palgrave pivot

Global Internet Governance

Influences from Malaysia and Singapore

Susan Leong
Terence Lee

palgrave macmillan

Global Internet Governance

"Putting aside all the technical jargon regarding the internet, the key question that worries governments, civil society and the citizens of the world generally is the question of its governance. This volume addresses this concern head-on. Its focus on the experiences of Malaysia and Singapore – two prominent Southeast Asian countries inextricably tied up with the technology – provides fresh insights into the debates surrounding internet oversight, accountability and legitimacy. This well-researched and theoretically-informed volume by prolific and experienced media academics, Susan Leong and Terence Lee, is timely, when the world is reeling from the effects of the COVID-19 pandemic and the (in)accuracy of information provided. A time, indeed, when the governance of the internet is vital."

—Professor Zaharom Nain, *Nottingham University, Malaysia*

"This book is a useful guide for countries caught in the middle of our contemporary information technology trade war. It outlines the history of two nations – Malaysia and Singapore – that escaped the binary trap of US-China Internet Governance: US-led multistakeholderism vs China-backed multilateralism. It proposes a hybrid model that is glocal, adaptive, and concurrently neoliberal and authoritarian. Susan Leong and Terence Lee review the historical situations and practices of Malaysia and Singapore over three decades by following a third path, a hybrid internet governance model, that seems particularly well-suited for a global post-pandemic future."

—Associate Professor Weiyu Zhang, *National University of Singapore*

"Internet governance remains in crisis, without a clear roadmap for the future — so where do we turn? This brilliant and timely new book by Susan Leong and Terence Lee urges us to look beyond the fixation with US or China, or multistakeholderism or multilateralism as the default options. They propose a 'hybrid model' as the way forward, showing how this has unfolded, warts and all, in the dynamic Southeast Asian region in the cases of Singapore and Malaysia. Their rich and persuasive account underscores the importance of understanding actually-existing Internet governance as the foundation to decolonising, debugging, and reforming Internet governance for all. This book is indispensable reading for anyone concerned about the crossroads in communication and technology governance and policy today."

—Professor Gerard Goggin, *Nanyang Technological University, Singapore*

Susan Leong · Terence Lee

Global Internet Governance

Influences from Malaysia and Singapore

palgrave
macmillan

Susan Leong
School of Arts and Social Sciences
Monash University Malaysia
Bandar Sunway, Selangor, Malaysia

Terence Lee
College of Arts, Business, Law and Social Sciences
Murdoch University
Murdoch, WA, Australia

ISBN 978-981-15-9923-1 ISBN 978-981-15-9924-8 (eBook)
https://doi.org/10.1007/978-981-15-9924-8

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover illustration: © John Rawsterne/patternhead.com

This Palgrave Pivot imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

To my beloved mother, Elsie Woo (1939–2018)
—Susan Leong

To the memory of my father, Eric Lee (1943–2019)
—Terence Lee

Acknowledgments

None of this would have been possible without the many fruitful discussions and snatched conversations along corridors with colleagues in Australia, Singapore and Malaysia. The authors wish specially to thank Ang Peng Hwa, Tania Lim, Emma Baulch, Zhang Weiyu, Michael Keane, Zaharom Nain and Helen Nesadurai for their collegiality and support.

We would also like to express our gratitude to the School of Arts and Social Science at Monash University of Malaysia for funding parts of the research work that went into this project.

Finally, to our family and friends who, as always, provide much of the most important day-to-day encouragement, words cannot fully express the thanks we have for your presence in our lives.

The later stages of this book's development took place in the shadow of the COVID-19 pandemic. Without the use of the Internet, we would have been hard pushed to collaborate as efficiently across Perth and Kuala Lumpur as we did. In this sense, then, this book is as much a product of the interoperability of the Internet as it is about global Internet governance.

