 1950*:

[194] *Peguam Negara Malaysia v Mkini Dotcom Sdn Bhd & Another* (Case No.08(L)-4-06/2020) [120].

[195] Annabelle Lee, 'Lawyers: Decision in Mkini case may curtail other news sites, social media' (*Malaysiakini*, 19 February 2021) <https://www.malaysiakini.com/news/563597> accessed 13 August 2021.

[196] Federal Constitution of Malaysia art 10 (2) (a) (b) (c).

[197] *Peguam* (n 44).

Malaysiakini shall be deemed as the publisher of the comments because (1) Malaysiakini depicted itself as the host of the comments, and (2) Malaysiakini facilitated the publication.

Malaysiakini argued that it had no knowledge of the comments before being notified by the police. The terms and conditions contained in its website warned users that any abusive or illegal posts will be banned. Malaysiakini has a filter program which bans the publication of certain words and flags suspicious words for further review by a comments administrator. It also relies on its peer reporting system, allowing other users to report offensive comments. It is impossible for the service provider to moderate comments before they are uploaded or to monitor every comment that is published due to the sheer load of traffic. Malaysiakini argues that it is protected from liability as long as it flags and takes down certain content as prescribed in the *Malaysian Communications and Multimedia Content Code ('Content Code') (Section 98(2) of the CMA)*. From these arguments, it is clear that Malaysiakini adopts a post-hoc approach in regulating the behaviours of its online users, only doing the bare minimum required in law.

In face of these arguments, the court sought to "protect the Judiciary as the third arm of government rather than individual judges".[198] Establishing the liability of online media publication is not as straightforward as traditional newspaper publications because online publications are posted directly on the media platform "without the usual editing process".[199] After discussing foreign approaches on the issue of online posting and contempt of court, the court found that a "degree of awareness is sufficient to establish the mens rea element" ((24)-(31)). Eventually, the court relied on *Section 114A* to hold Malaysiakini accountable — according to the Hansard of the Dewan Rakyat on 18 April 2012, the objective of this provision is to "tackle the issue of internet anonymity".

The court held Malaysiakini had constructive knowledge of those publications. Constructive knowledge is "deduced or inferred from the circumstances surrounding each particular event", considering in particular: (a) opportunities to obtain the knowledge and (b) whether there are any obstacles to the person acquiring that knowledge ((65), (71)). Even though Malaysiakini, as the intermediary, enjoys great traffic to its website, they "must assume responsibility for taking the risk of facilitating a platform for such purpose" and that the heavy volume of traffic is not a credible basis to claim lack of knowledge or escape from its legal responsibility as the facilitator ((77)).

Malaysiakini also cannot rely on its disclaimer to avoid legal responsibility for the offensive comments, which were simply insults, beyond "justified criticism".[200] The court cited an ECtHR case, which was materially similar to Malaysiakini's case. This concerned Delfi, one of the largest internet news portals in Estonia, which allowed readers to post personal threats against a person (L).[201] The comments were only taken down after six weeks after a request by L's lawyers. Delfi filed a complaint to ECtHR, asserting their freedom of expression (right to impart information) has been infringed. In that case, the ECtHR held the right to freedom of expression does not protect comments which were "vulgar, humiliating and defamatory and had impaired, the dignity of L's honour and reputation". Since Delfi chose to not exercise prior control over comments posted on its platform, it should have created some effective system to ensure the speedy removal of such comments. The measures taken by Delfi were insufficient and "contrary to the principle of good faith to place the burden of monitoring comments on potential victim". Owing to the fact that both Delfi and Malaysiakini have "substantial degree of control over readers' comments and it had been in the position to predict the nature of the comments", they are held liable.

To conclude, it is essential to reconsider the role online intermediaries play in providing a platform for the exercise of the right of freedom of expression, as well as regulating the abusive use of this platform to commit hate speech, contempt of court, and other internet crimes protected by anonymity. From the perspective of Malaysia, legal repercussions are the main driving force encouraging online intermediaries to shift from a post-hoc to proactive approach in 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?

Whether the guidelines and policies of online platforms account for the errors of its algorithm and human content moderators differ according to the intermediaries. For example, the guidelines of

[198] *Zainur Zakaria v Public Prosecutor* [2001] 3 MLJ 604.

[199] *Peguam* (n 44), [23].

[200] For the online comments, see the majority judgment. One of the comments even scolded the court if they are afraid of 'Allah' by letting the notorious minister go.

[201] *Delfi AS v Estonia* (Application No. 64569/09) (2015) (ECtHR).

