CHAPTER 4

Regulation of Technology

By Yeong Zee Kin[1]

A. INTRODUCTION

04.001 The regulation of technology is best understood by first recognising that this label is a misnomer. The law does not regulate technology in and of itself, but how technology is applied and supplied. Technology may be categorised into different layers. The fundamental bifurcation is between the infrastructure layer and the services layer. The law regulating technology generally follows this categorisation: telecommunications ("telecom") law regulates the infrastructure and carriage, while informational and online services are governed through content regulation. While an oversimplification, the "content *versus* carriage" paradigm is a helpful starting point.

04.002 Technology regulation needs to also be contextualised in the broader discussion of technology, media and telecom ("TMT") law. The study of TMT law covers two broad areas: laws that apply to how technology is applied and supplied (to which technology regulation belongs); and how technology is shaping the development of other (more established) areas of law, such as intellectual property, contract and financial regulation. While the other chapters in this book deal with the latter, this chapter focuses on the former.

1. Overview

04.003 This chapter provides a framework to understand the different laws and regulations that govern and regulate technology, along with

---

1 The author wishes to thank Royce Wee, Tan Sze Yao, Ng Song Yeong and Koh Li-Na for their helpful comments on earlier drafts of this chapter. The opinions and views expressed in this chapter are personal to the author and do not represent his employer.

the techniques and considerations for regulating this fast-evolving domain. We commence with the *regulation of infrastructure*, which deals with issues such as the allocation of and access to resources, whether in the form of access for the purpose of laying cables, or assignment of radio frequency spectrum or telephone numbers. The discussion of infrastructure regulations will also cover competition and access issues like interconnection and standards, so as to assure safety and interoperability of telecom networks and equipment.

04.004 Next, the discussion turns to *content regulation*, which is defined broadly to include the regulation of both *informational content* as well as the *online services*. Focus will be trained on the more horizontal regulations covering informational content, while a roadmap is provided to navigate the vertical regulations that apply to online services. The part on the *regulation of intermediaries* will attempt to chart the evolution that began with providing Internet intermediaries with protections, in the form of statutory immunities and safe harbour provisions, but which have lately expanded to include the imposition of obligations to block access to offending content and communicating corrections. As this is a fast-developing area, we will also discuss recent international and domestic developments in the regulation of intermediation services.

04.005 The chapter concludes with some remarks about *emerging regulatory issues and techniques*: (a) regulatory sandboxes and their role in supporting the pilots of emerging technologies; (b) issues around the flow of data across the domestic economy and across borders; and (c) regulatory convergence in the digital services market.

B. WHAT IS TECHNOLOGY REGULATION?

04.006 "Technology regulation" refers to the body of laws and regulations that apply to how technology is applied and supplied. Before proceeding further, we ought to commence with an appreciation of the role of regulation in policy-making. Policy-making typically commences with problem definition, followed by the generation of policy options and formulation of policy tools that achieve them.[2] Regulations are but one of several public policy tools that policy makers can rely on; other public policy tools include economic incentives, state enterprises and direct

2 This is, of course, an over-simplification as there are other important stages like setting objectives and identifying measurements for achieving them, and building support for the programme through consultation, engagement and communications: see generally Xun Wu *et al*, *Public Policy Primer: Managing the Policy Process* (Routledge, 2nd Ed, 2017) ch 3 ("Policy Formulation").

provision.[3] There are a number of recurring policy objectives – discerned through parliamentary speeches or self-evident from the regulations – that we will encounter in the remainder of this chapter: for example, (a) enabling technology adoption by addressing legal ambiguities;[4] (b) establishing technical standards to achieve interoperability, interconnection and equipment safety;[5] (c) addressing technology risks by establishing baseline standards;[6] (d) ensuring market access and efficiency through the promotion of competition;[7] (e) consumer protection;[8] (f) creating safe online spaces;[9] and (g) safeguarding the public interest.[10]

3 Apart from public tools, there are also private tools like market, family and voluntary organisations: Xun Wu *et al*, *Public Policy Primer: Managing the Policy Process* (Routledge, 2nd Ed, 2017) at pp 54–58. The form regulations take – at least from the perspectives of policy makers – may either be hard or soft. Hard regulations refer to those promulgated as a form of primary or subsidiary legislation, whereas soft regulations may take the form of voluntary codes of conduct or practices, guidelines, or accreditation or certification systems. The voluntary nature of these soft regulations means that enforcement is not through any licensing regime or law, but through private tools like market dynamics and consumer choice.

4 For example, giving legal recognition to electronic records and signatures through the Electronic Transactions Act (Cap 88, 2011 Rev Ed), and addressing the admissibility of computer output evidence through the Evidence Act (Cap 97, 1997 Rev Ed).

5 For example, the Code of Practice for Competition in the Provision of Telecommunication Services 2012 (hereinafter "TCC") and Infocomm Media Development Authority Line Terminal and Radio-communication Equipment Standards (October 2016).

6 For example, Monetary Authority of Singapore Technology Risk Management Guidelines (January 2021) and the Cybersecurity Agency Cybersecurity Code of Practice for Critical Information Infrastructure (1st Ed, September 2018).

7 For example, the TCC, the Code of Practice for Market Conduct (S 148/2010) and the access regime to payment systems under Pt 3, Div 4 of the Payment Services Act 2019 (Act 2 of 2019).

8 For example, TCC and the Artificial Intelligence Model Governance Framework (2nd Ed, 21 January 2020).

9 For example, the Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) and the "Internet Code of Practice" *Infocomm Media Development Authority* <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/content-and-standards-classification/PoliciesandContentGuidelines_Internet_InterneCodeOfPractice.pdf?la=en> (accessed 5 December 2020) (hereinafter "ICOP").

10 For example, control of equity interests and voting power (*eg*, Pt VA of the Telecommunications Act (Cap 323, 2000 Rev Ed) and para 10 of the TCC), emergency powers (*eg*, special administration order under Pt VB of the Telecommunications Act) and continuity and resilience of essential services (*eg*, regulation of critical information infrastructures under the Cybersecurity Act 2018 (Act 9 of 2018)).

04.007 The choice of implementing policy through either governing laws or by regulations is influenced by several considerations. Laws generally apply broadly to shape societal conduct by defining the boundaries of permissible conduct, with *ex post* enforcement in the courts through prosecution or civil action.[11] New laws are introduced if the policy is of general application across the economy. Examples of early technology laws that Singapore introduced in the 1990s that illustrate this are the Electronic Transactions Act[12] ("ETA"), Computer Misuse Act[13] ("CMA") and new provisions to the Evidence Act[14] ("EA") dealing with computer output evidence. The nature of such laws depends again on the policy objectives. For example, the CMA defined new offences relating to misconduct that were either directed at computers or which were facilitated through the use of computers; while the ETA and EA provisions enabled the use of technology by recognising the legality of electronic records and signatures in satisfying legal requirements of writing or signature, and how such electronic records may be admitted into evidence in court proceedings.

04.008 Regulations, by contrast, apply to specific roles – and in this sense, may be thought of as having narrower application – and operate by defining a set of obligations and responsibilities expected from organisations or individuals that occupy such roles. The imposition of these *ex ante* obligations and responsibilities is often through a form of registration or licensing regime, with enforcement entrusted to public agencies that regulate the relevant sector of the economy (with avenues of appeal to the courts or other forms of judicial oversight). Regulations are promulgated by the sector regulator empowered by a parent legislation. For example, the Telecommunications Act[15] ("TA") introduced a licensing regime to regulate the provision of telecommunication services, and is administered by the Infocomm Media Development Authority of Singapore ("IMDA") as the information communications and media sector regulator through regulations, codes of conduct and licence conditions.

04.009 The foregoing categorisation is a helpful one to bear in mind as we descend into the depths of technology regulation. It will soon be evident that things are often not so clear-cut. In the latter parts of this

11 For example, Computer Misuse Act (Cap 50A, 2007 Rev Ed) offences are enforced through prosecution; the Spam Control Act (Cap 311A, 2008 Rev Ed) is enforced by private civil action; the Protection from Harassment Act (Cap 256A, 2015 Rev Ed) provides for enforcement by both prosecution and private civil action.

12 Cap 88, 2011 Rev Ed.

13 Cap 50A, 2007 Rev Ed.

14 Cap 97, 1997 Rev Ed.

15 Cap 323, 2000 Rev Ed.

chapter, we will discover that there are laws and regulations that are not so neatly categorised. For example, the Broadcasting Act[16] ("BA") class licence applies to Internet content providers, which may appear at first blush to be a defined role, but the role is also one that includes practically anyone who has posted user-generated content ("UGC") on social media platforms; and a number of laws that define clear *ex post* obligations that apply only to Internet intermediaries, who may be subject to court orders or executive directions to block access or communicate corrections.

1. Technology laws and regulations: An illustration

04.010 Electronic records and electronic signatures make a good case study to illustrate the interactions between technology laws and technology regulations, and how they implement policy. "In the physical world today, there are requirements for documents to be in writing and for hand-written signatures. Such requirements need to be translated into the electronic realm."[17] Legal requirements for writing previously meant putting pen to paper, and requirements for signature referred to a handwritten (or wet ink) signature. Their digital twins are electronic records and electronic signatures respectively.

04.011 When the ETA was introduced in the 1990s, the policy objective was to provide a "conducive legal and policy framework ... to create an environment of trust, predictability and certainty" in order for "Singapore to play the role of a secure and trusted node where e-commerce transactions from the region and around the world are processed".[18] In order to do so, the ETA aims to create the legal framework for reliable authentication of identity and assurance of the integrity of electronically transmitted documents. This is achieved by giving legal recognition to electronic records (or documents),[19] and how the requirements of writing[20] and signatures[21] can be met by electronic records and electronic signatures. The ETA also recognises secure electronic records and signatures by providing for presumptions as to their authenticity (or non-repudiation) and integrity.[22] Notably, certain classes of electronic records were excluded from this: for example,

16 Cap 28, 2012 Rev Ed.

17 *Parliamentary Debates, Official Report* (29 June 1998), vol 69 at col 252 (Lee Yock Suan, Minister for Trade and Industry).

18 *Parliamentary Debates, Official Report* (29 June 1998), vol 69 at col 252 (Lee Yock Suan, Minister for Trade and Industry).

19 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 6.

20 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 7.

21 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 8.

22 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Pt III.

negotiable instruments, wills, indentures, trusts and powers of attorney, contracts for and conveyance of immovable property.[23]

04.012 The ETA, when it was enacted in 1998, implemented the United Nations Commission on International Trade Law Model Law on Electronic Commerce,[24] and was amended in 2010 to align with the United Nations Convention on the Use of Electronic Communications in International Contracts.[25] The ETA was amended in February 2021 to adopt the UNCITRAL Model Law on Electronic Transferable Records[26] and to extend its coverage to negotiable instruments. The latest amendments give legal recognition to electronic records that are transferable, in the sense that exclusive control may be passed from one party to another,[27] thereby enabling the digitisation of negotiable instruments. Digitalisation of negotiation is enabled and given legal recognition. For bearer documents, the functional equivalent of transfer of possession is met through the transfer of exclusive control;[28] while the functional equivalent of indorsement is met through the inclusion of information required for the indorsement in the electronic transferable records, such as transfer of possession, indorsement in writing and signature.[29]

04.013 Also in the 1990s, the EA was amended "to provide for the admissibility and weight of computer output produced by any computer or network as evidence in both civil and criminal proceedings".[30] The old section 35 of the EA certification regime for admissibility of computer output as evidence introduced in the 1996 amendments was recently replaced with evidential presumptions in relation to electronic records.[31] Thus, *accurate* copies of electronic records can be recognised

23 Electronic Transactions Act (Cap 88, 2011 Rev Ed) First Schedule.
24 *Parliamentary Debates, Official Report* (29 June 1998), vol 69 at col 253 (Lee Yock Suan, Minister for Trade and Industry).
25 (23 November 2005), 2898 UNTS 3 (entered into force 1 March 2013). See *Parliamentary Debates, Official Report* (19 May 2010), vol 87 at cols 593–594 (Lui Tuck Yew, Acting Minister for Information, Communication and the Arts).
26 A/RES/72/114, adopted by the United Nations General Assembly, 72nd session (7 December 2017).
27 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 16I.
28 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 16I(2).
29 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 16K.
30 *Parliamentary Debates, Official Report* (18 January 1996), vol 65 at col 449 (S Jayakumar, Minister for Law).
31 *Parliamentary Debates, Official Report* (14 February 2012), vol 88 at p 1127 (K Shanmugam, Minister for Foreign Affairs and Minister for Law); see also Yeong Zee Kin & Paul Chan, "Electronic Evidence in Singapore: Out with the Old, In with the New" in *International Conference on Electronic*

(cont'd on the next page)

by law as primary evidence[32] and, where conditions relating to integrity and reliability are met, as digital originals.[33] There are presumptions as to *authenticity* under sections 116A(1) to 116A(3) of the EA – electronic documents ordinarily produced by a device is presumed to have been produced by it, and proof of production is dispensed with when electronic evidence is from a person not a party in the proceedings or from an adverse party. There is also a presumption of *accuracy* when electronic documents are recorded or stored through an approved process under section 116A(6) of the EA.

04.014 The ETA and EA illustrate how *technology laws* enable technology adoption by addressing legal ambiguities, by giving legal recognition to and admissibility of electronic records and electronic signatures. They apply broadly to all applications of these technologies. Thus, the ETA has been applied in respect of e-mails,[34] instant messages,[35] electronic ledgers,[36] digital temporary certificates of entitlement,[37] and softcopies of forged payslips.[38] Likewise, the EA has been applied in respect of e-mails,[39] chat logs,[40] computer records of telephone discussions,[41] spreadsheets,[42] digital photographs,[43] electronic ledgers,[44] electronic system logs,[45] Global Positioning System data,[46] position and bearing data from a vessel's navigation system and the port authority's tracking and monitoring system,[47] and deleted folders recovered using forensic software.[48]

Litigation (Lee Seiu Kin editor-in-chief; Yeong Zee Kin gen ed) (Academy Publishing, 2012) at p 223 *ff*.
32 See Explanation 3 to s 64 of the Evidence Act (Cap 97, 1997 Rev Ed).
33 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 10.
34 For example, *Progressive Builders Pte Ltd v Long Rise Pte Ltd* [2015] 5 SLR 689; *Joseph Mathew v Singh Chiranjeev* [2010] 1 SLR 338; and *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] 2 SLR(R) 651.
35 *Anuva Technologies Pte Ltd v Advanced Sierra Electrotech Pte Ltd* [2020] 4 SLR 569.
36 *Mitfam International Ltd v Motley Resources Pte Ltd* [2014] 1 SLR 1253.
37 *Kenso Leasing Pte Ltd v Hoo Hui Seng* [2010] SGMC 8.
38 *Public Prosecutor v Rudy Lim* [2010] SGDC 174.
39 *Super Group Ltd v Mysore Nagaraja Kartik* [2019] 4 SLR 692.
40 *Public Prosecutor v Michael Frank Hartung* [2020] SGDC 113.
41 *Manjit Kaur Monica v Standard Chartered Bank* [2000] SGHC 205.
42 *Ng Koo Kay Benedict v Zim Integrated Shipping Services Ltd* [2010] 2 SLR 860; *Lim Mong Hong v Public Prosecutor* [2003] 3 SLR(R) 88.
43 *Public Prosecutor v Vijayan Mathan Gopal* [2019] SGMC 81.
44 *Mitfam International Ltd v Motley Resources Pte Ltd* [2014] 1 SLR 1253.
45 *Telemedia Pacific Group Ltd v Credit Agricole (Suisse) SA* [2015] 1 SLR 338.
46 *Tan Thai Wei Jasper v Superdi Bin Osman* [2020] SGDC 130.
47 *The Dream Star* [2018] 4 SLR 473.
48 *Public Prosecutor v Anthony Ler Wee Teang* [2001] SGHC 361.

04.015 Turning from governing laws to regulations, the regulation of *digital signatures* and the admissibility of the output of an *approved process* illustrate the definition of roles, imposition of *ex ante* obligations and responsibilities, and an enforcement regime. These regulations address a subset of electronic records and signatures, providing stronger legal support (for example, through presumptions or limitation of liability) as *quid pro quo* for more prescriptive *ex ante* obligations and responsibilities.

04.016 A public key infrastructure ("PKI") based digital signature is commonly relied on to create secure electronic records and signatures in order to enjoy the attendant benefits of presumptions as to their authenticity and integrity. The PKI system requires the establishment of a certification authority who hosts the public key and issues the private key that is used to create digital signatures or encrypt electronic records. The ETA provides the overarching legal framework for the regulation and accreditation of certification authorities,[49] and the establishment of standards and practices for digital signatures,[50] which is a specific subset of secure electronic signatures.[51] The standards and practices have to be adhered to in order for this class of secure electronic signatures to qualify as digital signatures, and thereby benefit from the additional presumption as to correctness of information listed in a digital certificate,[52] and limit the liability of an accredited certification authority to its recommended reliance limit.[53]

04.017 The relevant ETA provisions and Electronic Transactions (Certification Authority) Regulations 2010[54] define the roles and responsibilities of different stakeholders in the PKI system for digital signatures. The roles of Controller, certification authorities and subscribers are defined and their respective responsibilities established. The Controller has oversight of certification authorities, with powers of investigations.[55] The certification authority "must utilise trustworthy

49 Certification authorities are "designated persons" as specified in s 20 of and the Fourth Schedule to the Electronic Transactions Act (Cap 88, 2011 Rev Ed).

50 Digital signatures are "specified security procedures" as specified in s 21 of and the Second Schedule to the Electronic Transactions Act (Cap 88, 2011 Rev Ed).

51 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, para 3.

52 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, para 4.

53 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, para 10.