Contents

1 Introduction—A Pair of Governance Models or More? 1
Bibliography 9

2 The Internet in Malaysia (1990–2008): Visions of Technological Splendour 13
The Multimedia Super Corridor (MSC) to Open Dissent 18
Confidence Unfolding/Unfurling 21
Hybridising 25
Bibliography 28

3 The Internet in Singapore: From 'Intelligent Island' to 'Smart Nation' 31
Introduction 32
Internet Development in Singapore: The Historical, Political and Ideological 34
The 'Intelligent' Era: 1990s to 2010s 37
The Digital Era: iN2015 to 'Smart Nation' 42
Digital Smarts 44
Conclusion 47
Bibliography 48

4 Internet Governance—The Malaysia Way 51
If a Crime Is Committed … 53

China's Courtship and Anti-Westernism Redux 56
Internet Sovereignty 60
Private Platforms, Public Oversight 62
Bibliography 66

5 Internet Governance: Singapore's Regulatory Influence 71
Introduction: Singapore's Governance Setting 72
The Light-Touch Principle 75
Auto-Regulation: Disciplining the Internet 81
Conclusion: The Local Is Global 85
Bibliography 88

6 Towards a Hybrid Understanding of Internet Governance: Some Concluding Thoughts 91
Introduction 92
Glocalisation: Hybridising the Global 95
Conclusion 97
Bibliography 100

Index 103

CHAPTER 1

Introduction—A Pair of Governance Models or More?

Abstract This introductory chapter frames the background to the current debate on internet governance, which consists of intersecting developments and historical conditions. It looks at the legacy of the multistakeholder model that was developed alongside the co-invention of the Internet by Anglo-American scientists, technologists and enthusiasts from the 1960s. It accounts for the unexpected mass take-up of the internet across non-English speaking and non-democratic spheres from the mid-1990s. It then brings to bear China's emphatic support for the multilateral model of internet governance since 2010. Although many of the Internet's earliest adopters envisioned it being a democratising force for democratisation, they failed to realise that the internet's spread could equally have the opposite effect of curbing liberal discourses and diminishing humanitarian values. It sets the scene to examine how two of the smaller Southeast Asian countries, Malaysia and Singapore, have governed the Internet in their respective domestic spaces over the past three decades, and what influences and lessons they hold for global internet governance.

Keywords Interoperability · Scale · Standards · Techno-nationalism · Hybrid configurations

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

S. Leong and T. Lee, *Global Internet Governance*,
https://doi.org/10.1007/978-981-15-9924-8_1

> 10 years the top 10 internet companies were American. Today, 6 of the top 10 are Chinese. And this is about what kind of internet we want. Do we want an internet that's based on the values of free expression or where the government gets to decide what's allowed to be said? You know, do we want an internet where the individuals are the players or where the government itself is a major player? … America has de facto run the internet and it's based on American values because the companies were American and if that shifts to China, we will have a very different internet. . .What comes behind breaking up the US tech companies is not another US tech company right now. What clearly comes behind if you look at the numbers and the usage and the support they have, are Chinese companies. And that's a decision we have to make as a company, as a society.
>
> Sheryl Sandberg, COO, Facebook.[1]

On the face of it, Sandberg seems to have summed up the current state of the debate over internet governance (henceforth, IG). Do we maintain, on the one hand, that the internet should continue as it is with the individual right of freedom of expression enshrined as a guiding principle or can we countenance, on the other hand, a future where national governments determine how the internet is governed? The choice looks stark and for many the chasm between multistakeholderism and multilaterialism or what Nazli and Clark dub the distributed U.S. and the centrist China approach (Nazli and Clark 2013), makes the choice a foregone conclusion (Bradshaw and Denardis 2018; Carr 2015; Mueller 2017). Apart from those who for one reason or another are without choice, there are few adults who would opt to be more rather than less restricted in their use of a system of communication, trade and exchange than need be. The free world must rise to defend its liberalism against the creeping "neo-authoritarian" credo of Chinese communism (Jiang 2013). Indeed, as Singer and Friedman write, "many are now framing the US-Chinese relationship in cyberspace as a digital echo of that between the United States and USSR during the Cold War" (Singer and Friedman 2014). Whatever their stance what scholars of IG agree on is this: the internet is now so integrated into our daily lives (in the developing and developed world) and hence, socially, culturally, politically and economically influential that to leave the question of how the system(s) is governed

[1] A Conversation with Sheryl Sandberg, *The Future of the Internet*. Aired on Bloomberg Channel, 15 December 2019. https://www.bloomberg.com/news/videos/2019-11-27/a-conversation-with-sheryl-sandberg-video (accessed 6 January 2020).

to goodwill, ad hoc software engineering and make-do protocols is akin to misplaced trust. To decide on how the internet is governed we need, to paraphrase Berners-Lee, inventor of the World Wide Web, to "ensure that the society we build with the [Internet] is of the sort we intend" (Berners-Lee and Fischetti 1999, p. 133). To not decide is to leave the continuing function of the Internet to the "relatively flat, open, sprawling, ad hoc, and amorphous" structure that has worked so far (Bygrave and Michaelsen 2009, p. 92).