Malaysiakini.com do not account for the fallibility of their algorithm and human content moderators when it comes to certain comments without vulgar language, due to the massive incoming daily traffic the website gets. In comparison, Facebook has its own oversight board which oversees all policies and decisions Facebook makes in removing certain content, holding it accountable for the fallibility of its algorithm and human content moderators.[202]

Algorithm and human content moderators are insufficient to maintain the social cohesion of an online community. Most online intermediaries use algorithmic moderation systems to remove content which may be hateful and vulgar. For example, Malaysiakini.com uses a filter program which bans the use of certain vulgar words — any article or comment failing the filter will not be posted. Algorithmic moderation systems increase the opacity of decision-making, which essentially reduces an online intermediary's accountability because such practices are difficult to understand and regulate. Such algorithmic moderation systems make fundamentally political decisions on content moderation and its opacity makes the fairness and justice of decision-making obscure.[203]

Considering the case study of Malaysiakini, it failed to take down contemptuous comments against the courts and faced legal repercussions. However, even after the court case, there seems to be no obvious changes or additions onto the terms of service.[204] If users felt there was an error in rejecting the comment, they can write an email to the editors of Malaysiakini.com. This shows the lack of accountability within the community guidelines of the website, which therefore justifies the imposition of legal accountability by the court.

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?

Community guidelines should act as the first line of defence against internet crimes. If there is a conflict between community guidelines, public policy and international human rights, the primary focus should be on domestic public policy. This is because Malaysia brands itself as a nation which focuses more on Internet sovereignty than Internet freedom. In simpler words, domestic public policy that maintains racial harmony and public order will take precedence over online freedom and liberties. This theme is prevalent in a country which follows Asian values, which is illustrated by the essence of the Malaysian constitution and judicial will (no rights can be absolute).

What is the role of community guidelines? Community guidelines act as a code of conduct and are often binding contracts for online users. Hence, it should respect national policies and socio-cultural differences that mandate the blocking and filtering of certain user content. However, an intermediary cannot escape legal responsibility for the acts of third parties on its website after implementing its community guidelines as a post-hoc, harm-prevention tool. They must be proactive in regulating the use of technology and stay cognizant of certain anti-social behaviours online.

Nations have different perspectives on how the terrain of conflict between community policies, national interests and international human rights should be resolved. There are two main competing schools of thought: internet freedom and internet sovereignty. Internet freedom essentially focuses on internet access as a fundamental tool to exercise individual rights. Proponents tend to legitimise this agenda by relying on universal human rights and the "alleged inherent values of internet technology, such as openness and globality". On the contrary, internet sovereignty focuses on "information protection, cultural autonomy and national security". It is important to note that internet freedom and internet sovereignty exist on the same spectrum — different nations promote different internet policies, placing a focus on either agenda, more often as "an attempt to relate to their people and to the world". In this manner, nations market their own agenda for internet governance, "seeking the support of other nations, international organisations and users while delegitimising competing visions". This practice is known as "nation branding".[205]

As discussed before, Malaysia is a nation which focuses more on internet sovereignty than on internet freedom. A good illustration is the way freedom of expression is viewed (online and offline). The right of

[202] For more information, see the bylaws of the oversight board.

[203] Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance' (2020) 1 Big Data & Society 1.

[204] For more information, see Malaysiakini, 'Terms of Service' (Malaysiakini) <https://about.malaysiakini.com/terms-of-service/> accessed 28 June 2021.

[205] Melissa Aronczyk and Stanislav Budnitsky, 'Nation Branding and Internet Governance: Framing Debates over Freedom and Sovereignty' in Uta Kohl (eds), *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance* (CUP 2017), 63.

freedom of expression is contained in *Article 10 of the Malaysian constitution*. However, the exercise of this right is subject to parliamentary restrictions that are necessary to protect the interests of national security, racial harmony and public order. Therefore, any speakers of controversial speech against the core tenets of the Malaysian constitution are to be punished, such as: "the special rights of Malays and other indigenous people (bumiputera), Islam as national religion, the rights of immigrant races (especially Chinese and Indians) to citizenship, the position of the King, and the status of the Malay language as the national language and a host of other issues that could potentially be sensitive in the context of the fragile race relations in the country."[206] This legal position is also supported by the judiciary: "one cannot insist on freedom of speech which transgresses on the rights of others in society".[207] From a religious perspective, the exercise of freedom of speech online and offline must be limited to "sustain and preserve the sanctity of Islam", and it must not violate the Quran and al-Hadith or oppress the rights of others.[208] Islamic scholars place strict conditions on individuals who write, voice or publish their opinions on Islamic law (mujtahid), primarily to prevent views which are incoherent with the teachings of Islam. Only the mufti and other authorised persons bear the responsibility of explaining and interpreting such religious matters.

Therefore, considering user-generated content, community guidelines and policies are the first line of defence against hate speech and other forms of internet crimes. If there is a conflict between international human rights (freedom of speech) and national policy concerns (public order and political stability), national interests shall come first. Sacrificing freedom of speech for the sake of national security has always been a slippery slope: "the perceived need of a strong government that is able to deal with the competing demands of an ethnically diverse society may be seen as undemocratic and denying people their legitimate rights". Hence, to conclude, there should be effective mechanisms to balance the exercise of freedom of speech with the need to protect national security.[209]

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?

All advertisement policies and sponsored content of online platforms in Malaysia should respect its multiculturalism and promote racial harmony. National agencies should frame these policies and the final arbiter shall engage in an open and transparent decision-making process.