54 S 650/2010.

55 Electronic Transactions Act (Cap 88, 2011 Rev Ed) ss 23 and 24.

systems in performing its services",[56] and its duties include mandatory disclosures, establishing the process for issuing, suspending and revoking certificates.[57] The duties of subscribers concerning the generation of the PKI key pair and control of their private key are also spelt out.[58]

04.018 The Electronic Transactions (Certification Authority) Regulations 2010 establishes a regime for *accreditation* of certification authorities to standards established in the Compliance Audit Checklist.[59] An accredited certification authority enjoys the additional protection of limiting its liability to the reliance limit that it commits to when issuing a certificate.[60] Presently, accreditation is voluntary and Netrust Pte Ltd appears to be the only certification authority accredited under this regime.[61] In a recent consultation, views were sought as to whether the existing voluntary nature of certification authority accreditation should be maintained.[62]

04.019 As to the admissibility of electronic records as evidence, we have discussed the presumptions as to authenticity and accuracy in sections 116A(1) to 116A(3) of the EA. Section 116A(6) of the EA and the Evidence (Computer Output) Regulations[63] create an additional regulatory framework for the production of accurate copies of electronic records through an approved process. The regulations define the role of a certifying authority, establish the procedures for appointing and revoking the appointments of certifying authorities,[64] and prescribe the

56 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, para 12.

57 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, Pt II.

58 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, Pt III.

59 Available at <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Acts-Regulations/CA_AuditChecklist.pdf?la=en> (accessed 13 November 2020).

60 Electronic Transactions Act (Cap 88, 2011 Rev Ed) Third Schedule, paras 10 and 11.

61 "Accredited CAs in Singapore" *Infocomm Media Development Authority* <https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations/controller-of-certification-authorities/accredited-cas-in-singapore> (accessed 18 December 2020).

62 See Infocomm Media Development Authority, *Consultation Paper on Review of the Electronic Transactions Act (ETA) (Cap. 88)* (27 June 2019) at pp 28 and 29.

63 Cap 97, Rg 1, 1997 Rev Ed.

64 Evidence (Computer Output) Regulations (Cap 97, Rg 1, 1997 Rev Ed) regs 13 and 14. KPMG and PricewaterhouseCoopers ("PwC") are appointed as certifying authorities: for KPMG, see "Evidence Act Certification" *KPMG* <https://assets.kpmg/content/dam/kpmg/sg/pdf/2017/12/Evidence-Act-certification-brochure.pdf> (accessed 13 November 2020) and for PwC, see "Evidence Act" *PwC* <https://www.pwc.com/sg/en/audit/evidence_act.html> (accessed 13 November 2020).

requirement of independence of the certifying authority.[65] Certifying authorities can certify that an imaging system complies with criteria that cover document capture, storage and output, and assures physical and system security.[66] The output of the approved process will benefit from the presumption as to accurate reproduction in section 116A(6) of the EA. The approved process is helpful when implementing large-scale imaging systems to capture, store and reproduce images of documents; and it is in use by the Singapore Customs[67] and the Inland Revenue Authority of Singapore.[68]

C. REGULATION OF INFRASTRUCTURE

04.020 In this part, an overview is provided on the regulation of the provision of the communications infrastructure (that is, carriage layer). Apart from telecom networks and systems, the telecom regulations extend to telco facilities like installations and plants. However, the construction and operation of data centres (often included as infocomm infrastructure) are not regulated, although there are voluntary technical standards (or green standards) for energy efficiency.[69]

04.021 While the preponderance of the ensuing discussion will be about technology regulations implemented through a licensing regime, it ought not to be forgotten that these are complemented by supporting laws.[70] The regulation of infrastructure is best understood

65 Evidence (Computer Output) Regulations (Cap 97, Rg 1, 1997 Rev Ed) reg 11.

66 Evidence (Computer Output) Regulations (Cap 97, Rg 1, 1997 Rev Ed) First Schedule.

67 Singapore Customs, *Keeping and Maintaining Records in Image System* (Version 1.2, 13 May 2016).

68 Inland Revenue Authority of Singapore, *IRAS e-Tax Guide: Record Keeping Guide for GST-Registered Businesses* (6th Ed, 12 October 2020).

69 See "Green Data Centre Standards" *Infocomm Media Development Authority* <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Green-Data-Centre-Standard> (accessed 18 December 2020); and "BCA-IMDA Green Mark for Data Centres Scheme" *Infocomm Media Development Authority* <https://www.imda.gov.sg/programme-listing/green-ict/initiatives/bca-imda-green-mark-for-data-centres-scheme> (accessed 18 December 2020).

70 For example, control of equity interests and voting power in designated telecom licensees, *etc*, under Pt VA of the Telecommunications Act (Cap 323, 2000 Rev Ed) ("TA"); and offences under Pt VI of the TA: *eg, Public Prosecutor v Tan Khoon Shan Terrance* [2012] 4 SLR 1121, where the accused damaged fibre splicing boxes in order to disrupt Internet access and connectivity, and *Public Prosecutor v Boon Yu Kai John* [2004] 3 SLR(R) 226, where the accused knowingly transmitted a false message to the police.

as the regulation of the provision of telecom services, supply of telecom equipment and the allocation of the limited resources that are necessary in order to do so. Telecom services are essentially the connection of calls or transmission of information between different end-point devices on the same or different telecom networks. It is therefore necessary to ensure the interoperability of these networks and the equipment or devices that are used. Telecom regulations are directed at ensuring a set of baseline technical standards to enable interoperability and the safety of the equipment and devices, as well as to ensure that there is open access for interconnection between networks. The regulations also deal with upstream issues such as the allocation of limited resources, and downstream issues like access to premises and the protection of consumers who have subscribed to telecom services.

Services Based Operator (Dominant/Non-Dominant)		
Facilities Based Operator (Public Telecom Licensee; Dominant/Non-Dominant)		
Spectrum	**Telephone Number**	**Satellite Orbital Slot**

Table 1

1. Provision of telecommunications service

04.022 The exclusive privilege to operate and provide telecom systems and services in Singapore is granted to IMDA by virtue of section 3 of the TA, but with exceptions for persons running telecom services for his own use or business where all the equipment is situated within a single set of premises in single occupation (including vessel, aircraft, or vehicle), or by uniformed services (for example, the Singapore Armed Forces, Singapore Police Force, Singapore Civil Defence Force or visiting forces). The IMDA may grant licences to run telecom systems and services.[71] Licences for the provision of telecom services are either for facilities-based operations ("FBO") or services-based operations ("SBO"). Individual licences are issued for FBO, while individual or class licences may be issued for SBO.

71 Telecommunications Act (Cap 323, 2000 Rev Ed) s 5.

(a) Facilities-based operations licensees

04.023 An FBO licence is required if there is deployment or operation of telecom network, systems or facilities.[72] Requirements for FBO licensees include providing and adhering to their network and services rollout plan, implementing and supporting number portability, meeting applicable Quality of Service ("QoS") standards and providing interconnection and access.[73] However, the deployment of infrastructure requires the balancing of telcos' interests in providing uninterrupted and quality telecom services and the interests of land and building owners, while protecting consumers as well in the midst of striking this balance:

(a) *Land owners* have to abide with some intrusions on their right of quiet enjoyment. In order to ensure the strength and quality of transmission signals passing over their land, prior notice has to be provided before construction of any new building higher than 30m within 200m of a telecom licensee's installation or plant.[74] To prevent disruption of telecom services, cable detection has to be carried out before earthworks within vicinity of telecom cables.[75]

(b) The Code of Practice for Info-communication Facilities in Buildings[76] issued under section 19 of the TA establishes the balance of rights and responsibilities for the provision of space for the installation of telecom systems. It establishes a *building owner's* obligations to provide space and facilities at its own costs and expense, and its duties in respect of such spaces and facilities. It also deals with the duties of telecom licensees when deploying or operating telecom systems in buildings.

72 The focus of the discussion is the deployment of networks on land, but it ought to be noted that deployment of submarine cables is subject to additional guidelines: see Infocomm Media Development Authority Guidelines on Deployment of Submarine Cables into Singapore (updated 1 October 2016) and Infocomm Media Development Authority Guidelines on the Management of Submarine Cable Damage Incidents in Singapore Port Limits and the Traffic Separation Scheme Zone (updated 6 October 2020).

73 See Annex 2 to the Guidelines on Submission of Application for Facilities-Based Operations Licence (Version 5, 16 June 2020) <https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Licensing/Telecommunication/Facilities-Based-Operations/FBOGuidelines.pdf?la=en> (accessed 14 November 2020).

74 Telecommunications Act (Cap 323, 2000 Rev Ed) s 20.

75 Telecommunications Act (Cap 323, 2000 Rev Ed) s 29.

76 "Code of Practice for Info-communication Facilities in Buildings" *Infocomm Media Development Authority* (15 December 2018) <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Consultations/completed-consultations/consultation-papers/11/COPIF-2018.pdf?la=en> (accessed 14 November 2020).

(c) Land and building owners are prohibited from entering into exclusive agreements for the provision of telecom services or installation of systems, thereby ensuring that *occupiers* have choice and other telcos have access to the land or building.[77]

04.024 An FBO licensee may be designated as a public telecom licensee under section 6 of the TA. Part III of the TA provides public telecom licensees with certain privileges to access property (including state land) to survey and install telecom systems (subject to payment of compensation for "damage, disturbance or disability"),[78] and thereafter to inspect, maintain and repair any such installation or plant.[79] The owner or occupier of the land may request for alteration or relocation of the installation or plant when this is necessary or convenient for his use of the land or building.[80] The public telecom licensee has to ensure safety to persons and property when executing works;[81] for example, when removing trees or undergrowth that pose dangers to their installation or plant.[82] A public telecom licensee in control of critical support infrastructure ("CSI") may be subject to a special administration order under section 32I of the TA to ensure security and reliability of the supply of telecom services in Singapore.[83]

(b) Services-based operations licensees

04.025 SBO licences are intended for resellers of FBO telecommunication services or for operators that intend to lease telecommunication network elements (for example, transmission capacity and switching services) from an FBO licensee. There is no limit to the number of class licensees.[84] The categories of SBO (Individual) Licences are listed in the SBO licence application guidelines;[85] and the categories of class licenses (for example, Voice over Internet Protocol and public Internet access services) are established through the Telecommunications (Class Licences) Regulations.[86]

77 Telecommunications Act (Cap 323, 2000 Rev Ed) s 22.

78 Telecommunications Act (Cap 323, 2000 Rev Ed) ss 12–14.

79 Telecommunications Act (Cap 323, 2000 Rev Ed) s 16.

80 Telecommunications Act (Cap 323, 2000 Rev Ed) s 17.

81 Telecommunications Act (Cap 323, 2000 Rev Ed) s 24.

82 Telecommunications Act (Cap 323, 2000 Rev Ed) s 18.

83 Telecommunications Act (Cap 323, 2000 Rev Ed) s 32I(2)(*a*).

84 See Infocomm Media Development Authority Guidelines for Submission of Application for Services-based Operations Licence (Version 5a, 11 September 2020) at para 3.2.

85 Infocomm Media Development Authority Guidelines for Submission of Application for Services-based Operations Licence (Version 5a, 11 September 2020) at para 2.4.

86 Cap 323, Rg 3, 2002 Rev Ed.

(c) Telecom Competition Code

04.026 The Code of Practice for Competition in the Provision of Telecommunication Services 2012 ("TCC") is a sector-specific competition code issued under section 26 of the TA, which applies to telecom licensees *in lieu* of the general competition regime established by the Competition Act.[87] Competition policy in the telecom sector places general reliance on market forces in promoting consumer welfare, while promoting effective and sustainable competition through facilities-based competition and proportionate regulation.

04.027 FBO and SBO licensees are initially classified as either dominant or non-dominant,[88] with dominant licensees required to provide all services on just, reasonable and non-discriminatory terms,[89] and on an unbundled basis;[90] and whose tariffs are subject to review and publication.[91] For resellers, dominant licensees cannot prevent resale of its end user services[92] and have to provide equal opportunity to all sales agencies.[93] Dominant licensees also have Universal Service Obligations ("USO"), *viz* they have to provide service to any end user upon reasonable request.[94] In order to provide services, USO necessarily extends to network coverage. Thus, a financial penalty was imposed on OpenNet when it was unable to provide optical fibre services to certain physical addresses due to delays in the deployment of its network.[95] The

87 Cap 50B, 2006 Rev Ed. Paragraph 5 of the Third Schedule and para 1(*c*) of the Fourth Schedule to the Competition Act excludes the application of ss 34, 47 and 54 prohibitions to the provision of telecom services, as competition jurisdiction in the telecom sector has been given to the Infocomm Media Development Authority under the Telecommunications Act (Cap 323, 2000 Rev Ed) and TCC; see also *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2010] SGHC 97 at [25] *ff*.

88 For reclassification, see the Info-communications Development Authority of Singapore Advisory Guidelines Governing Petitions for Reclassification and Requests for Exemption under Sub-sections 2.3 and 2.5 of the Code of Practice for Competition in the Provision of Telecommunication Services 2012 (25 April 2014).

89 TCC para 4.2.1.2.

90 TCC para 4.2.1.3.

91 TCC para 4.4; tariffs for specified services have to be filed (para 4.4.1) and reviewed (para 4.4.3), while tariffs for all services have to be published (para 4.5).

92 TCC para 4.2.2.2.

93 TCC para 4.2.2.3.

94 TCC para 4.2.2.1.

95 "OpenNet Failed to Meet Universal Service Obligation and Quality of Service Standards" *Infocomm Media Development Authority* (20 November 2013) <https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2013/opennet-failed-to-meet-universal-service-obligation-and-quality-of-service-standards> (accessed 8 May 2021).

following telcos have been classified as dominant licensees: Singapore Telecommunications Ltd, Starhub Cable Vision Ltd, and the former OpenNet Pte Ltd, now restructured as NetLink NBN Management Pte Ltd and NetLink Management Pte Ltd.[96]

04.028 Competition law is a broad topic and the ensuing discussion about the application of competition law in the telecom sector will not cover general market conduct such as abuse of dominant position, unfair methods of competition and agreements that unreasonably restrict or distort competition,[97] or approvals for takeovers and consolidation of telcos.[98] It will focus on issues that are specific to the telecom sector.

(i) Interconnection

04.029 As discussed earlier, the interconnection of networks is essential to connect calls and transmit information. All telcos have a duty to interconnect,[99] disclose interconnection interfaces (both physical and logical),[100] and to comply with interconnection technical standards.[101] FBO licensees must provide interconnection to other licensees at a level of interconnection quality that it provides to itself or its affiliates, that is, non-discriminatory interconnection quality.[102] These measures ensure not just interoperability but also that the controller of the telecom infrastructure does not compete unfairly when providing the same

96 Info-communications Development Authority of Singapore Notice – Classification of Dominant Licensee Under Code of Practice for Competition in the Provision of Telecommunication Services 2010 (21 January 2011); Info-communications Media Development Authority Notice – Classification of Dominant Licensee Under Code of Practice for Competition in the Provision of Telecommunication Services 2012 – NetLink Management Pte Ltd (13 April 2017); OpenNet Pte Ltd has since been acquired by NetLink Trust and restructured into a business trust, with NetLink NBN Management Pte Ltd as the trustee-manager and NetLink Management Pte Ltd as the trustee: see "Our History" *NetLink Trust* <https://netlinktrust.com/about-us/about/our-history.html> (accessed 9 January 2021), and "Trust Structure" *NetLink NBN* <https://www.netlinknbn.com/trust_structure.html> (accessed 9 January 2021).

97 See Info-communications Development Authority of Singapore Advisory Guidelines Governing Abuse of Dominant Position, Unfair Methods of Competition and Agreements involving Licensees that Unreasonably Restrict Competition (25 April 2014).

98 See Info-communications Development Authority of Singapore Advisory Guidelines Governing Consolidation Review and Tender Offer Process (9 April 2012).

99 TCC para 5.2.

100 TCC para 5.7.1.

101 TCC para 5.7.2.

102 TCC para 5.4.2.

services to other SBO licensees on its network, or connecting calls that originate from other networks.