Where, you ask, is the harm in that? If the Internet had retained its modest size as an intertwined network of networks, shared between the military, engineers, scientists and academics in the Anglocentric world, rather than global network it is now, the task of IG would not have needed to stretch to much more than addressing "technical design and administrative issues" (DeNardis 2014, p. 20). The problem of how to go about IG begins, then, with an issue of scale. With the masses of data we generate, create, consume and circulate daily via the Internet, a lack of genuine oversight over how the data – personal, public and shared – is handled leaves individuals, communities, nations and a significant portion of the world vulnerable to mischief, manipulation and harm (Gillespie 2018) as demonstrated by the revelations about Cambridge Analytica (Dyer-Witheford and Matviyenko 2019, p. 1) and, those of Edward Snowden and Chelsea Manning (Van Cleave 2013). Data breaches and compromised networks are what cybersecurity fears and measures seek to eradicate. The European Union's General Data Protection Regulation (GDPR) enacted in 2018 is one initiative devised to guard the privacy of Europe's citizens.[2] At the very least, the GDPR should deter mishandling of personal data yet as the EU's own survey of small businesses found recently the gap between awareness and knowledge of the regulation, and its enforcement is wider than imagined.[3] The EU might have put a check on the compromise of customer and user data by big businesses (Kazzini 2019), still, in practice, what would be the effect of businesses separating the personal data of EU citizens from that of others? The experiment conducted and featured by the *New York Times* in 2018 (Singer and Prashant 2018) demonstrated the gulf between the amount of personal

[2] General Data Protection Regulation (GDPR) Compliance Guidelines. (2020). https://gdpr.eu/ (accessed 6 January 2020).

[3] GDPR Small Business Survey. (2019). https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf (accessed 6 January 2020).

data on themselves individuals can obtain from digital platforms Amazon, Facebook, Google, LinkedIn, Twitter, their mobile providers and digital marketing analytics companies from the UK and the US. Microsoft has gotten round the problem by placing customers in control of their own data through a privacy dashboard (Brill 2018). The next issue that arises is how GDPR compliance might affect the interoperability of the Internet.

Interoperability is the mantra of every engineer whose designs are intended to enable the flow, be that of people, electricity and information. To compromise compatibility between the various parts and layers, in both soft and hardware terms, is to place the seamless function of the somewhat haphazardly governed Internet in jeopardy. Broadly speaking, interoperabilty rests on all parties concerned agreeing upon, setting and adhering to said standards to ensure differences are smoothed out. Transport and communication technologies were among the earliest beneficiaries of interoperability. From the first transcontinental railways (Harding 1845) and radio systems to telephone networks, interoperability hinges on faithful application of standards. Interoperability facilitates scaling. What is often obscured when standards are established, is the advantage accrued to whoever leads and establishes the standard. These days most technical standards are set by corporations based in nation-states rather than individuals so the advantage of being the originator also extends to their country of origin. This is why the U.S. government is adamant that 5G (fifth generational) technology developed by China's Huawei should not be established as the standard. Putting aside the generational leaps 5G would bring to all digital networks and users, the economic advantages of being the standard setter are enormous. As Fägersten and Rühlig (2019, p. 3) from the Swedish Institute of International Affairs observe:

> Technical standard setting might appear to be a consensual search for the technically most appropriate solution leading to absolute gains such as lower transaction costs, more efficient markets and subsequent economic growth. After all, the interoperability of products should facilitate economic growth and trade. In contemporary world affairs, however, technical standardization is more and more turning into a crucial arena for political and commercial conflict.

Whipping up concerns that wiretaps typically built into technical systems to satisfy U.S. law enforcement requirements would give Huawei (and