Advertisement is defined as "an announcement of a public nature whether for the sale or purchase or provision of goods or services or constituting of an invitation to participate in an activity and conveyed by or through any signage, image or sound disseminated through electronic medium for advertising purposes".[210] Since advertising is a huge industry, Malaysia has enacted certain laws and practice codes to govern such activities. However, there is no specific legislation codifying all laws on advertising.

The Advertising Standards Authority ('ASA') is the Malaysian national agency regulating advertisements. All advertising and sponsored content in Malaysia should adhere to the *Malaysian Communications and Multimedia Content Code* and the *Malaysian Code of Advertising Practice*. As a general standard, all advertisements must be "legal, decent, honest and truthful", complying with the *General Principles of Malaysia (Rukun Negara)*, and it must not identify any racial group or gender, traditional values and backgrounds.[211] Most importantly, advertisements cannot contain statements which "offend the religious, political, sentimental or racial susceptibilities of any community".[212] For example: there was a banned Raya (Eid) advertisement featuring a wombat, which was mistakenly perceived as a pig, and hence an "unclean

[206] Mohd Azizuddin Mohd Sani, 'Freedom of Speech and Democracy in Malaysia' (2008) 16 Asian Journal of Political Science 85, 86

[207] *Peguam* (n 44), [37].

[208] Wan Mohd Khairul Firdaus Wan Khairuldin, Abdul Hanis Embong, Wan Nur Izzati Wan Nor Anas, Daud Ismail, Ibtisam Ibrahim, Nurfaizah Fauzi, 'Freedom of Speech: A Comparative Study between Islam and Malaysian Laws' (2017) 7 International Journal of Academic Research in Business and Social Sciences 908, 912.

[209] Mohd Azizuddin Mohd Sani, 'Balancing Freedom of Speech and National Security in Malaysia' (2013) 5 Asian Politics and Policy 585, 604.

[210] Farhanin Abdullah Asuhaimi, Nur Amani Pauzai, Mohd Lotpi Yusob and Khairun-Nisaa Asari, 'Rules on Advertisement in Malaysia' (2017) 35 World Applied Sciences Journal 1723.

[211] Malaysian Code of Advertising Practice, paras 1.1-1.3.

[212] ibid, para 15.2.

animal... spark[ing] public outrage". [213] However, the Code does not restrict the freedom of expression of opinions by "political parties, foreign governments, religious or charitable bodies or other organisations or individuals".[214]

Digital technology influences political advertising in two main ways. First, people tend to become overwhelmed by the vast amount of information available online and they may choose to trust a certain personal social media network to help them evaluate the accuracy and importance of certain news. This is known as the "trust filter effect", which can either persuade or dissuade a person's allegiance to a political party. Social media also offers an avenue for citizens and political leaders to connect, encouraging public responsiveness and accountability – the "civic engagement effect". Sometimes, seeing photos of friends who have voted tend to encourage the users to vote. This small but powerful encouragement is known as the "nudge effect".[215]

Second, digital technology has made political advertising more influential through micro-targeted advertising. This involves collecting huge amounts of data using social media platforms and the results from these data are used to target voters based on their preferences and location. Statistical analysts can use this vast amount of data to develop targeted adverts to persuade prospective people to vote across the nation.

Needlessly to say, online platforms have provided a powerful tool of propaganda never before imagined. However, who should regulate political advertising? Although the government can prevent political speech that spreads fake news, they have little authority over the regulation of political advertisements. There should be a clear and fair policy on election and political advertising. This can be done by setting up a committee of working groups with the consent of the Election Commission of Malaysia (Suruhanjaya Pilihan Raya, 'SPR'), and MCMC should act as the boundary manager. The drafting of the election advertising policy should also encompass views from all political parties. SPR is viewed by the public as a trusted election body. However, there is a need to reform laws to give this election body more autonomy over "its legislative authority, financial allocation, human resource system, and so on, so that it can have more freedom to conduct free and fair elections".[216]

To conclude, all advertisement policies should focus on the interests of a nation as a whole to ensure a fair and transparent decision-making process. Digital technology has influenced political advertising in many ways and this powerful tool must be regulated to prevent its misuse. Most importantly, the final arbiter shall make the maintenance of national stability and racial harmony as the crux of its policies.

[213] For more examples, see Joanne Kong, 'Advertising Compliance in Malaysia' (Wong Jin Nee & Teo) <https://www.wjnt-law.com/intro/advertising-compliance-in-malaysia/> accessed 14 July 2021.

[214] ibid, para 2.2.

[215] Steve Jarding, Steve Bouchard and Justin Hardley, 'Modern Political Advertising and Persuasion' in Christina Holtz-Bacha and Marion Just (eds), *Routledge Handbook of Political Advertising* (Routledge 2017).

[216] Muhammad Fathi Yusof, Mohd Al'Ikhsan Ghazali, Nurhidayu Rosli & Muhammad Sakirin Alias, 'Public Perception towards the Election Commission in Malaysia' (2015) 11 Asian Social Science 347, 356.

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