04.030 Dominant licensees are subject to higher standards. While interconnection agreements between non-dominant licensees are subject to review by the regulator, they can nevertheless take effect *upon submission* for regulatory approval.[103] However, interconnection agreements with a dominant licensee require *ex ante* approval before they are effective.[104] The same applies to modifications of interconnection agreements.[105]

04.031 Dominant licensees must publish a Reference Interconnection Offer ("RIO"),[106] which is subject to public consultation and regulatory approval.[107] The TCC articulates existing obligations for just, reasonable and non-discrimination, and services unbundling, in the context of interconnection services. Thus, the obligation to provide services on just, reasonable and non-discriminatory terms is articulated as a prohibition on discrimination;[108] and the obligation to provide unbundled services is articulated as the requirement for RIO to be clear, complete and modular.[109] Despite the published RIO, dominant licensees may still engage in negotiation for interconnection pursuant to an individualised interconnection agreement but they have a duty to negotiate in good faith.[110]

(ii) Infrastructure sharing

04.032 Physical infrastructure may be costly to replicate, either because the number of subscribers in the area are too few to justify costs of replicating infrastructure or the absolute cost is prohibitive. Apart from costs, space is a limited resource and the land or building owner may not have the space to accommodate requests from multiple telecom licensees. Thus, it makes sense for infrastructure sharing which may take place in either of two situations: first, where infrastructure sharing is in the public interest;[111] and second, where the infrastructure is a CSI. Examples of CSI include radio distribution systems for mobile coverage in train or road tunnel, in-building cabling, lead-in ducts and associated

103 TCC para 5.3.
104 TCC para 5.3(*a*)(i).
105 TCC para 5.6.6.1.
106 TCC paras 6.2.1 and 6.3.
107 TCC para 6.3.6.
108 TCC para 6.3.3.1.
109 TCC para 6.3.3.2.
110 TCC para 6.4.1.5.
111 TCC para 7.3.2.

manholes, monopoles and radio towers.[112] The considerations for determining when an infrastructure should be designated a CSI include: (a) the necessity of the infrastructure to the provision of telecom services; and (b) the ability of a new entrant to replicate the infrastructure or obtain access to the infrastructure on commercial terms that would not prevent its entry into the market. In making the determination, competing interests of the CSI controller – availability of spare capacity for sharing and whether CSI controller has legitimate justifications for refusing to share[113] – and the larger interest of achieving competition in the telecom market, have to be balanced.[114] The keen competition lawyer may notice that the considerations for determining a CSI echoes the elements of the essential facilities doctrine.[115] The regulator may designate the CSI either on request[116] or on its own initiative.[117]

(d) Consumer protection

04.033 Telecom licensees have extensive insight into their subscribers' usage of their telecom services. They also occupy a position in the subscription relationship with unequal control and bargaining power. As consumers are the ultimate beneficiaries of competition law and policy, the TCC establishes some boundaries in the telco–subscriber relationship. Before commencement of the subscription relationship, transparency of pricing and subscription terms[118] enables consumers to make informed decisions about taking up a subscription. During the subscription relationship, telecom licensees have to comply with QoS standards,[119] and subscribers are protected from undesirable marketing practices like charging for unsolicited services[120] or services supplied on a trial basis,[121] unless they have consented to receive the service. Telecom licensees have a duty to prevent unauthorised use of end-user service information.[122] Consent is required unless the use is

112 TCC para 7.5.1.
113 Telecommunications Act (Cap 323, 2000 Rev Ed) s 32G; TCC para 7.3.1.
114 TCC para 7.3.1.
115 The elements of the essential facilities doctrine as articulated in the US are: (a) control of the essential facility; (b) inability practically or reasonably to duplicate it; (c) denial of the use of the facility to a competitor; and (d) feasibility of providing the facility: see Organisation for Economic Co-operation and Development, *The Essential Facilities Concept* (OCDE/GD(96)113, 1996) at p 8.
116 TCC para 7.4.2.
117 TCC para 7.5.
118 TCC para 3.2.2.
119 TCC para 3.2.1.
120 TCC para 3.2.8.
121 TCC para 3.2.9.
122 TCC para 3.2.6.

for network planning, interconnection, provision of roaming services, law enforcement, regulatory compliance, debt recovery or fraud prevention.[123] To ensure that subscribers' choice to end the relationship is not compromised, telecom licensees are prohibited from imposing disproportionate early termination charges in order to ease switching;[124] nor can they switch subscribers to another telecom licensee's services without consent – a practice referred to as "slamming".[125]

2. Allocation of limited resources

04.034 We have seen that access to land and building and the sharing of infrastructure are important aspects of infrastructure regulation, particular for FBO licensees. Apart from access to physical resources, there are other limited resources that need also to be assigned. This includes telephone numbers that uniquely identify callers and recipients, so that calls can be connected; and allocation of radio frequencies (that mobile telephony and data connections depend on) to the right types of usage, in order to avoid interference and to ensure the quality of service. Just as physical space is a limited resource (for example, infrastructure sharing), orbital slots for satellites are also limited resources that have to be managed. Examples of limited resources are as follows:

(a) *Spectrum* is a limited resource with multiple competing needs: for example, provision of public mobile services, broadcasting services, private land mobile networks, and short-range devices like cordless phones. The IMDA is empowered under section 5A of the TA to grant spectrum rights. The Radio Spectrum Master Plan provides information of upcoming spectrum availability while the Spectrum Allocation Chart[126] tracks current radio frequency allocations.

123 TCC para 3.2.6.2. See *Odex Pte Ltd v Pacific Internet Limited* [2007] SGDC 248, where the predecessor to the TCC – the Code of Practice for Competition in the Provision of Telecommunications Services 2005 ("Code of Practice") – was raised as a shield to pre-action discovery application but the applicant failed to establish a strong *prima facie* case of wrongdoing. The court cited *Computerland Corp v Yew Seng Computers Pte Ltd* [1991] 3 MLJ 201 and implied that had the case for pre-action discovery been sufficiently strong, the application could have been granted despite the Code of Practice.

124 TCC para 3.2.3.

125 TCC para 3.2.5.

126 "Singapore Spectrum Allocation Chart" *Infocomm Media Development Authority* <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Frameworks-and-Policies/Spectrum-Management-and-Coordination/SpectrumChart.pdf?la=en> (accessed 13 November 2020).

The Spectrum Management Handbook[127] provides information on frequency allocations, licence applications and frequency fees. Spectrum rights are centrally allocated through auctions, tenders or assignments. Auctions are called where the market is fairly mature and the expected use of spectrum is well established. Auctions provide a transparent mechanism for open competition, where market demand is greater than the spectrum available. An example is the recent auction for the fourth telco licence.[128] Direct allocation mechanisms, such as a call for proposals, are considered in the case of nascent technologies, for example, 5G, where the business case and commercial use cases are still uncertain.[129] A broadcasting licensee under the BA (also administered by the IMDA) will also be assigned rights to use specified frequency or satellite orbits (if necessary), without the need to obtain separate allocation under a TA licence.[130]

(b) *Telephone numbers* are allocated to ensure fairness and transparency in order to provide a level playing field for competition. The National Numbering Plan[131] details how numbers are administered and managed, setting out usage, eligibility and assignment criteria, and applications and assignment procedures. For example, eight-digit numbers with leading digits 8 and 9 are reserved for radio networks, eight-digit numbers with leading digit 6 are reserved for public switched telephony services, and IP telephony services can use eight-digit numbers with leading digits 3 or 6.

(c) *Satellite orbital slots* are also limited resources. Satellite systems may be categorised into geostationary or non-geostationary satellite orbits. The global registration, co-ordination and operation of satellites is managed by the International Telecommunications Union ("ITU") and satellite network filings may only be submitted by ITU member states. Singapore is represented by the IMDA. The IMDA is also empowered to grant licences for the use of satellite orbital slots under section 5B of the TA. The Guidelines on Satellite

127 Issue 1, Rev 2.10, June 2020.

128 See Eileen Yu, "TPG Outbids MyRepublic to Snag Singapore's Fourth Telco Licence" *ZDNet* (14 December 2016); and Faris Mokhtar & Siau Ming En, "Australia's TPG Wins Battle for Fourth Telco Licence in Singapore" *Today* (14 December 2016).

129 See Aaron Tan, "IMDA to Issue 5G Spectrum to Singtel and StarHub-M1 Venture" *ComputerWeekly.com* (29 April 2020); and Lester Wong, "Singapore Awards 5G Licences to 3 Local Telcos" *The Straits Times* (30 April 2020).

130 Broadcasting Act (Cap 28, 2012 Rev Ed) s 24.

131 Issue 1.2 (August 2019).

Network Filing[132] set out procedures for application for satellite orbital slots licences and fees.

3. Supply of telecommunication equipment

04.035 The supply of network and telecom equipment is also regulated to ensure compliance with technical standards, for the purpose of interoperability as well as safety. While telecom equipment has to be approved under the TA before use,[133] the installation, importation and sale and operation of broadcasting apparatus are regulated under the BA.[134]

04.036 Dealers importing telecom equipment are required to apply for type-approval and an import permit.[135] This ensures that telecom equipment meets minimum technical standards covering areas like line terminal equipment, radio-communication equipment and reference standards established by the Telecommunications Standards Advisory Committee.[136] After importation, telecom equipment will first have to be certified or tested, before they can be registered, and thereafter offered for sale.[137] The IMDA has entered into mutual recognition arrangements[138] for telecom conformity assessments (both test reports and equipment certificates). Apart from technical standards, there are optional security product certifications like the Singapore Common Criteria Scheme,[139] which evaluates IT products against a common set

132 Available at <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Licensing/licenses/GuideSatelliteNetworkFiling.pdf?la=en> (accessed 13 November 2020).

133 Telecommunications Act (Cap 323, 2000 Rev Ed) s 9; Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed) reg 18.

134 Broadcasting Act (Cap 28, 2012 Rev Ed) s 20, *eg*, Television Receive-Only ("TVRO") system licence to install, operate or possess a TVRO satellite system to receive satellite TV channels from terrestrial satellites.

135 Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed) regs 18(2) and 20.

136 "Compliance to IMDA Standards" *Infocomm Media Development Authority* <https://www.imda.gov.sg/regulations-and-licensing-listing/dealer-and-equipment-registration-framework/compliance-to-imda-standards> (accessed 21 November 2020).

137 Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed) reg 21.

138 "Mutual Recognition Arrangements" *Infocomm Media Development Authority* <https://www.imda.gov.sg/Who-We-Are/international-relations/mutual-recognition-arrangements> (accessed 21 November 2020).

139 "Singapore Common Criteria Scheme" *Cyber Security Agency* <https://www.csa.gov.sg/programmes/csa-common-criteria/about> (accessed 21 November 2020).

of security functions, and the Cybersecurity Labelling Scheme[140] to improve IoT security for consumer smart devices.

04.037 Dealers of type-approved, registered or scheduled exempt telecom equipment[141] are subject to a Dealer's Class Licence under the Telecommunications (Dealers) Regulations[142] and have to be registered.[143] The Dealer's Class Licence establishes *ex ante* standards of conduct on the types of telecom equipment that can (and cannot) be sold:[144] for example, labelling of registered equipment intended for use in Singapore, how export-only equipment ought to be labelled and the conditions for sale. An individual licence is required when dealing in telecom equipment that is not registered or exempted from the registration requirement. Individual licensees may only sell to another individual licensee or to another person (not holding a class licence) for re-export.[145]

4. Ensuring cybersecurity standards

04.038 Before leaving the discussion of infrastructure regulation, we turn to consider new cybersecurity regulations that apply to critical information infrastructure ("CII"). Owners of computer systems necessary for continuous delivery of an essential service which, if compromised, will have a debilitating effect on the availability of the essential service may find that their computer or computer system is designated as a CII.[146] Essential services are listed in the First Schedule to the Cybersecurity Act 2018,[147] covering 46 services across 11 sectors, including info-communications (that is, fixed and mobile telephony, broadband Internet access and national domain name registry services) and media (that is, broadcasting of free-to-air television and radio services). Hence, it would not be surprising if *public* telecom licensees, *dominant* FBO and SBO telecom licensees and *free-to-air* broadcasting

140 "Cybersecurity Labelling Scheme" *Cyber Security Agency* <https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls> (accessed 21 November 2020).

141 See First Schedule to the Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed) for the list of telecom equipment that are exempted from the type-approval requirement.

142 Cap 323, Rg 6, 2004 Rev Ed.

143 Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed) reg 3.

144 Class licensees cannot set equipment listed in the Third Schedule to the Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed).

145 Telecommunications (Dealers) Regulations (Cap 323, Rg 6, 2004 Rev Ed) reg 4.

146 Cybersecurity Act 2018 (Act 9 of 2018) s 7.

147 Act 9 of 2018.

licensees had part of their infrastructure designated as CIIs, given their market position and reach.

04.039 Unlike more traditional regulatory approaches which put the onus on the provider of a regulated service or supplier of a regulated product to apply for a licence before carrying on with their business, not all owners or controllers of computer systems that support the delivery of essential services have to comply with the CII regulations. Only CIIs that have been designated by the Commissioner of Cybersecurity ("the Commissioner"), after analysing the threats posed and the likelihood and impact of the risks, need to do so. Designation of a computer system as a CII lasts for five years unless withdrawn earlier.[148]

04.040 The process of designation commences with a notice for the owner or any person exercising control over the potential CII to furnish information so that the Commissioner can ascertain whether the computer system fulfils the criteria of a CII.[149] If so, designation is initiated by notice issued to the CII owner. The CII owner may appeal to the minister in charge of cybersecurity, whose decision is final,[150] over the designation within 30 days.[151] In deciding appeals over the designation, the minister may seek the advice of an independent Appeals Advisory Panel appointed to advise on the appeal,[152] without being bound by their advice.[153]

04.041 Once designated as a CII, owners have to furnish information relating to the CII to the Cyber Security Agency ("CSA").[154] They also have to ensure that the CII complies with codes of practice or standards of performance.[155] The Cybersecurity Code of Practice for Critical Information Infrastructure[156] sets out compliance requirements covering areas such as risk-based governance requirements, protection requirements (for example, access controls, hardening of systems,

148 Cybersecurity Act 2018 (Act 9 of 2018) ss 7(3) and 9.

149 Cybersecurity Act 2018 (Act 9 of 2018) s 8; Cybersecurity (Critical Information Infrastructure) Regulations 2018 (S 519/2018) reg 3.

150 Cybersecurity Act 2018 (Act 9 of 2018) s 17(9).

151 Cybersecurity Act 2018 (Act 9 of 2018) ss 17(1) and 17(2).

152 See ss 17(8) and 18(1) of the Cybersecurity Act 2018 (Act 9 of 2018) and Pt 3 of the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (S 519/2018); as to the independence of the Appeal Advisory Panel, see s 18(5) of the Cybersecurity Act 2018 (Act 9 of 2018).

153 Cybersecurity Act 2018 (Act 9 of 2018) s 17(8).

154 Cybersecurity Act 2018 (Act 9 of 2018) s 10: see reg 4 of the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (S 519/2018) for the details of the information required to be furnished.

155 Cybersecurity Act 2018 (Act 9 of 2018) s 11.

156 1st Ed, September 2018 (hereinafter "Cybersecurity Code of Practice for CII").

securing remote connections and connections to removable storage media), resiliency requirements (that is, business continuity and disaster recovery) and vendor management requirements when outsourcing operations.

04.042 CII owners also have to implement processes to monitor and detect cybersecurity events and threats, and establish a cybersecurity incident response and crisis communication plans in order to meet mandatory cybersecurity incidents reporting requirements.[157] They also have to participate in cybersecurity exercises for the purpose of testing the state of readiness to respond to significant cybersecurity incidents.[158] Additionally, CII owners have to conduct regular audits and rectifications at frequencies of at least once every two years; and risk assessments such as vulnerability assessments and penetration tests at frequencies of once every 12 months for IT systems or 24 months for systems used in monitoring or control of physical processes.[159]

04.043 Public telecom licensees, dominant FBO and SBO telecom licensees and free-to-air broadcasting licensees whose infrastructures are designated as CIIs will be subject to overlapping regulatory oversight. Additionally, Internet Service Providers ("ISPs") have to comply with the Telecommunications Cybersecurity Code of Practice.[160] As we have seen earlier, telecom regulations do also impose technical standards (for example, interconnection, radio-frequency and equipment safety). In order to reduce inconsistent or conflicting regulatory requirements, assistant commissioners for cybersecurity are appointed from sector regulators. With their experience and insight into the complexities

157 Section 14 of the Cybersecurity Act 2018 (Act 9 of 2018) establishes the mandatory incident reporting duty and reg 5 of the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (S 519/2018) prescribes the reporting requirements. See also cll 6 and 7 of the Cybersecurity Code of Practice for CII.

158 Cybersecurity Act 2018 (Act 9 of 2018) s 16; see also cl 9 of the Cybersecurity Code of Practice for CII.

159 Cybersecurity Act 2018 (Act 9 of 2018) s 15; Cybersecurity (Critical Information Infrastructure) Regulations 2018 (S 519/2018) reg 6; Cybersecurity Code of Practice for CII cll 2 and 5.5. See also the Cyber Security Agency of Singapore Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure (February 2021) and the Cyber Security Agency of Singapore Guidelines for Auditing Critical Information Infrastructure (January 2020), both accessible at "Supplementary References" *Cyber Security Agency* <https://www.csa.gov.sg/legislation/supplementary-references> (accessed 22 November 2020).

160 See "Telecommunications Cybersecurity Code of Practice" *Infocomm Media Development Authority* <https://www.imda.gov.sg/regulations-and-licensing-listing/infocomm-media-cyber-security> (accessed 22 June 2021).

peculiar to their sectors, they are expected to be able to balance cybersecurity needs with operational considerations.[161]

04.044 Finally, it should be noted that the CSA's general powers to investigate and prevent cybersecurity threats or incidents extend beyond CIIs, but those powers are investigatory in nature.[162] Where the severity of the cybersecurity threat or incident creates risk of significant harm to CII or disruption of an essential service,[163] they have more intrusive powers to access, monitor and scan, copy electronic records or computer programs, take remedial measures, and perform examination or analysis.[164]

D. CONTENT REGULATION

04.045 The content layer is much thicker than the carriage layer. Before wading into the weeds of content regulation, several features of this landscape ought to be highlighted. First, what exactly do we mean by "content"? In general, content may take one of two forms: the provision of information or the provision of online services. *Information* may be provided *gratis* (for example, blogs or social media channel) or it may involve some form of subscription (for example, over-the-top ("OTT") media services and subscription-based news services, which may be subject to sectoral regulation in the form of broadcasting licences). Online services may take the form of *transactional services* (for example, online retail) or *software-as-a-service* (especially cloud-based software-as-a-service or online games), which may be combined with professional services (for example, Security Operations Centre services). We exclude from our discussion the provision of *pure* professional services that also utilise software (for example, penetration testing services or incidental use of online file-sharing while providing accounting or legal advisory services).

04.046 Second, content regulation is also frequently implemented through sectoral regulation. In the ensuing discussion, focus will be on

161 See "How Will the Act Empower Sector Leads?" under "Frequently Asked Questions" *Cyber Security Agency* <https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx?FAQ=2109830> (accessed 19 December 2020).

162 Cybersecurity Act 2018 (Act 9 of 2018) s 19.

163 Cybersecurity Act 2018 (Act 9 of 2018) ss 20(3)(*a*) and 20(3)(*b*). Other severity thresholds are threats to national security, defence, foreign relations, economy, public health, public safety or public order, and the objective severe nature of the harm that may be caused to persons, number of computers or value of information put at risk: Cybersecurity Act 2018 ss 20(3)(*c*) and 20(3)(*d*).

164 Cybersecurity Act 2018 (Act 9 of 2018) s 20(2).

content regulation that is of broader application (for example, providing informational content) while discussions on sectoral regulation of services are deferred to subsequent chapters (for example, electronic payment and modern fintech services are discussed in the financial regulations chapter). Strictly speaking, regulating the provision of information online is sectoral regulation, that is, media regulation. However, with social media democratising content creation, anyone who ventures online would have posted UGC as some point. This justifies giving it a horizontal, as opposed to vertical or sectoral, treatment.

04.047 Third, it is apt to separate the discussion of intermediary regulation from content regulation. One way to distinguish between provision of online services and intermediation services is whether the service is provided directly to end-users (for example, payment services, online file-sharing) or whether the service is provided to link end-users with other end-users or service providers (for example, search engines, e-commerce and social media platforms). At a superficial level, it may be said that the intermediation services provided by Internet intermediaries – for example, search engines, e-commerce and social media platforms – can also be considered online services, but the central position that they occupy in two-sided markets, and the issues that have recently arisen (for example, competition and unfair practices), are sufficiently distinct that they warrant discussion separately from the more traditional provision of online services. A more detailed discussion of this distinction is undertaken in the intermediary regulation section.

04.048 Finally, a reminder to bear in mind is that the distinction between more general *laws* that govern content and the *regulation* of content provision. For example, the Personal Data Protection Act 2012[165] ("PDPA") is a general data protection law that governs the collection, use and disclosure of personal data and its Do Not Call provisions and the Spam Control Act[166] are laws that govern the specific use of contact information when sending direct marketing messages (predominantly through e-mails and instant messaging platforms these days).[167] Similarly, there are provisions in both the Protection from Online Falsehoods and Manipulation Act 2019 ("POFMA") and the Protection from Harassment Act[168] ("POHA") dealing with disinformation,[169] and provisions in the

165 Act 26 of 2012.

166 Cap 311A, 2008 Rev Ed.

167 These are discussed in ch 22.

168 Cap 256A, 2015 Rev Ed.

169 See Pt 2 and ss 10–15 of the Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019) for disinformation that injures the public interest; and Div 2 of Pt 3 of the Protection from Harassment Act (Cap 256A, 2015 Rev Ed) for disinformation against private individuals: see *Attorney-General v Ting Choon Meng* [2017] 1 SLR 373.

POHA that deal with online harassment and doxxing,[170] that govern online public discourse.[171] These are examples of *laws* that govern online activities carried out by a *broad segment of society*, although there are specific provisions in these laws that *regulate* the conduct of *Internet intermediaries* that will be discussed in the following part.

Online content (eg, blogs, online publications, social media)	**Transactional services** (eg, online retail)	**Software as a service** (eg, online gaming)
Digital utilities (eg, identity and trust services, e-payment services)		
Digital infrastructure (eg, broadband and IoT)		

Table 2

1. Internet content providers

04.049 The publication of information has a historical lineage that can be traced to the advent of the printing press. The Newspaper and Printing Presses Act[172] is probably one of the oldest forms of technology regulation. A printing press licence is required to keep and use a press for the printing of documents,[173] and permission to use premises as a printing press is required from the Urban Redevelopment Authority of Singapore. Newspaper permits are also required for printing or publishing newspapers,[174] or for the sale and distribution of Malaysian or offshore newspapers.[175] Local and imported publications are also subject to content guidelines, for example, not to feature content which causes racial or religious disharmony or undermines prevailing social

170 Sections 3–5 of the Protection from Harassment Act (Cap 256A, 2015 Rev Ed) ("POHA") apply to real-world and online acts that cause harassment, alarm or distress; ss 3(1)(*c*) and 5(1A) are anti-doxxing provisions that were more recently added to the POHA.

171 These are discussed in ch 24.

172 Cap 206, 2002 Rev Ed.

173 Newspaper and Printing Presses Act (Cap 206, 2002 Rev Ed) s 3; although there are exemptions if the press is used for the printing of invoices, name cards, bill heads, letterheads or collaterals for a company's own usage: see "Printing Press Licence" *Infocomm Media Development Authority* <https://www.imda.gov.sg/regulations-and-licensing-listing/printing-press-licence> (accessed 21 December 2020).

174 Newspaper and Printing Presses Act (Cap 206, 2002 Rev Ed) s 21.

175 Newspaper and Printing Presses Act (Cap 206, 2002 Rev Ed) ss 22 and 23.

norms (such as nudity, sex, drug abuse, crime and violence, gambling, or national security.)[176]

04.050 This detour into traditional (brick-and-mortar) technology regulation allows us to identify different roles that will remain relevant as our discussion segues into publication using online technologies: the technology platform (that is, printing press), the publisher (that is, newspaper company and its distribution network), and the content (that is, content guidelines). Authors have the most direct control over content; while publishers' role in pre-publication selection and editorial control forms the traditional basis for publishers' liability for content.[177] We will see that the content provider and publisher layers are where content regulation is at its thickest. It is in the technology layer that we have seen the greatest evolution in treatment over the past couple of decades as online publication (or distribution) technology evolved from Web 1.0 to social media: *viz*, evolving from protection from liability for network service providers ("NSPs") with no control over content that pass through their conduits, to the recognition that Internet intermediaries have some control over content cached or hosted on, or linked from, their platform, and are thus able to exercise some form of *ex post* access and correction influence. The ensuing discussion focuses mainly on the content provider and publisher layers, while we defer the platform discussion to the intermediary regulation section.

(a) Authors and publishers

04.051 The provision of online content – and we include not just the written word but also videos and music – is regulated through the BA. Broadcasting regulation is a specific domain of media regulation that traditionally applied to broadcasters providing linear programming or on-demand ("VOD") content; for example, free-to-air radio and television services, nationwide subscription television (or Pay-TV) services and OTT television services. Broadcasting licensees are assigned rights to use specified frequency or satellite orbits (if necessary),[178] have obligations

176 "Publications and Audio Materials" *Infocomm Media Development Authority* <https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/publications-and-audio-materials> (accessed 5 December 2020).

177 For examples of publishers' liability for defamation, see *Review Publishing Co Ltd v Lee Hsien Loong* [2010] 1 SLR 52, and *Chen Cheng v Central Christian Church* [1998] 3 SLR(R) 236; see also *Godfrey v Demon Internet Ltd* [2001] QB 201; [2000] 3 WLR 1020, where the defendant, ISP, was found not to be a publisher, but could still be potentially liable for publication as distributor after having been notified of the defamatory nature of a Usenet posting.

178 See para 04.034(a).

to carry public service broadcast content (for example, educational, news, arts and culture, drama and sports programmes),[179] and, through the "must carry" provision, provide for transmission and reception of free-to-air nationwide terrestrial television channels.[180] Similar to the telecom sector, the media sector is subject to its own competition code – the Code of Practice for Market Conduct in the Provision of Media Services[181] – which imposes, *inter alia*, public interest obligations to cross-carry content (for example, premium sports content).[182] Broadcast licensees have to comply with content codes for linear programming and OTT, VOD and niche services, covering classification and selection of programming content (for example, safeguarding racial and religious harmony, and preserving social norms and values, while ensuring it does not promote gambling, glorify crime and anti-social behaviour, or undermine national and public interests).

04.052 Reliance on the broadcasting laws to regulate Internet content provision is probably unique to Singapore. Broadcasting regulation has traditionally focused on establishing content standards for media channels with mass reach. It is therefore not surprising that its policies and machinery were extended to regulate the provision of content over the Internet when its *raison d'être* is to establish a baseline standard of responsibility when making content available online. Online content regulation is implemented through the Broadcasting (Class Licence) Notification,[183] which is issued under section 9 of the BA, and applies to two broad categories: Internet content providers ("ICPs") and ISPs. Our

179 Broadcasting Act (Cap 28, 2012 Rev Ed) ss 17 and 18.

180 Broadcasting Act (Cap 28, 2012 Rev Ed) s 19; Cable television ("TV") and Internet Protocol TV ("IPTV") licensees must carry free-to-air nationwide terrestrial TV channels: see paras 5.3.2(b) (for cable TV) and 5.4.2(b) (for IPTV) of the Infocomm Media Development Authority Code of Practice for Television Broadcast Standards (entry into force 4 May 2015).

181 Issued under Pt 7 of the Info-communications Media Development Authority Act 2016 (Act 22 of 2016), which grandfathered the Code of Practice for Market Conduct (S 148/2010) that was previously issued by the Media Development Authority.

182 Code of Practice for Market Conduct (S 148/2010) paras 2.1.5 and 2.7. This has been used for cross-carriage of the Union of Europe Football Associations European Championship 2012, Barclays Premier League 2013–2016, and Fédération Internationale de Football Association World Cup 2014: "Cross Carriage Measures" *Ministry of Communications and Information* <https://www.mci.gov.sg/portfolios/infocomm-media/initiatives/factsheets/cross-carriage-measure> (accessed 3 January 2021); see also David Lee, "Football TV Rights: Why It's Not Easy to Get It Right" *The Straits Times* (23 September 2020).

183 Cap 28, N 1, 2004 Rev Ed.

focus now is on ICPs, but we will discuss the roles and responsibilities of ISPs (in their various forms) later in this part.[184]

04.053 ICPs as a class have a broad catchment as its definition includes individuals, corporates and groups of individuals who provide any programme on the World Wide Web through the Internet.[185] As an aside, "programme" as defined under the BA is not limited to the linear programming content that we typically associate with terrestrial broadcasting services, but means "any matter the primary purpose of which is to entertain, educate or inform all or part of the public", including advertising.[186] "Programme", therefore, includes websites, blogs and even social media channels. Thus, ICPs include both authors of individual articles as well as publishers of curated content. The class licence imposes on ICPs and ISPs an obligation to comply with the Internet Code of Practice ("ICOP") that establishes ground rules for online discourse.[187] Under the ICOP, a couple of obligations are of particular relevance to ICPs. First, ICPs are to ensure that prohibited material is not hosted or included in its services, or access is denied when prohibited material is discovered or notified.[188] Prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.[189] Second, ICPs have an obligation to remove content that breaches the ICOP or is against public interest, public order or national harmony, or offends against good taste or decency.[190] Additionally, class licensees have obligations to assist in investigations,[191] and provide information to the IMDA concerning the provision of its service as required.[192]

04.054 The class licence applies automatically to any ICP, without more, but there are two notable exceptions. First, there are registration requirements for ICPs that are political parties or who engage in

184 See paras 04.059–04.060 and 04.073 *ff*.

185 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) para 2.

186 Broadcasting Act (Cap 28, 2012 Rev Ed) s 2.

187 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed); ICOP.

188 ICOP para 3(3).

189 ICOP para 4(a); see para 4(b) for a list of factors to be taken into account in considering whether material is prohibited material.

190 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 16.

191 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 9.

192 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 12.

propagation, promotion or discussion of political or religious issues;[193] and similarly, ICPs providing subscription-based online newspapers or individuals who engage in propagation, promotion or discussion of political or religious issues have to be registered with the IMDA if required to do so by written notice.[194] Second, if an ICP provides, on average, over any two consecutive months, at least one Singapore news programme (that is, article) per week that is accessed from at least 50,000 different IP addresses in Singapore per month, then the IMDA may notify the ICP in writing that it is excluded from the class licence,[195] in which case an individual licence under section 8 of the BA will probably be necessary in order to continue operating the website, blog or social media channel.[196] As of January 2014, there were ten online news licences issued to new portals that report regularly on Singapore's news and current affairs and enjoy significant reach among Singaporeans.

(b) User-generated content

04.055 Organisations that publish websites or individuals who maintain blogs will probably not chafe at being labelled ICPs. Web 1.0 technology was such that the publication of a website was a deliberate affair, requiring the author to understand domain name and website hosting, and use web-editing tools to compose their website. With advances in Web 2.0, technologies like blogs made publication by individuals even easier. The size of the class of content authors has been growing exponentially as publication technology developed from traditional print publication to Web 1.0 and to Web 2.0 technologies. Social media platforms like Facebook, Twitter, YouTube, Instagram and, more recently TikTok, make it a lot easier for the casual user to contribute UGC. The uploading of a video or adding some commentary when sharing links or retweeting, while still conscious actions, do not involve the same degree of deliberation as a website or blog publication. One may therefore question whether social media users should come under the umbrella definition of ICPs, and their social media posts be treated as licensable programmes. But the argument cuts both ways, as the democratisation of content creation makes it all the more necessary

193 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, paras 3 and 4.

194 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 5.

195 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) para 3A.

196 See *Parliamentary Debates, Official Report* (20 January 2014), vol 91 "Oral Answers to Questions: Criteria for Registration under Broadcasting (Class Licence) Notification Framework" (Lawrence Wong, Senior Minister of State for Communications and Information).

that the baseline of responsible behaviour applies to all, even the casual social media contribution, if we are to ensure the safety and harmony of our digital spaces.

04.056 The debate as to whether UGC needs to comply with the ICOP is moot, as the ICOP requires ICPs that provide social media platforms that host UGC to use best efforts to ensure that UGC conforms with applicable code of practices.[197] This implies that UGC is subject to the class licence and social media contributors of UGC are themselves also ICPs (which should not be surprising given the broad definitions of "ICP" and "programme"). But it is worth highlighting that the approach that has been taken is somewhat more calibrated and pragmatic, as it suggests that the primary responsibility is placed on the social media platform providers to police compliance, probably through acceptable use policies enforced through content moderation supported by technologies like AI.[198]

2. Online services

04.057 Internet content can also take the form of online services that allow users to conduct transactions (for example, online retail and electronic banking) or consume software-as-a-service (for example, file-sharing, online photo albums, and web mail).[199] Unlike online *informational* content, which is subject to broad regulation through the class licence and ICOP discussed in the preceding section, the provision of *online services* is not subject to similar horizontal regulation, but vertical or sectoral regulations. By nature of the diverse range of online services, this part can only attempt to provide a brief map of the different technological layers with examples of the types of sectoral regulations that may apply, and provide references to subsequent chapters that delve deeper into these domains. The ensuing discussion deals first with digital infrastructure and digital utilities, which are horizontal services that are designed to be consumed by different vertical applications, before discussing transactional services and software-as-a-service, which are vertical in nature.

197 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 14.

198 For example, Kate Conger, "Facebook Says It Is More Aggressively Enforcing Content Rules" *The New York Times* (23 May 2019); and Adi Robertson, "Facebook Says AI Has Fueled a Hate Speech Crackdown" *The Verge* (19 November 2020).

199 See also para 04.045.

(a) Digital infrastructure

04.058 Sitting closest to physical infrastructure, digital infrastructure is a critical enabler for the digital economy and provides the foundation on which online services are built.[200] The Organisation for Economic Co-operation and Development ("OECD") identifies broadband and the IoT as examples of digital infrastructure.[201] The IMDA Digital Economy Framework for Action contemplates digital infrastructure to include key digital technologies that businesses can plug into when building products and services. Unlike telecom infrastructure, the boundaries of digital infrastructure have not been definitively demarcated. For the purpose of discussing the regulation of digital infrastructure, we will draw a distinction between digital infrastructure that are more amenable to horizontal regulations and digital utilities that are likely to be subject to vertical or sectoral regulations.

(i) Broadband

04.059 ISPs that provide broadband data services for businesses and consumers to access the internet are referred to as Internet access service providers ("IASPs").[202] IASPs have to obtain either an FBO or SBO telecom services licence, and they are also subject to the broadcasting class licence. IASPs have to offer to their subscribers Internet content filtering arrangements that prevent access to undesirable, harmful or obscene content.[203] They must also refrain from subscribing to newsgroups containing prohibited materials, or unsubscribe from newsgroups as directed by the IMDA.[204]

04.060 Such filtering services offered to and controlled by subscribers should not be confused with filtering at the network level. The concept of net (or network) neutrality is that network traffic should be treated in a non-discriminatory manner, regardless of origin, content or destination.

200 See "Digital Economy Framework for Action" *Infocomm Media Development Authority* (21 May 2018) at p 33 <https://www.imda.gov.sg/-/media/Imda/Files/SG-Digital/SGD-Framework-For-Action.pdf> (accessed 3 January 2021).

201 "Digital Infrastructure" *Organisation for Economic Co-operation and Development* <https://www.oecd.org/going-digital/topics/digital-infrastructure/> (accessed 3 January 2021).

202 Apart from Internet access service providers, localised and non-localised resellers of Internet access services also come within the definition of Internet service providers: Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) para 2.

203 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 2A.

204 Para 3(2) of the ICOP.

This was implemented in the US through the Federal Communications Commission's ("FCC's") 2015 Open Internet Order[205] that established the principles that there should be no blocking, throttling or paid prioritisation of network traffic. In its 2018 Restoring Internet Freedom Order[206] ("2018 Order"), the FCC scaled back on these clear mandates, re-emphasising consumer protection and transparency instead. In the European Union ("EU"), Article 3 of the Open Internet Access Regulation[207] mandates net neutrality while permitting reasonable traffic management measures. Singapore's approach to net neutrality lies closer to the US FCC's 2018 Order in that it emphasises competition by promoting information transparency, while protecting consumers by requiring ISPs to adhere to QoS standards. Niche or differentiated Internet service offers are allowed,[208] but blocking of legitimate content – whether outright blocking or through discriminatory practices that effectively render such content inaccessible – is prohibited.[209] As the nature of broadband traffic changes, for example, with the increased consumption of videos and proliferation of IoT services, the flexibility to offer differentiated services (to both businesses and consumers) and manage network traffic will ensure that there is effective competition.

(ii) Internet of Things

04.061 High bandwidth, low latency broadband (for example, 5G) enables the IoT, where more computing takes place at the edge of the network and endpoint devices (for example, smart home devices and manufacturing equipment). The legal and regulatory issues are essentially around cybersecurity, application programming interfaces ("APIs") and data protection. The IoT is essentially about machine-to-machine ("M2M") communications, but with more consumer IoT devices in the mix, cybersecurity risks are accentuated. These risks can

205 FCC 15-24 (12 March 2015).

206 FCC 17-166 (4 January 2018).

207 Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

208 For example, zero-rating data usage for value-added services like WhatsApp or Spotify.

209 Info-communications Development Authority of Singapore, *Decision Issued by the Info-communications Development Authority of Singapore: Net Neutrality* (16 June 2011). See also the discussion on non-discriminatory interconnection quality at para 04.029.

be somewhat ameliorated by adopting cybersecurity standards, such as the Cybersecurity Labelling Scheme,[210] for consumer endpoint devices.

04.062 M2M communication depends on adopting IoT communications protocols (for example, ZigBee) and exposing web services or web APIs for communications. While APIs enjoy copyright protection,[211] the recent US Supreme Court decision in *Google v Oracle* clarified how the doctrine of fair use applied to APIs.[212] The value of APIs increases when more computer programmers use them, hence the US Supreme Court held that the application of fair use is unlikely to undermine the copyright protection of computer programs. In this case, copying of code was limited to those lines necessary to allow programmers to put their accrued talents to work in creating a new and transformative platform: the Android platform. Not only is the Android platform not a market substitute for the Java platform, but the latter in fact also stood to benefit from the reimplementation of its API in a different market. This decision is expected to support the adoption of standards, especially when there is transformative use in the creation of new products and services. However, it is not likely to significantly alter the contractual arrangements necessary for M2M communication and electronic data interchange.[213]

04.063 Data is a significant part of the payload for each transmission: for example, voice commands from smart home devices or sensor readings from wearable smart devices. The regulation of data is a complex tapestry of horizontal and vertical regulations. While machine data is generally unregulated, the collection, use and disclosure of personal data is governed by general data protection laws such as the PDPA, as well as sectoral laws and regulations: for example, the Banking Act[214] protects the privacy of customer information,[215] the Private Hospitals and Medical Clinics Act[216] regulates the protection of medical records,[217] and the TA and TCC prevents unauthorised use of end user service information data.[218] Sectoral regulations will play a significant role in the regulation

210 "Cybersecurity Labelling Scheme" *Cyber Security Agency* <https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls> (accessed 21 November 2020).
211 *Oracle America, Inc v Google LLC* 886 F 3d 1179 (Fed Cir, 2018).
212 *Google LLC v Oracle America, Inc* 141 S Ct 1183 (2021).
213 The copyright protection of application programming interfaces is discussed in detail in ch 16.
214 Cap 19, 2008 Rev Ed.
215 Banking Act (Cap 19, 2008 Rev Ed) s 47.
216 Cap 248, 1999 Rev Ed.
217 Private Hospitals and Medical Clinics Regulations (Cap 248, Rg 1, 2002 Rev Ed) reg 12.
218 See para 04.033.

of IoT devices and data, for example, connected medical devices. Data protection laws are sufficiently complex to deserve separate treatment in its own chapter.[219]

(b) Digital utilities

04.064 Application systems generally follow the three-tier architecture[220] – presentation, application and data tiers – with functions built as independent modules that are interchangeable and reusable.[221] These reusable modules are available commercially or as open-source software.[222] Increasingly, some of these functionalities are made available as web services that can be called (for example, through web APIs). This is the idea behind digital utilities, where such functions are made available over the Internet as a form of utility service that apps and systems may call.[223] A common example is user authentication which can either be modules that are integrated into the application or an electronic identification and trust service that can be called.[224] The ETA enables the use of such technologies when applied to identify users or electronically sign documents.[225] Electronic payment is another example of a common digital utility. The Payment Services Act 2019[226] regulates specified payment services, which are categorised as either payor or payee services.[227]

219 See ch 22.
220 See generally, "Multitier Architecture" *Wikipedia* <https://en.wikipedia.org/wiki/Multitier_architecture> (accessed 24 December 2020); and "Three-Tier Architecture" *IBM Cloud Education* (28 October 2020) <https://www.ibm.com/cloud/learn/three-tier-architecture> (accessed 24 December 2020).
221 See generally "Modular Programming" *Wikipedia* <https://en.wikipedia.org/wiki/Modular_programming> (accessed 24 December 2020); and "Modular Approach in Programming" *GeeksforGeeks* (last updated 7 September 2018) <https://www.geeksforgeeks.org/modular-approach-in-programming/> (accessed 24 December 2020).
222 For example, Pluggable Authentication Modules. See "Using Pluggable Authentication Modules (PAM)" *Red Hat* <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pluggable_authentication_modules> (accessed 24 December 2020).
223 Dzof Azmi, "IMDA: Utilities for a Digital Age to Be 'Dumb', Integrated and Inclusive" *Digital News Asia* (6 June 2019).
224 For example, SingPass and OpenID. See "What Is OpenID?" *OpenID* <https://openid.net/what-is-openid/> (accessed 24 December 2020).
225 See earlier discussion on electronic records and signatures, and the regulation of digital signatures at para 04.010.
226 Act 2 of 2019.
227 Part 1 of the First Schedule to the Payment Services Act. The regulation of payment services is discussed in ch 15.

04.065 The evolution of modules into services is motivated by the pursuit of positive network externalities as the value of trust and payment services increases with more consumers and businesses on the service. Unsurprisingly, the providers of these services tend to occupy positions and take on roles that are similar to Internet intermediaries, although they do not provide *intermediation* as a service. We will return to the discussion of whether these service providers should be classified as Internet intermediaries subsequently.[228] Given their central role, these are also areas that have attracted domestic and cross-border regulatory attention, in order to drive convergence of rules, mutual recognition and harmonisation of standards for interoperability. Examples of cross-border regulations include the eIDAS Regulation on electronic identification, authentication and trust services,[229] and the Payment Services Directive 2 on payment services.[230]

(c) Transactional services

04.066 Vertical online services largely fall into one of two categories. First, they allow the customer to execute transactions with the business; and second, the customer uses the software as *the* service. The conduct of transactions through the internet can best be understood by using the common online business-to-consumer retail use case. The business provides an online portal from which the customer can select items for purchase, place them in the shopping basket, and then make payment when checking out. This *online sales stage* is followed by the *order fulfilment stage* where the items are then shipped from warehouse and delivered to the customer's doorstep.

04.067 The laws that govern and regulate e-commerce are myriad. Fundamental to the online sales stage is the conclusion of a binding contract of sale. There are attendant fundamental contractual law issues, such as the time and place of acceptance[231] and incorporation of terms (including unilateral mistake),[232] but with added complexities like

228 See paras 04.074–04.075.

229 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

230 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

231 See s 13 of the Electronic Transactions Act (Cap 88, 2011 Rev Ed).

232 For example, *Chwee Kin Keong v Digilandmall.com Pte Ltd* [2005] 1 SLR(R) 502.

whether contracts can be concluded or performed by partly automated means.[233]

04.068 The order fulfilment stage brings up perennial and evolving legal issues like electronic trade documentation, as goods are shipped from the warehouse and delivered to the customer's home. One of the key technological challenges thus far has been to replicate the transfer of exclusive control in order to digitise negotiable trade finance documentation like the bill of lading, which entitles the holder to receive the shipment of goods. With recent advances in distributed ledger technology ("DLT"), this challenge appears to have been solved. There have been a number of successful proof of concepts implementing trade finance registries using DLT.[234] Concomitantly, the UNCITRAL Model Law on Electronic Transferable Records[235] ("MLETR") provides a standard for legal harmonisation, and the ETA was recently amended to remove the exclusion of negotiable instruments and to adopt the MLETR.[236]

04.069 The provision of online transactional services may also be subject to sectoral laws (for example, consumer protection laws for online retail and financial regulations for electronic banking and remittance) and regulations (for example, the online sale of telecom equipment may require type approval and conformity assessments, and dealers are subject to a class licence).[237]

(d) Software-as-a-service

04.070 By way of recapitulation and context-setting, the discussion in this section focuses on software that is provided for customers to *use*, and follows earlier discussions on provision of information for consumers to consume (that is, online content publication) and businesses using online services to enable customers to carry out transactions. The days of

233 See s 15 of the Electronic Transactions Act (Cap 88, 2011 Rev Ed). These issues are covered in greater detail in ch 9.

234 For example, Karry Lai, "How Singapore's First Trade Finance Digital Registry Works" *DLT Ledgers* (28 October 2020); "Standard Chartered uses blockchain for trade finance in Singapore" *Ledger Insights* (24 January 2019) <https://www.ledgerinsights.com/standard-chartered-blockchain-trade-finance-singapore/> (accessed 24 December 2020); and "Hong Kong and Singapore Unveil DLT Trade Finance Project" *The Association of Corporate Treasurers* <https://www.treasurers.org/hub/treasurer-magazine/hong-kong-and-singapore-unveil-dlt-trade-finance-project> (accessed 24 December 2020).

235 A/RES/72/114, adopted by the United Nations General Assembly, 72nd Session (7 December 2017).

236 See para 04.012.

237 See para 04.035.

software distribution through optical discs and shrink-wrap licences are probably behind us now. Software can be sold and downloaded through the Internet – in which case, it is another example of online retail – or software can be offered as an online service for customers to use over the Internet. Increasingly, software-as-a-service integrates a downloadable program or app with an online feature set.

04.071 The provision of software is largely unregulated. Online gaming is a rare exception. The Remote Gambling Act 2014[238] makes the use and provision of remote gambling services offences.[239] "Gambling" includes gaming, which is a game of chance for money or money's worth.[240] Video games are also subject to regulation in the areas of content classification, distribution and advertising. Video games are console-[241] or personal computer-based,[242] but with a significant online component these days. The Films Act[243] defines "film" to include cinematograph film, video recording and video games.[244] The Video Game Classification Guidelines[245] establishes two classification ratings: Advisory 16 ("ADV16") is an advisory rating, while Mature 18 ("M18") is an age-restricted rating enforceable by law.[246] Video game distribution is subject to a class licence,[247] permitting the distribution of video games classified as "M18" or "ADV16", or exempted from classification by virtue of the Films (Classification – Exempt Video Games) Notification 2019.[248]

238 Act 34 of 2014.

239 Section 8 of the Remote Gambling Act 2014 (Act 34 of 2014) criminalises the use of remote gambling services by individuals, while ss 9–11 prohibit the provision of remote gambling services, whether based in Singapore or overseas (but with a Singapore-customer link); but lotteries for customers or by non-commercial organisations are exempted: see Remote Gambling (Exempt Persons) Order 2015 (S 127/2015).

240 Remote Gambling Act 2014 (Act 34 of 2014) s 2.

241 For example, Nintendo, Sony PlayStation and Xbox.

242 Including Macintosh.

243 Cap 107, 1998 Rev Ed.

244 Films Act (Cap 107, 1998 Rev Ed) s 2.

245 Infocomm Media Development Authority (29 April 2019). Classification takes into consideration social norms and values, protecting the young, and safeguarding racial and religious harmony, and not undermining public order or national interest.

246 Infocomm Media Development Authority, Video Games Classification Guidelines (29 April 2019) at para 5.

247 Films (Class Licence for Video Games Distribution) Order 2019 (S 342/2019), issued under s 10A of the Films Act (Cap 107, 1998 Rev Ed).

248 S 339/2019. An exempt video game is one that does not contain explicit sexual matters or behaviour or frequent use of coarse language, or any matter that offends racial or relegation harmony, promotes drugs, crime, violence or antisocial behaviour, promotes any views or publicises any cause: see definition of "exempt video game" in s 2 of the Films (Classification – Exempt Video Games) Notification 2019.

04.072 Loot boxes in video games introduce a game of chance by randomising the rewards that are unlocked through in-app purchases. These are a departure from the more traditional in-game rewards that are unlocked through credits accumulated through gameplay (or even in-app purchases) where the player knows exactly what enhancements he will get. Loot boxes are now in the crosshairs of policy makers looking to regulate them as gambling so as to protect vulnerable children.[249] The Ministry of Home Affairs recently sought comments through a public consultation on their intention to permit loot boxes in online games if the transferable virtual items given as prizes are retained within the game, but not used as a form of stake in (for example) another skin-betting site.[250]

E. REGULATION OF INTERMEDIARIES

04.073 The regulation of intermediaries is an evolving area of law. It is apt to commence with a definition of who Internet intermediaries are. We should not conflate gatekeeping and the pursuit of positive network externalities with the role of intermediation, notwithstanding that these may also be features of an intermediary. Thus, providers of identification, trust services and e-payment services may be gatekeepers, and their success very much dependent on the number of users they can amass on their services, but the services that they provide are not intermediation services.

1. Overview and future trajectory

04.074 Internet intermediaries "bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet-based services to third parties".[251] They often operate two-sided platforms that provide "technologies,

249 See generally Makena Kelly, "How Loot Boxes Hooked Gamers and Left Regulators Spinning" *The Verge* (19 February 2019); David Lazarus, "Are 'Loot Boxes' in Video Games a Form of Gambling?" *Los Angeles Times* (11 December 2020); and Zoe Kleinman, "Video Game Loot Boxes: Another Form of Gambling?" *BBC* (23 September 2020).

250 Ministry of Home Affairs, Public Consultation on Proposed Amendments to Laws Governing Gambling Activities (12 July 2021) at para 16 <https://www.mha.gov.sg/docs/default-source/media-room-doc/public-consultation-on-proposed-amendments-to-laws-governing-gambling-activities.pdf> (accessed 7 August 2021).

251 Organisation for Economic Co-operation and Development, *The Economic and Social Role of Internet Intermediaries* (OECD, April 2010) at p 9.

products or services that create value primarily by enabling direct interactions between two or more customer or participant groups".[252] Thus, *intermediation services* match parties from both sides, in order to allow them to interact directly: for example, matching consumers to businesses so that the latter can provide services or supply goods to the consumers. This can be contrasted with, for example, e-payment services, where although the success of the service depends very much on the number of merchants recruited, it is the e-payment service provider that is providing the payor or payee services.

04.075 In the performance of their role, intermediaries are expected to remain *neutral* and *passive* providers of intermediation services, delivering their services through *automated* technical means. These are enshrined as conditions for their protections from liability. The expectation of neutrality echoes the requirement of net neutrality for ISPs (at least in the EU and US), and the requirement of just, reasonable and non-discriminatory conduct expected of dominant FBO licensees that we have encountered earlier.[253] The passive role of intermediaries is exemplified in the notice and take-down ("NTD") safe harbour provisions that we will soon encounter. Finally, the basis for their protection from liability lies in how their intermediation services are provided: *viz.* automatically and through a technical platform. But as we shall see, this protection is calibrated based on their knowledge and technical ability to control content that is transmitted through, stored on or linked from their platform. Examples of Internet intermediaries include:

(a) IASPs and ISPs;[254]
(b) data processing and web hosting providers;
(c) Internet search engines and portals (for example, content aggregation and directory services);[255]
(d) e-commerce marketplaces;[256]

252 Andrei Hagiu, "Strategic Decisions for Multisided Platforms" *MIT Sloan Management Review* (19 December 2013).
253 See para 04.027.
254 Where an Internet service provider qualified as an intermediary, see *John Bunt v David Tilley* [2007] 1 WLR 1243.
255 Where a search engine (Google) qualified as an intermediary, see *Metropolitan International Schools Ltd v Designtechnica Corp* [2011] WLR 1743.
256 For a discussion as to whether an online e-commerce market place qualifies, see *L'Oreal SA v EBay International AG* [2009] EWHC 1094 (Ch) at [436] *ff.*

(e) social media platforms (for example, blogs, file-, photo- and video-sharing services);[257] and
(f) application stores.[258]

(a) Historical protection from liability for content

04.076 The impetus to regulate Internet intermediaries stems from the gatekeeping role they have on the two-sided platforms that they provide. They contribute effectively towards achieving policy objectives[259] and are equally efficacious in achieving enforcement outcomes.[260] We are experiencing an evolution in the regulation of Internet intermediaries. The earlier legislative interventions had focused on protection from liability for content through immunities and limitations on liabilities: for example, the enactment of the immunity provision in section 26 of the ETA in 1990 and introduction of safe harbour provisions in Part IXA to the Copyright Act[261] ("CA") in 2000 for NSPs. This coincided with global trends: *viz* EU's E-Commerce Directive[262] in 2000 that provided immunity for intermediary service providers that were mere conduits, and established safe harbours for caching and hosting intermediary services; which mirrored similar developments across the Atlantic where

257 Where a social media platform (Facebook) qualified as an intermediary, see *Richardson v Facebook* [2015] EWHC 3154 (QB).
258 Examples collated from: Organisation for Economic Co-operation and Development, *The Economic and Social Role of Internet Intermediaries* (OECD, April 2010) ("OECD report") at p 7; Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services ("hereinafter P2B Regulation") Preamble at para 11. See definition of "internet intermediary service" in s 2 of the Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019) ("POFMA"). Internet payment systems were listed as an example of Internet intermediaries in the OECD report, while the P2B Regulation excludes them; the author's view is that these should be classified as e-payment services instead. Likewise, Internet-based messaging services are included in the POFMA definition of "internet intermediary service", but the author's view is that these should be classified as communications services instead.
259 For example, neutrality as a condition for protection from liability under the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society service, in particular electronic commerce, in the Internal Market (hereinafter "E-Commerce Directive") and the basis for disclosure requirements in the P2B Regulation.
260 For example, access blocking and correction communication orders.
261 Cap 63, 2006 Rev Ed.
262 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society service, in particular electronic commerce, in the Internal Market.

the US had, just two years earlier in 1998, introduced: (a) § 512 of the US Digital Millennium Copyright Act[263] ("DMCA") providing Internet intermediaries safe harbour provisions for caching, hosting and linking; and (b) § 230 of the Communication Decency Act ("CDA")[264] providing immunity from civil liability for Internet intermediaries that restrict access to offensive content.

04.077 While immunities and limitations on liabilities hitherto granted to Internet intermediaries have powered their growth, there is emerging recognition that they are able to exercise some level of control over access, if not the content proper. Internet intermediaries currently do not have a general obligation to monitor their services or actively identify illegal activities,[265] and cannot be ordered to install filtering systems that requires monitoring of all communications on their network for peer-to-peer traffic in order to identify infringing content.[266] But there is increasing expectation for Internet intermediaries to act, as opposed to react. Thus, while intermediaries may not be jointly liable for trademark infringement, they are nevertheless amenable to injunctions that prevent further infringement.[267] This expectation can also find a toehold in the US DMCA safe harbour provisions, which are conditional on the adoption of "standard technical measures"[268] that could provide an avenue for the introduction of filtering and other technical measures, at least for copyright infringing content. The same result can be achieved under the US CDA immunity provision for objectionable content. Should this expectation gain traction, issues of fair distribution of costs and due process will have to be addressed, as Internet intermediaries shift from *ex post* content moderation (for example, disabling access and communicating corrections) towards exercising more *ex ante* editorial control (for example, content filters).[269]

263 17 USC (US) § 512.

264 47 USC (US) § 230.

265 E-Commerce Directive Art 15; Digital Millennium Copyright Act 17 USC (US) § 512(m)(1).

266 See Judgment of 24 November 2011, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs*, C-70/10, EU:C:2011:771 and Judgment of 16 February 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA v Netlog NV*, C-360/10, EU:C:2012:85.

267 But the scope that such an injunction may take was unclear and referred to the European Court of Justice: see *L'Oreal SA v EBay International AG* [2009] EWHC 1094 (Ch) at [444]–[465].

268 Digital Millennium Copyright Act 17 USC (US) § 512(i).

269 For further discussion, see Organisation for Economic Co-operation and Development, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (OECD, 2011), in particular ch 12.

04.078 In Singapore, there has been a distinct trend this past decade – with the enactment of POHA and amendments to the CA in 2014,[270] and the recent enactment of POFMA in 2019 – to require Internet intermediaries to disable access or communicate corrections. While still largely reactive and after-the-fact, these developments echo the shift away from immunities and safe harbours, wherein Internet intermediaries have a more passive role, towards imposing obligations to take positive action. Again, things are not so cut-and-dry as the POFMA Office has issued codes of practices that require prescribed Internet intermediaries to establish *ex ante* processes and adopt standards for giving prominence to credible online sources of information (and de-prioritising online locations that are subject to directions issued under Parts 3 and 4 of the POFMA).[271]

(b) Future trajectory in the regulation of conduct

04.079 The issues concerning Internet intermediaries are presently evolving. Businesses are increasingly dependent on Internet intermediaries for visibility and discoverability online. As gatekeepers – and even in the absence of dominance as defined by competition law – the asymmetry of market strength between Internet intermediaries and the businesses that depend on them have raised concerns: for example, fairness of Internet intermediaries' trading practices, treatment of businesses on their platform and transparency of ranking parameters. Business models of Internet intermediaries also introduce the need for transparency over differentiated treatment: for example, Internet search engines that sell advertisements may promote the visibility of their paying customers in search results, and e-commerce marketplaces may offer similar goods for sale in competition with other merchants on their platform. Access to data – that crucial digital infrastructure – generated by merchants and their customers' activity on the Internet intermediary's platform has also emerged as a topic of concern.[272] These issues provided the impetus to impose *transparency* obligations on Internet intermediaries through regulations such as Japan's Act on Improving Transparency and Fairness of Digital Platforms[273] and the EU

270 Namely, the introduction of provisions allowing applications to block flagrantly infringing online locations.

271 See para 04.097.

272 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services* (COM(2018) 238 final) at pp 1 and 2.

273 "Digital Platforms" *Ministry of Economy, Trade and Industry* <https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html> (accessed 22 June 2021).

P2B Regulation[274] which apply to providers of online intermediation services and online search engines that match business users to consumers.[275] In the main, they impose transparency obligations and fair trading practices in the following areas:

(a) establishing a baseline standard for terms and conditions for business users (for example, minimum notice period for changes to terms and conditions, obligation to provide reasons for restrictions on or suspension of services);[276]
(b) disclosure of and grounds for any restrictions on merchants from offering the same product or service on different terms via other channels;[277]
(c) disclosure of and considerations for any differentiated treatment given to similar or competing products or services offered by the Internet intermediary or affiliates it controls;[278]
(d) disclosure of the main parameters determining search ranking and their relative importance, including how ranking may be influenced through remuneration (for example, payments to improve ranking);[279] and
(e) to disclose whether business users have access to personal or other data generated through their use of the online intermediation services.[280]

04.080 This step towards regulation of Internet intermediaries' conduct – even if essentially (and initially) to impose transparency requirements – stands in stark contrast to the historical focus on protection from liability for content found in the older EU E-Commerce Directive. The forward

274 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
275 Examples of B2C online intermediation services are enumerated in para 11 of the Preamble, but the P2B Regulation excludes B2B intermediation services, online advertising services and exchanges, and online payment services.
276 P2B Regulation Arts 3, 4 and 8; Ministry of Economy, Trade and Industry, *Key Points of the Act on Improving Transparency and Fairness of Digital Platforms* (METI, 1 February 2021) at p 2.
277 P2B Regulation Art 10.
278 P2B Regulation Art 7.
279 P2B Regulation Art 5 and paras 25 and 26 of the Preamble. Note: it is *parametric* transparency that is required, not *algorithmic* transparency: Art 5(6); see also, Ministry of Economy, Trade and Industry, *Key Points of the Act on Improving Transparency and Fairness of Digital Platforms* (METI, 1 February 2021) at p 2.
280 P2B Regulation Art 9; Ministry of Economy, Trade and Industry, *Key Points of the Act on Improving Transparency and Fairness of Digital Platforms* (METI, 1 February 2021) at p 2.

trajectory, in the EU at least, appears to be increasing focus on conduct regulation of Internet intermediaries. Draft laws in the form of the Digital Services Act[281] and the Digital Markets Act[282] look set to expand conduct regulation for Internet intermediaries.[283] Singapore has also taken an initial step in *sectoral regulation* of Internet intermediaries with the enactment of the Point-to-Point Passenger Transport Industry Act 2019,[284] which introduced a licensing regime for ride-hailing platforms like Grab and Gojek that intermediate between drivers and riders.[285]

2. Nature of regulatory protections and obligations

04.081 The ensuing discussion focuses on the types of protections and obligations that may be found across our statute books, drawing comparisons with global developments where relevant. Before delving into the woods, the lay of the land can be briefly surveyed. The EU E-Commerce Directive establishes immunity for mere conduits and safe harbour provisions for system caching, hosting and linking. The US establishes immunity for Internet intermediaries blocking and screening offensive material, and immunity from copyright infringement for mere conduits, while relying on safe harbour provisions for system caching, hosting and linking for copyright infringement. In Singapore, there is immunity for civil and criminal liability for Internet intermediaries, except that for copyright infringement, the CA provides for immunity for mere conduits and safe harbours for system caching, hosting and linking.

<table>
<tr><th></th><th>Mere Conduit</th><th>System Caching</th><th>Hosting & Linking</th></tr>
<tr><td>EU</td><td>Immunity from civil liability</td><td colspan="2">Safe harbour for civil liability</td></tr>
<tr><td rowspan="2">US</td><td colspan="3">Immunity for blocking offensive material</td></tr>
<tr><td>Immunity for copyright infringement</td><td colspan="2">Safe harbour for copyright infringement</td></tr>
</table>

281 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC* (COM(2020) 825 final, 15 December 2020).
282 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)* (COM(2020) 842 final, 15 December 2020).
283 See para 04.111.
284 Act 20 of 2019.
285 See Justin Ong, "4 Firms Awarded Ride-hailing Licences; Rules for Point-to-point Transport Operators to Start Oct 30" *Today* (30 October 2020).

	Mere Conduit	System Caching	Hosting & Linking
Singapore	Immunity from civil and criminal liability (except copyright)		
	Immunity for copyright infringement	Safe harbour for copyright infringement	

Table 3

04.082 Once we move beyond the more established regulatory framework around immunities and safe harbours for Internet intermediaries, there is – at least in Singapore – an emerging trend of laws that leverage their gatekeeper role to implement public policies, in the form of access blocking and correction communication orders. These are not, strictly speaking, *ex ante* regulations in the more traditional forms that we have been encountering in most of this chapter, but they do take on certain features of technology regulations, in that they are specific to identified classes and impose on them an obligation to take action. With this roadmap in hand, let us enter the woods.

(a) Immunities

04.083 The starting point is a consideration of the immunity provision in section 26 of the ETA, which provides that NSPs are not subject to civil or criminal liabilities (including liability under the PDPA) in respect of third-party material when they are merely providing access. The natural meaning of "access" is to obtain or retrieve information stored in a computer's memory,[286] and would therefore naturally include transmission, hosting and linking. The phrase "provides access" is defined to include automatic and temporary storage, that is, system caching.[287] This broad immunity from civil liability when providing access mirrors Art 12 of the EU E-Commerce Directive for Internet intermediaries that are mere conduits, but is broader than its safe harbour provisions in Arts 13 (caching) and 14 (hosting). By comparison, the US CDA provides Internet intermediaries with similar immunities for blocking and screening offensive material.[288] However, it ought to be noted that the ETA immunity does not apply to copyright infringement, for which the safe harbour provisions in the CA take precedence.[289]

04.084 Specifically for copyright infringements, Internet intermediaries *qua* NSPs falling under limb (*a*) of section 193A(1) of the CA

286 "Access" *Lexico* <https://www.lexico.com/definition/access> (accessed 28 December 2020).
287 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 26(3).
288 Communication Decency Act 47 USC (US) § 230(c)(2).
289 Electronic Transactions Act (Cap 88, 2011 Rev Ed) s 26(2)(*d*).

definition – "transmission or routing of data" or "transient storage" – cannot be ordered to pay monetary relief except for blocking access or terminating account. To qualify as "mere conduits", they must satisfy certain criteria: (a) the transmission is initiated by a third party such that the NSP does not select its recipients; and (b) the transmission or transient storage is carried out through an automatic technical process and the NSP does not make substantive modification to the transmission content.[290] This mirrors § 512(a) of the US DMCA. In *RecordTV Pte Ltd v MediaCorp TV Singapore Pte Ltd*,[291] the plaintiff sought to rely on this immunity. The court held that this provision was meant to protect *bona fide* NSPs from inadvertently being found liable for copying copyrighted material, but did not apply to the plaintiff who was in the business of operating a website that makes copies of copyrighted material. Further, the plaintiff had pre-selected the defendant's channels from which its own users could select specific programmes for recording. As a great amount of volition had gone into the plaintiff's pre-selection, it did not meet the condition of "automatic technical process".

04.085 While the foregoing examples of immunities are given to Internet intermediaries *qua* NSPs, immunities are also given to Internet intermediaries when they carry out access blocking orders. Under the POFMA, where a person fails to comply with a correction or stop communication direction issued under Part 3, or where an Internet intermediary is subject to a disabling or correction direction under Part 4 or account restriction direction under Part 6 in respect of fake accounts, and fails to comply with the direction, Internet intermediaries *qua* IASPs may be ordered to disable access to the online location by an access blocking order issued by the minister. IASPs are immune from any civil or criminal liability for complying with such orders.[292] In egregious cases where the owner of an online location is subject to three or more Part 3 or 4 directions over a six-month period, the online location may become a declared online location under section 32. Internet intermediaries (including IASPs) required to block access to the declared online location will be immune from any civil or criminal liability for complying with such site-blocking orders.[293]

290 Copyright Act (Cap 63, 2006 Rev Ed) s 193B(2).
291 [2010] 2 SLR 152.
292 See ss 16, 28 and 43 of the Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019) for the immunity provisions in respect of Parts 3, 4 and 6 directions respectively.
293 See ss 33(5) and 34(5) of the Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019) for the immunity provisions in respect of Internet access service providers and Internet intermediaries respectively.

(b) Safe harbour

04.086 The NTD provisions in the CA are a prime example of a statutory safe harbour, whereby an Internet intermediary is given immunity by establishing and operating an NTD system. The following discussion will deal with works of authorship under Part IXA of the CA, but the reader should note that there are *in pari materia* provisions under Part XII that protect performers' rights.[294] The safe harbour provisions apply to infringing copies that are transmitted, cached or stored on the Internet intermediary's primary network, that is, the network it operates or exercises control over.[295] These functions mirror those in Arts 12 (mere conduit), 13 (caching) and 14 (hosting) of the EU E-Commerce Directive; and similar provisions in US DMCA – §§ 512(b) (system caching), 512(c) (hosting) and 512(d) (linking).

04.087 The safe harbour provisions cover NSPs that perform the following functions:

(a) *mere conduits* that provide transmission or routing of data, including incidental transient storage (that is, the same class that benefits from immunity discussed in the preceding section);
(b) automatic *caching* of copies to facilitate efficient access by users;
(c) *hosting* of users' content; and
(d) *linking* though a search engine or directory service.

"NSP" is a decidedly older term. In comparison, newer legislation such as the POHA and POFMA have started to define Internet intermediary services as either: (a) providing end-users access to third party content (hosting); (b) transmission of such content to end-users (mere conduit); or (c) linking end-users to third-party content from an index of search results (linking).[296] For all intents and purposes, the NSPs defined under the CA and the Internet intermediaries defined under the POHA and POFMA are similar (with the exception that NSPs under the CA include automatic caching), and we will use the more modern term "internet intermediaries" as the superset; it more accurately describes their roles.

04.0887 The archetypal approach for the NTD safe harbour usually involves establishing the NTD process, publishing information about it (including notification requirements and forms), and providing a point

294 See s 252A *ff* of the Copyright Act (Cap 63, 2006 Rev Ed).
295 See definition of "primary network" in s 193A of the Copyright Act (Cap 63, 2006 Rev Ed).
296 See definition of "internet intermediary service" in s 2 of Protection from Harassment Act (Cap 256A, 2015 Rev Ed) and Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019).

of contact.[297] The NTD process commences with the complainant giving notice to the Internet intermediary identifying the infringing content, who will then take reasonable steps to remove or disable access to the infringing material.[298] After access to infringing content is removed or disabled, the Internet intermediary notifies the user who had made the content available and provides the user with a copy of the notice of complaint.[299] If the user provides a counter-notice, then the Internet intermediary will furnish the complainant with a copy of the counter-notice, notifying him that unless court proceedings are commenced by the copyright owner within the next ten working days, access to the allegedly infringing content will be restored. The Internet intermediary can proceed to restore access if court proceedings have not been commenced or the complainant fails to notify it that proceedings have been commenced.[300]

04.089 The premise of this approach is based on the Internet intermediary acquiring knowledge through the NTD process, by virtue of which it takes down the infringing material by removing or disabling access to it. This means of acquiring knowledge through notification is common to all Internet intermediaries: that is, caching, hosting and linking. Additionally, the safe harbour contemplates that Internet intermediaries that host or link to infringing material can also acquire actual knowledge of infringement or of the primary facts that lead to the inevitable conclusion that there is infringement.[301] It is worth noting that Articles 13 (caching) and 14 (hosting) of the EU E-Commerce Directive have similar provisions for the actual knowledge.

04.090 Adherence to the NTD process provides Internet intermediaries with a safe harbour such that they will not be subject to any liability under any rule of law in respect of actions taken in good faith by removing material or disabling access.[302] In copyright proceedings, reliefs available against Internet intermediaries are typically limited to removing or disabling access to infringing copies or terminating

297 Copyright Act (Cap 63, 2006 Rev Ed) ss 193C(2)(*b*) (for system caching), 193D(2)(*c*) (for storage) and 193D(4)(*c*) (for linking); see also the Copyright (Network Service Provider) Regulations (Cap 63, Rg 7, 2009 Rev Ed) for the form of notice, information requirement for the point of contact and how notice may be given.
298 Copyright Act (Cap 63, 2006 Rev Ed) ss 193C(2)(*b*) (for system caching), 193D(2)(*b*)(iii) (for storage) and 193D(4)(*b*)(iii) (for linking).
299 Copyright Act (Cap 63, 2006 Rev Ed) s 193DA(2)(*a*).
300 Copyright Act (Cap 63, 2006 Rev Ed) s 193DA(2)(*b*).
301 Copyright Act (Cap 63, 2006 Rev Ed) ss 193D(2)(*b*)(i) and 193D(2)(*b*)(ii) (for storage) and 193D(4)(*b*)(i) and 193D(4)(*b*)(ii) (for linking).
302 Copyright Act (Cap 63, 2006 Rev Ed) s 193DA(1).

user accounts.[303] There are, however, certain conditions that Internet intermediaries have to abide by in order to enjoy the safe harbour protection. System caching should be through an automatic process and for the purpose of facilitating efficient access to users' requests,[304] with no substantive modification made to the cached copy.[305] For hosting or linking, the Internet intermediary cannot receive financial benefit from hosting or linking to the infringing content.[306] It is worth noting that these conditions are similar to those in §§ 512(b) and 512(c) of the US DMCA, for system caching, and hosting and linking respectively.[307] Equally notable, the recent 2019 EU Copyright Directive[308] made a dent in the safe harbour for *online content-sharing* intermediaries[309] by making it subject to the conditions that they had made best efforts to: (a) obtain authorisation of copyrighted works; and (b) disable access to or remove infringing content that had been identified by rights holders.[310]

(c) Access blocking

04.091 Access blocking and correction communications order are not safe harbours in the form that we have just encountered.[311] These laws subject Internet intermediaries as a class to obligations in the form of *ex post* orders of court or executive directions to block access or to carry corrections. They capitalise on the gatekeeper role of Internet intermediaries for the effective implementation of public policy, mainly in the areas of piracy and disinformation. The role of

303 Copyright Act (Cap 63, 2006 Rev Ed) s 193DB(2).
304 Copyright Act (Cap 63, 2006 Rev Ed) s 193C(1).
305 Copyright Act (Cap 63, 2006 Rev Ed) s 193C(2)(*a*).
306 Copyright Act (Cap 63, 2006 Rev Ed) ss 193D(2)(*a*) (for storage) and 193D(4)(*a*) (for linking).
307 See *A&M Records, Inc v Napster, Inc* 239 F 3d 1004 (9th Cir, 2001) and *Perfect 10, Inc v Amazon.com, Inc* 508 F 3d 1146 (9th Cir, 2007), where the US Ninth Circuit Court of Appeal considered that the Digital Millennium Copyright Act 17 USC (US) § 512 safe harbour provisions were potentially applicable to hosting (*Napster*) and linking (*Amazon*) when remitting the appeals back to the District Court for trial.
308 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC ("hereinafter Copyright Directive").
309 The definition of "online content-sharing service provider" encompasses Internet intermediaries (hosting) that organise, store and give public access to a large amount of copyright-protected works uploaded by their users, although the definition excludes not-for-profit endeavours, online marketplaces, and cloud services for B2B or personal use: Copyright Directive Arts 2(6) and 17(3).
310 Copyright Directive Art 17(4) and para 70 of the Preamble.
311 See paras 04.086–04.090.

Internet intermediaries is largely reactive, but they are given a right to be heard as they have to implement the access blocking and correction communication orders or directions, which may incur not merely compliance cost but also sometimes costs to the performance and user-experience of their services. In the ensuing discussion, focus will be on the roles and responsibilities of Internet intermediaries, with the discussion on the substantive laws (for example, disinformation) deferred to subsequent chapters.[312]

04.092 Provisions that enable the courts or law enforcement agencies to give access blocking orders or directions have found their place in our statute books. We first encountered site-blocking directions in the broadcasting class licence, where IASPs may be requested to modify their content filter services to block access to undesirable, harmful or obscene programmes.[313] Since then, there has been increasing reliance on site-blocking to implement public policy, principally to maintain safe common digital spaces. The Remote Gambling Act 2014 empowers an authorised officer to direct the IMDA to order an ISP to disable access to online locations where individuals in Singapore may access remote gambling services.[314] Under the POFMA, Internet intermediaries may be directed under Part 4 of the POFMA to disable access to material containing false statement of facts pursuant to a disabling direction issued under section 22. However, search engines are partially exempted from this requirement.[315]

04.093 The courts may also issue access blocking orders. Under the POHA, access blocking orders may be made requiring an Internet intermediary to disable access by its end-users to material containing false statements of fact.[316] Under the CA, rights holders may apply to court for an order against an Internet intermediary *qua* NSP providing transmission or routing services (that is, "mere conduit"), whose services have been used to access a flagrantly infringing online location.[317] The applicant has to issue a cease and desist notice to the owner of the online location and may only notify the NSP of its intention to apply for the court

312 See ch 24.
313 Broadcasting (Class Licence) Notification (Cap 28, N 1, 2004 Rev Ed) Schedule, para 2A(5).
314 Remote Gambling Act 2014 (Act 34 of 2014) s 20; see also Remote Gambling (Access and Payment Blocking Orders) Regulations 2015 (S 49/2015).
315 See the Protection from Online Falsehoods and Manipulation (Exemptions from Sections 21(2)(*a*) and (*b*) and 22(2)(*a*)) Order 2019 (S 663/2019), which exempts Baidu and Google Search.
316 Protection from Harassment Act (Cap 256A, 2015 Rev Ed) s 15C.
317 Copyright Act (Cap 63, 2006 Rev Ed) s 193DDA(1).

order after expiry of the prescribed 14-day compliance period.[318] The court may grant the order after considering matters such as the primary purpose of the online location, its owner's general regard for copyright, and the frequency and volume of access to the online location.[319] In *PCCW Media Ltd v M1 Ltd*,[320] it was held that this statutory remedy is not assignable and only copyright owners or exclusive licensees may apply for site-blocking orders.

04.094 One of the issues that has arisen in respect of access blocking orders – and which is probably equally applicable to enforcement directions – is the ease with which the offending content can be made accessible via alternate sites. The procedural formalities and attendant delays in amending a court order prompted an innovative approach: coupling a dynamic injunction to the main site-blocking order. Thus, in *Disney Enterprises, Inc v M1 Ltd*,[321] the rights holders applied for a main injunction to block 53 websites and a dynamic injunction to block additional domain names, URLs and/or IP addresses of those sites. The court considered the dynamic injunctions to be "reasonable steps to disable access", since they did not require NSPs to block additional websites that had not already been included in the main injunction, but only required NSPs to block new means of access (that is, new domain names, URLs and/or IP addresses) to the 53 websites enumerated in the main injunction. The court recognised that the dynamic injunction was necessary to ensure that main injunction operated effectively as circumventive measures can be taken with ease and speed in order to evade the main injunction by changing the domain name, URL and/or IP address.

(d) Communicating corrections

04.095 The communication of corrections is an important tool to combat disinformation. Internet intermediaries may be ordered by the courts or directed by enforcement agencies to take an active role in communicating corrections, typically after exhausting the avenues for procuring the content provider to make those corrections directly.

04.096 Under the POHA, Internet intermediaries may be ordered by the courts to publish a targeted correction notice to all end-users in Singapore accessing material containing false statements of fact through

318 Copyright Act (Cap 63, 2006 Rev Ed) s 193DDB(1); see also the Copyright (Flagrantly Infringing Online Location) Regulations 2014 (S 802/2014) for (a) the 14-day prescribed period; and (b) the form of notice.
319 Copyright Act (Cap 63, 2006 Rev Ed) s 193DDA(2).
320 [2018] 5 SLR 375.
321 [2018] 5 SLR 1318.

their Internet intermediary services.[322] The targeted correction notice has to identify the false statement of fact and contain a statement either correcting the false statement of fact or linking to another location where the corrective statement may be found.[323] The targeted correction notice has to be easily perceived, by reason of its placement near the offending material, and by being conspicuous and not easy to miss.[324] Thus, in *Attorney-General v Lee Kwai Hou Howard*,[325] the District Judge ordered that a prominent notice of not less than 30 seconds communicating the counter-narrative and a link to a statement from the Ministry of Defence be carried at the commencement and the end of a video. However, on appeal, both the High Court[326] and the Court of Appeal,[327] held that the Government had no right to invoke this provision.

04.097 Under the POFMA, Internet intermediaries may be ordered under Part 4 of the POFMA to carry a targeted correction direction in respect of material containing false statement of facts under section 21. The correction notice may, instead of stating the counter-narrative, link to another location that carries it. The correction notice has to be communicated to all end-users in Singapore. Similar to the POHA requirements, the correction notice has to be easily perceived, by reason of its placement near the offending material, and by being conspicuous and not easy to miss.[328] However, search engines are partially exempted from this requirement.[329] Prescribed digital advertising intermediaries are required to take reasonable steps not to facilitate publicity of the online location that is subject to the correction direction.[330] The POFMA Office has issued a Code of Practice for Giving Prominence to Credible Online Sources of Information[331] establishing the due diligence standard expected of Internet intermediaries in search ranking, *viz* increasing visibility of authoritative information, while reducing visibility of material

322 *Attorney-General v Lee Kwai Hou Howard* [2015] SGDC 114.
323 Protection from Harassment Act (Cap 256A, 2015 Rev Ed) s 15D.
324 Protection from Harassment Act (Cap 256A, 2015 Rev Ed) s 16BB.
325 [2015] SGDC 114.
326 *Ting Choon Meng v Attorney-General* [2016] 1 SLR 1248.
327 *Attorney-General v Ting Choon Meng* [2017] 1 SLR 373.
328 See para 04.096.
329 See the Protection from Online Falsehoods and Manipulation (Exemptions from Sections 21(2)(*a*) and (*b*) and 22(2)(*a*)) Order 2019 (S 663/2019), which exempts Baidu and Google Search.
330 Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019) s 47; see also reg 5 of the Protection from Online Falsehoods and Manipulation Regulations 2019 (S 662/2019), prescribing the following digital advertising intermediary services: Google Ads and Audience Network.
331 Effective 2 October 2019.

subject to a Part 4 direction and providing indicators of trustworthiness of authoritative sources.[332]

04.098 In exigencies, prescribed Internet intermediaries may be directed to communicate a general correction direction. Presumably, such directions should be rare since there is no requirement to identify any material containing false statements of facts; and the nature of the Internet intermediaries that have been prescribed suggest that they have a certain reach to Internet users in Singapore.[333]

(e) Reduced set of responsibilities

04.099 Under the PDPA, data intermediaries are data processing organisations that process personal data for the purposes and on behalf of the data controlling organisation pursuant to a contract.[334] It should be noted at the outset that not all data intermediaries are Internet intermediaries, but the definition of "processing" can accommodate transmission and hosting intermediary services.[335] Internet intermediaries who are data intermediaries are not subject to the full set of data protection obligations, but only to the protection and retention limitation obligations.[336]

F. EMERGING REGULATORY ISSUES AND TECHNIQUES

04.100 The objective of this chapter is to provide a framework to understand how the application and supply of technology is regulated. Truth be told, the content *versus* carriage paradigm was first conceived in the early days of Internet regulation. Since the technology landscape has changed significantly in the past couple of decades, the framework has also evolved into the three layers that is presented in this chapter; and the contours within each layer continues to shift in reaction to advances

332 The Code of Practice for Giving Prominence to Credible Online Sources of Information (effective 2 October 2019) applies only to Google Search, YouTube, Facebook, Instagram, Twitter, WeChat and Baidu: List of prescribed intermediaries subject to the Codes of Practice, available at <https://www.pofmaoffice.gov.sg/documents/list-of-prescribed-intermediaries-31-jan.pdf> (accessed 3 January 2021).

333 See reg 3 of the Protection from Online Falsehoods and Manipulation Regulations 2019 (S 662/2019), prescribing the following intermediary services: Google Search, Facebook and Instagram, Twitter, Hardwarezone and Baidu.

334 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(2).

335 See definition of "processing" in s 2 of the Personal Data Protection Act 2012 (Act 26 of 2012), which includes the following processing operations: "recording, holding, retrieval, ... transmission, ...".

336 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(2).

in technology and innovation in business models. It is therefore apt to conclude with some predictions on how this framework might continue to flex and adapt.

1. Regulatory sandboxes: Supporting innovation

04.101 The ETA and EA provided us with illustrations of the classical interactions between technology laws and regulations, and their role as public policy tools in achieving policy objectives in enabling the deployment and adoption of technology. Moving upstream from deployment, regulations that support innovation may, at first blush, appear as a contradiction in terms. Regulation has traditionally been seen as the antithesis of innovation. When the problem is defined as supporting innovation, and we take a dispassionate approach to the generation of policy options, there is no reason why regulations cannot stand alongside economic incentives, state enterprises and direct provision as policy tools that can be utilised to achieve this policy objective. Hence, regulatory sandboxes have emerged in the last few years as a policy tool to support innovation in regulated sectors, by creating space for piloting new technologies and new policies.

04.102 Regulatory sandboxes may be classified in two categories. First, regulatory sandboxes created within a licensing regime like in the financial services[337] and the energy market.[338] These operate by lifting licensing requirements for the duration of the trial, with the objective of understanding how licensing conditions may need to be adjusted or how regulatory requirements may be met by trial participants. Since supporting innovation through regulatory innovation is a policy objective of regulatory sandboxes, it may be argued that another form of regulatory sandboxing is the reservation of limited resources to boost innovation and competition. The 2016 IMDA 4G spectrum auction reserved spectrum lots that only new entrants are eligible to bid for.[339]

04.103 The second category is a statutory regulatory sandbox. The regulatory sandbox for trials of autonomous vehicles is the prime

337 "Overview of Regulatory Sandbox" *Monetary Authority of Singapore* <https://www.mas.gov.sg/development/fintech/regulatory-sandbox> (accessed 29 December 2020).

338 "Regulatory Sandbox" *Energy Market Authority* <https://www.ema.gov.sg/Sandbox.aspx> (accessed 29 December 2020).

339 See Info-communications Development Authority, *Auction of 700MHz Spectrum Rights (2016), 900 MHz Spectrum Rights (2016), 2.3 GHz Spectrum Rights (2016) and 2.5 GHz Spectrum Rights (2016): Information Memorandum* (IDA, 29 April 2016) at para 7.1 *ff*.

example of this approach. The Road Traffic Act[340] ("RTA") was amended in 2017 to introduce a statutory framework for trials and use of autonomous vehicles.[341] The statutory sandbox is time-bound for five years, whereupon the RTA would presumably be amended.[342] IMDA's data regulatory sandbox is another example that depends on statutory powers to grant exemptions,[343] with the objective of working with the industry to prototype new policies that can eventually be introduced through advisory guidelines or statutory amendments.[344] An example is the business improvement exception which was introduced in the recent PDPA amendments[345] to implement the industry's recommendations concerning the use of data to support business innovation.[346]

2. Digital infrastructure: Regulation of data

04.104 With the important role that data plays in digital infrastructure, it should not be long before the contours around data regulation are clearly formed as a distinct digital infrastructure. This section attempts to identify where these contours might be. An evolving data issue is the flow of data across the domestic economy and across borders. While not quite a global consensus, there is momentum and support behind the principle that there should be free flow of non-personal data across borders, with reliance on data protection transfer mechanisms for personal data flows across borders. The EU has introduced a regulatory framework to prevent member states from enacting any barriers to the free flow of non-personal data in the single market;[347] and during Japan's chairmanship of the G20, the principle of "data free flow with

340 Cap 276, 2004 Rev Ed.

341 Road Traffic Act (Cap 276, 2004 Rev Ed) s 6A; see also the Road Traffic (Autonomous Motor Vehicles) Rules 2017 (S 464/2017).

342 Road Traffic Act (Cap 276, 2004 Rev Ed) s 6A(3).

343 Personal Data Protection Act 2012 (Act 26 of 2012) s 62.

344 "Data Collaboratives Programme (DCP)" *Infocomm Media Development Authority* <https://www.imda.gov.sg/programme-listing/data-collaborative-programme> (accessed 29 December 2020).

345 See Pt 5 of the First Schedule and Pt 2 of the Second Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012), introduced *vide* the Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020), which was passed by Parliament on 2 November 2020 and assented to by the President on 25 November 2020.

346 Yeong Zee Kin, Deputy Commissioner, Personal Data Protection Commission, keynote speech at AI and Commercial Law: Re-imagining Trust Governance and Private Law Rules conference (5 December 2019).

347 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union Art 4.

trust" was endorsed via a ministerial statement.[348] However, this chapter is still being written as there are still proponents of data localisation requirements either in the form of data protection laws,[349] or cyber and data security laws.[350]

The Chinese Administration of Cyberspace recently commenced a national security review of DiDi's transfer of data to the US, when it was preparing for its listing on the New York Stock Exchange, to ascertain compliance with Chinese cybersecurity laws.[351]

04.105 Even where there is consensus on the cross-border flow of personal data, there are myriad transfer regulations – for example, Chapter V of the EU General Data Protection Regulation[352] ("GDPR"), the APEC Cross Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP") systems, and the ASEAN Framework on Digital Data Governance[353] – and transfer mechanisms (for example, contract clauses, binding corporate rules, certification systems and white-listing or adequacy assessments). Interoperability of regional data protection blocs – for example, between EU GDPR and APEC CBPR/PRP – is on the agenda, although discussions are expected to be protracted. Interoperability in the short term may instead take the form of harmonisation of transfer mechanisms, for which there is much greater consensus, and standardisation of the templates and processes for adopting them.

04.106 Equally important for supporting innovation is the flow of data across the domestic economy. Singapore's Trusted Data Sharing

348 G20, "G20 Ministerial Statement on Trade and Digital Economy" at para 2 <https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf> (accessed 30 December 2020).

349 For example, the Russian data protection law: Natalia Gulyaeva, Maria Sedykh & Bret Cohen, "Russian Data Localization Law: First Day in Force and Schedule for Compliance Inspections" *Chronicle of Data Protection* (1 September 2015); and the draft Indian data protection bill: see Ashima Obhan & Vrinda Patodia, "India: Data Protection Or Data Localisation" *Mondaq* (20 January 2020).

350 For example, the Chinese cybersecurity act and data security law: Samuel Yang, "China: Data Localisation" *Global Data Review* (18 December 2020).

351 Tracy Qu, "Didi Cybersecurity Review Expected To Set Precedent For Future 'National Security' Probes Into Data Collection" *South China Morning Post* (5 July 2021).

352 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

353 See ASEAN Telecommunications and Information Technology Ministers Meeting, *Framework on Digital Data Governance* (6 December 2018) Strategic priority 2 on cross border data flows.

Framework[354] is an attempt at a non-regulatory approach to support B2B data-sharing. We can expect to see further developments of ideas that support data-sharing across the domestic economy beyond frameworks. For example, the UK Open Data Institute is piloting the concept of data trusts as an *institutional* approach to data stewardship that may support broader data-sharing across the economy.[355] In the EU, there are proposals for a *regulatory framework* for data-sharing services in their upcoming Data Governance Act[356] to increase data-sharing by building trust in data-sharing intermediaries.[357]

04.107 The use of data for machine learning is another area to watch. The regulation of AI has seized the attention of policy makers. The OECD has published their Principles on AI,[358] which has been adopted by the G20,[359] and the EU has similarly published their Ethics Guidelines for Trustworthy AI[360] ("AI Guidelines"); the United Nations Educational, Scientific and Cultural Organization has embarked on a two-year process to elaborate the first global standard-setting instrument on the ethics of AI in the form of a recommendation.[361] While Singapore has taken a soft-regulatory approach with the publication of its Model AI Governance Framework,[362] the winds blow differently along the corridors in Brussels. The EU has published a proposal for an Artificial Intelligence Act ("AI Act"), which takes a risk-based approach that prohibits specific

354 Available at <https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf> (accessed 30 December 2020).

355 See generally "Data Trusts: Lessons from Three Pilots" *Open Data Institute* (15 April 2019); see also Jack Hardinges, "Data Trusts in 2020" *Open Data Institute* (17 March 2020).

356 See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance* (COM(2020) 767 final, 25 November 2020).

357 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance* (COM(2020) 767 final, 25 November 2020) ch III.

358 Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, 22 May 2019).

359 G20, "G20 Ministerial Statement on Trade and Digital Economy" <https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf> (accessed 24 January 2021).

360 High-Level Expert Group on Artificial Intelligence *Ethics Guidelines for Trustworthy AI* (8 April 2019).

361 "Elaboration of a Recommendation on the Ethics of Artificial Intelligence" *United Nations Educational, Scientific and Cultural Organization* <https://en.unesco.org/artificial-intelligence/ethics> (accessed 24 January 2021).

362 "Artificial Intelligence" Infocomm Media Development Authority <https://www.imda.gov.sg/infocomm-media-landscape/SGDigital/tech-pillars/Artificial-Intelligence> (accessed 24 January 2021).

uses of AI, regulates high-risk AI, imposes transparency obligations for specific AI and encourages voluntary compliance for low or no-risk AI:[363]

(a) The use of AI systems that subliminally manipulate social behaviour, exploit societal vulnerabilities or enable social ranking by public authorities will be prohibited; while the use of AI systems that perform real-time remote biometric public surveillance by law enforcement will be severely restricted.[364]

(b) The proposed AI Act takes key features of the EU AI Guidelines – such as data and data governance, technical documentation, record-keeping, human oversight, and accuracy, robustness and cybersecurity, *etc*[365] – and converts them into regulatory requirements for high-risk AI systems, which are defined as AI systems used in safety components or stand-alone AI systems used in a white-list of situations.[366] The proposed AI Act essentially mandates process documentation,[367] information disclosure,[368] and risks or quality assessments[369] for high-risk AI systems. While explainability is not mandated, accuracy, consistency, robustness and cybersecurity will be;[370] as well as the requirement of human oversight when high-risk AI systems are in use.[371] The proposed AI Act also prescribes conformity assessments as the means for compliance: third-party conformity assessments will be required for AI used in safety components,[372] while internal conformity assessments will be permissible for other stand-alone high-risk AI systems.[373]

(c) Transparency obligations – *viz*, informing individuals when they are interacting with AI systems or output – are mandated for

363 European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (COM(2021) 206 final) ("hereinafter "AI Act").

364 AI Act Art 5.

365 AI Act Title III, Chapter 2.

366 AI Act Art 6, read with Annexes II and III; the white-list of stand-alone high risk AI systems include: (a) real-time biometric surveillance; (b) management and operation of critical infrastructure; (c) assignment and assessment of students in educational and vocational training; (d) employment and management of workers; (e) access to essential public services and benefits or credit scoring; (f) law enforcement; (g) immigration; and (h) administration of justice.

367 AI Act Arts 10–12, 18 and 20.

368 AI Act Arts 13 and 22.

369 AI Act Arts 9 and 17.

370 AI Act Art 15.

371 AI Act Art 14.

372 AI Act Art 6(1).

373 AI Act Art 19 and para 64 of the Preamble.

AI systems that interact with natural persons, or are capable of recognising emotions or biometric information; and deep fakes have to be labelled as such.[374]

(d) AI systems that are not high-risk are not subject to regulation under the AI Act, although EU member states are encouraged to support the adoption of voluntary codes of conduct.[375]

3. Intermediary regulation: Convergence

04.108 Regulation of intermediaries has emerged as a new layer in the schematic for technology regulation. There has been a distinct shift from the protection of Internet intermediaries through immunities and safe harbours, towards regulating their market conduct given their gatekeeper role and the positive network externalities that some Internet intermediaries have achieved. Developments in the regulation of Internet intermediaries look set to continue along its current trajectory and pace. Currently, there is regulatory convergence in the sense that different regulators are bringing their powers to bear on Internet intermediaries.

04.109 Unsurprisingly, *competition* authorities have trained their sights on Internet intermediaries. In the EU, the European Commission has commenced investigating Apple's practices in relation to its app store and Apple Pay rules;[376] and Amazon's use of data from sellers on its marketplace in order to unfairly compete with them in price.[377] Across the Atlantic, the US Senate published a damning report on the anti-competitive practices of big tech.[378] This coincided with the Department of Justice's investigations into Google's monopolistic practices in online search and AdTech;[379] which was followed by the Federal Trade Commission's anti-trust investigations into Facebook's market conduct in buying up rivals in order to squash competition.[380] In China, Alibaba has been hit with a massive antitrust fine for anticompetitive

374 AI Act Art 52.
375 AI Act Art 69.
376 Tom Warren, "EU Opens Apple Antitrust Investigations into App Store and Apple Pay Practices" *The Verge* (16 June 2020).
377 Adam Satariano, "Amazon Charged with Antitrust Violations by European Regulators" *New York Times* (10 November 2020).
378 Shirin Ghaffary & Jason Del Rey, "The Big Tech Antitrust Report Has One Big Conclusion: Amazon, Apple, Facebook, and Google Are Anti-competitive" *Vox* (6 October 2020).
379 Cecilia Kang, "US Accuses Google of Illegally Protecting Monopoly" *New York Times* (20 October 2020).
380 Cecilia Kang & Mike Isaac, "US and States Say Facebook Illegally Crushed Competition" *New York Times* (9 December 2020).

practices, including its practice of preventing merchants from selling their goods on other platforms.[381] In recognition that the gatekeeping role of Internet intermediaries gives them outsized market power even before breaching the thresholds traditionally established by competition law, the EU intends to rely on a system for designating core platform providers in order to bring them within regulatory remit.[382]

04.110 Apart from competition law, Internet intermediaries are also facing pressure on the *copyright* front. The EU Copyright Directive[383] strengthened the bargaining powers of authors and publishers against Internet intermediaries, by: (a) giving publishers new rights for reproduction and communication to the public for the online use of their press publications;[384] (b) clarifying that online content-sharing intermediaries perform acts of communication or making available to the public when they give public access to copyrighted works hosted on their platform; and (c) imposing an obligation on online content-sharing intermediaries to obtain authorisation from rights holders by concluding a licensing agreement.[385] Thus in France, Google has had to enter into an agreement with French news organisations to pay new sites for using snippets.[386] The Australian approach to sustain its news industry is somewhat different. It amended its Competition and Consumer Act 2010[387] to mandate information disclosure[388] by designated Internet intermediaries against whom Australian news businesses have a significant bargaining power imbalance.[389] Processes are established for bargaining and, if unsuccessful, mediation for the *licensing* of news content, with the additional avenue of arbitration for *remuneration* to be paid for news content.[390] With the enactment of the new law, both

381 Raymond Zhong, "China Fines Alibaba $2.8 Billion in Landmark Antitrust Case" *New York Times* (9 April 2021).
382 See para 04.111; see also European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)* (COM(2020) 842 final, 15 December 2020) at pp 3 and 4.
383 See para 04.090. See also Matt Reynolds, "What Is Article 13? The EU's Divisive New Copyright Plan Explained" *Wired* (24 May 2019).
384 Copyright Directive Art 15.
385 Copyright Directive Art 17(1).
386 Timothy B Lee, "Google: We'll Shut Down Australian Search before We Pay News Sites for Links" *Ars Technica* (23 January 2021).
387 Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021 (Act No 21 of 2021) (Aus).
388 News Media and Digital Platforms Mandatory Bargaining Code, sections 52R and 52S.
389 News Media and Digital Platforms Mandatory Bargaining Code, section 52E.
390 News Media and Digital Platforms Mandatory Bargaining Code, Divisions 6 (bargaining & mediation) and 7 (arbitration).

Google[391] and Facebook[392] have entered into licensing agreements for Australian news content.

04.111 Policy makers in the EU have eschewed competition law in favour of *sui generis* regulations. Following the introduction of the P2B Regulation,[393] there are proposals to upgrade the E-Commerce Directive and extend the regulatory mandate of Brussels in the digital services market.[394] The proposed regulations – the Digital Services Act and the Digital Markets Act[395] – segments Internet intermediaries into four tiers with increasing regulatory obligations: micro or small enterprises, general Internet intermediaries, designated very large online platforms and designated core platform providers. The P2B Regulation continues to apply to Internet intermediaries providing online intermediation services to business users as *lex specialis*.[396]

04.112 The proposed Digital Services Act upgrades the immunity and safe harbour protections of intermediaries from the E-Commerce Directive into EU regulations,[397] while reinforcing the principle that Internet intermediaries have no general obligation to monitor their platform.[398] However, in a shift away from passive neutrality, Internet intermediaries (that are not micro or small enterprises) will soon be expected to introduce technical or other measures to take action on flagged illegal content on their platform,[399] and also to notify law enforcement if they have information giving rise to suspicion of serious criminal offence that threatens life or safety.[400] Other new regulatory obligations are introduced in the following areas:

(a) First, Internet intermediaries will have clear duties to take action against illegal content and provide information, when requested to do so by judicial or administrative authorities.[401] The duty to take action echoes the access blocking orders discussed above.[402]

(b) Second, transparency requirements similar to the P2B Regulations will also be prescribed in the following areas:
   (i) all Internet intermediaries have to be transparent about terms and conditions that restrict use of their services;[403]
   (ii) Internet intermediaries that are not micro and small enterprises will have to be transparent about the main parameters used to determine how online advertisements are displayed to recipients;[404] and
   (iii) designated very large online platforms[405] will have (A) additional parametric transparency obligations for recommendation engines that they use, and (B) the obligation to provide APIs to allow access to an archive of metadata relating to online advertisements that had been displayed on their platform.[406]

(c) Third, in order to manage systemic risks, designated very large online platforms will have obligations to conduct risk assessments and implement measures to mitigate identified risks; and be subject to compliance audits.[407]

04.113 The proposed Digital Markets Act will apply only to designated core platform providers who occupy a gatekeeping role for business users and consumers, have significant impact and enjoy entrenched and durable positions in their operations.[408] Internet intermediaries (including online search engines) are one class of gatekeepers that will come within its ambit. The proposed Digital Markets Act could be viewed as complementary to the P2B Regulation, extending beyond the latter's transparency requirements by prescribing fair trading practices. Thereby, establishing a higher tier of regulatory obligations for designated gatekeepers that includes:

(a) requiring express consent from data subjects before gatekeepers may combine personal data of customers obtained from other sources;[409]

391 Damien Cave, "Google Is Suddenly Paying for News in Australia. What About Everywhere Else?" *New York Times* (18 February 2021).
392 Livia Albeck-Ripka, "Facebook Agrees to Pay for Murdoch's Australia News Content" *New York Times* (16 March 2021).
393 See para 04.079.
394 Billy Perrigo, "How the EU's Sweeping New Regulations against Big Tech Could Have an Impact beyond Europe" *Time* (15 December 2020); see also Digital Services Act, Chapter IV Implementation, cooperation, sanctions and enforcement, and Digital Markets Act, Chapter IV Market Investigation.
395 See para 04.080.
396 Digital Services Act at p 4.
397 Digital Services Act Arts 3–5.
398 Digital Services Act Art 7.
399 Digital Services Act Art 19.
400 Digital Services Act Art 21.
401 Digital Services Act Arts 8 and 9.
402 See para 04.091.
403 Digital Services Act Art 12.
404 Digital Services Act Art 24.
405 Threshold for designation is 45 million users or 10% of EU population: Digital Services Act Art 25(2).
406 Digital Services Act Arts 29 and 30.
407 Digital Services Act Arts 26–28.
408 Digital Markets Act Art 3.
409 Digital Markets Act Art 5(a).

(b) requiring gatekeepers to allow merchants to offer the same products or services on different terms through other platforms,[410] and allowing merchants and end-users to conclude transactions off-platform;[411]

(c) forestall unfair competition with merchants by preventing gatekeepers from using data generated by merchants' (and their customers') activities on their platforms, unless the data is made publicly available,[412] and proscribing discriminatory search ranking that favours similar products or services offered by gatekeepers (or their affiliates);[413] and

(d) provide access to and portability of data generated by merchants' business activity or personal data generated by their customers' transactions,[414] including providing to third-party online search engines anonymised ranking and usage data generated by activities on their platform.[415]

G. CONCLUSION

04.114 The traditional content *versus* carriage paradigm has evolved to provide greater definitions of the contours within each layer, with the emergence of intermediaries as a new layer. Regulation of the carriage layer is perhaps the most mature, *viz* infrastructure regulations for the provision of telecom services and supply of telecom equipment. The recent addendum with the introduction of regulations for cybersecurity is not earth-shaking, but should be seen as another rachet in the historical regulation of network security, expanded to critical information infrastructure. The ongoing deployment of 5G networks rests on a stable regulatory framework, which has proved to be sufficiently malleable and responsive through successive generations of mobile network technologies. Its higher bandwidth and lower latency promise to push computing to the edge of the network, enabling use cases in areas such as smart estates, smart manufacturing, and urban mobility.

04.115 The intermediaries layer is undergoing a tectonic shift away from historical protections from liability for Internet intermediaries, towards regulation of their conduct *vis-à-vis* users of their platform. The elements of these new and draft regulations are picked from the more traditional domains of competition, fair trading, and consumer protection law, but

410 Digital Markets Act Art 5(b).
411 Digital Markets Act Art 5(c).
412 Digital Markets Act Art 6(1)(a).
413 Digital Markets Act Art 6(1)(d).
414 Digital Markets Act Arts 6(1)(h) and 6(1)(i).
415 Digital Markets Act Art 6(1)(k).

adapted for the relationships and dynamics of this new intermediaries layer. New elements are added, for example, in parametric (if not algorithmic) transparency, and access to and portability of transactional data. The stage is set and the forthcoming act is expected to play out in the immediate term.

04.116 In the medium term, the regulatory challenges that are expected to emerge are likely to be in the digital infrastructure and digital utilities strata of the content layer. First, the lines in the sand for the net neutrality debate could be redrawn with a new administration in the US. Second, we can expect thickening in the sectoral regulation of digital services, as we have witnessed for e-payments and digital identity and trust services; and as we speak, we can already see the frisson for regulating AI. Third, data regulation can be expected to extend beyond personal data into businesses' activity data and public data, as well as move into regulating the instruments or institutions for data sharing: for example, data altruism, data trusts and data intermediaries or exchanges.

04.117 In providing a framework to understand the regulation of technology, this chapter has also charted the evolution and ongoing development in this area. We can expect the contours within each layer to see better definition, as emergent issues take their form and regulatory responses are crafted. Such is the beauty and attraction of a constantly evolving area of TMT law like technology regulation: as technology advances, new business models emerge and the regulatory framework responds.

Content	**Online content** (*eg*, blogs, online publications, social media)	**Transactional services** (*eg*, online retail)	**Software-as-a-service** (*eg*, online gaming)
	Digital utilities (*eg*, identity & trust services, e-payment services)		
	Digital infrastructure (*eg*, broadband and IoT)		
Intermediaries	**Mere conduit**	**System caching**	**Hosting and linking**
Carriage	**Services-based operator** (dominant/non-dominant)		
	Facilities-based operator (public telecom licensee; dominant/non-dominant)		
	Spectrum	**Telephone number**	**Satellite orbital slot**

Table 4. A schematic of the regulation of technology

Further reading

Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press, 4th Ed, 2019) chs 4, 7.3 and 12.3

Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 5th Ed, 2016) chs 1 and 3

Ian Walden, *Telecommunications Law and Regulation* (Oxford University Press, 4th Ed, 2012)

CHAPTER 5

Practice of Law – Courts

By Justice Aedit Abdullah and Tan Ken Hwee

A. INTRODUCTION

05.001 Courts can play a significant role in innovation and the adoption and development of technology in the legal system: the courts are still at the centre of much dispute resolution, and are where persons most associate with getting wrongs righted, and rights enforced. In recognition of that centrality, the courts in Singapore, under the leadership of the various chief justices, have always striven to be open to technology, and to help push, where necessary, the adoption of new technologies and tools. Courts that are ill-equipped, or which use antiquated systems or processes, not only impede their own efficiency but also endanger access to justice, the achievement of just outcomes in disputes, and weigh down the entire legal system. It is with that responsibility in mind that the Judiciary in Singapore has always aimed to never be complacent and to always aim to improve its systems.

B. HISTORY

05.002 In 1979, a Committee for National Computerisation was created to help Singapore implement a computerisation programme for the whole of the Government. A five-year National Computerisation Plan was proposed. This in turn evolved into the Civil Service Computerisation Programme, and led to the establishment of the National Computer Board.[1] Various large scale plans followed, including the IT2000 Vision of an Intelligent Island, the National IT Plan, the e-Commerce Hotbed

1 See generally, Lulin Reutens, *Innovationation: 25 Years of Infocomm in Singapore – The Big Switch* vol 1 (Infocomm Development Authority of Singapore, 2006); National Computer Board Act (Cap 195, 1985 Rev Ed) (repealed).