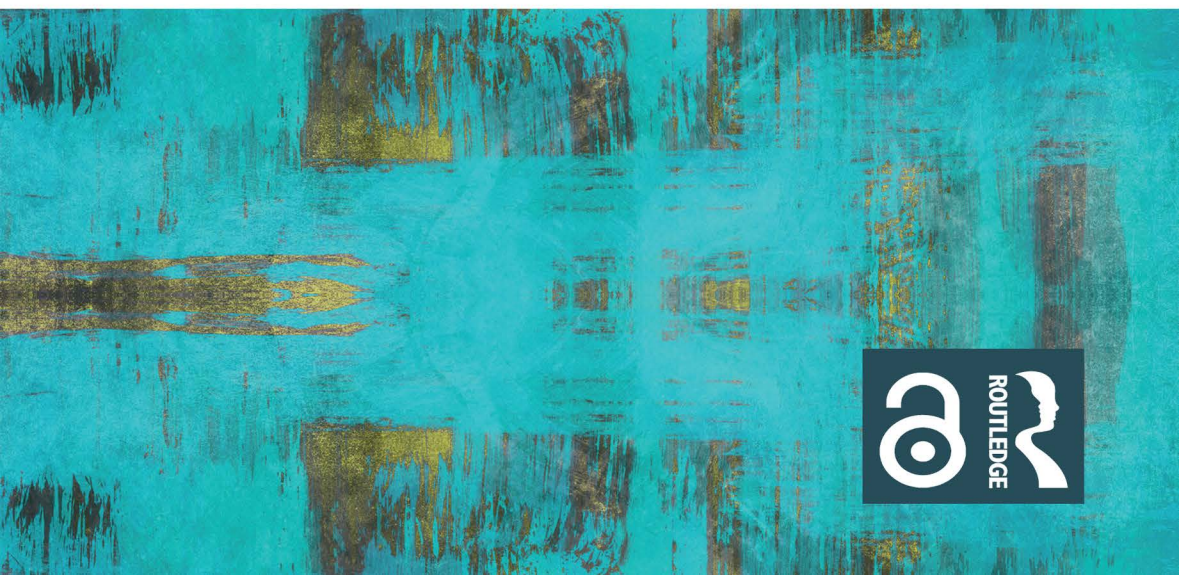
Routledge Global Cooperation Series

POWER AND AUTHORITY IN INTERNET GOVERNANCE

RETURN OF THE STATE?

Edited by
Blayne Haggart, Natasha Tusikov
and Jan Aart Scholte



Power and Authority in Internet Governance

Power and Authority in Internet Governance investigates the hotly contested role of the state in today's digital society. The book asks: Is the state "back" in internet regulation? If so, what forms are state involvement taking, and with what consequences for the future?

The volume includes case studies from across the world and addresses a wide range of issues regarding internet infrastructure, data and content. The book pushes the debate beyond a simplistic dichotomy between liberalism and authoritarianism in order to consider also greater state involvement based on values of democracy and human rights. Seeing internet governance as a complex arena where power is contested among diverse non-state and state actors across local, national, regional and global scales, the book offers a critical and nuanced discussion of how the internet is governed – and how it should be governed.

Power and Authority in Internet Governance provides an important resource for researchers across international relations, global governance, science and technology studies and law as well as policymakers and analysts concerned with regulating the global internet.

Blayne Haggart is Associate Professor of Political Science at Brock University in St. Catharines, Canada, and Research Fellow, Käte Hamburger Kolleg/Centre for Global Cooperation Research University of Duisburg-Essen, Germany.

Natasha Tusikov is Assistant Professor of Criminology at York University in Toronto and a visiting fellow with the School of Regulation and Global Governance (RegNet) at the Australian National University.

Jan Aart Scholte is Chair of Global Transformations and Governance Challenges at Leiden University and Co-Director of the Centre for Global Cooperation Research at the University of Duisburg-Essen.

Routledge Global Cooperation Series

The *Routledge Global Cooperation* series develops innovative approaches to one of the most pressing questions of our time – how to achieve cooperation in a culturally diverse and politically contested global world?

Many key contemporary problems such as climate change and forced migration require intensified cooperation on a global scale. Accelerated globalisation processes have led to an ever-growing interconnectedness of markets, states, societies and individuals. Many of today's problems cannot be solved by nation states alone and require intensified cooperation at the local, national, regional and global level to tackle current and looming global crises.

Series Editors:
Tobias Debiel, Dirk Messner, Sigrid Quack and Jan Aart Scholte are Co-Directors of the Käte Hamburger Kolleg / Centre for Global Cooperation Research, University of Duisburg-Essen, Germany. Their research areas include climate change and sustainable development, global governance, internet governance and peacebuilding. Tobias Debiel is Professor of International Relations and Development Policy at the University of Duisburg-Essen and Director of the Institute for Development and Peace in Duisburg, Germany. Dirk Messner is President of the German Environment Agency (Umweltbundesamt – UBA). Sigrid Quack is Professor of Sociology at the University of Duisburg-Essen, Germany. Jan Aart Scholte is Professor of Global Transformations and Governance Challenges at Leiden University, Netherlands.

Patricia Rinck is editorial manager of the series at the Centre for Global Cooperation Research.

www.routledge.com/Routledge-Global-Cooperation-Series/book-series/RGC

Titles:

China's New Role in African Politics
From Non-Intervention towards Stabilization?
Edited by Christof Hartmann and Nele Noesselt

Hegemony and World Order
Reimagining Power in Global Politics
Edited by Piotr Dutkiewicz, Tom Casier and Jan Aart Scholte

Power and Authority in Internet Governance
Return of the State?
Edited by Blayne Haggart, Natasha Tusikov and Jan Aart Scholte

Power and Authority in Internet Governance

Return of the State?

Edited by Blayne Haggart, Natasha Tusikov and Jan Aart Scholte

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Centre for
Global
Cooperation
Research

SPONSORED BY THE
Federal Ministry
of Education
and Research

First published 2021
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book has been requested

ISBN: 978-0-367-44203-3 (hbk)
ISBN: 978-1-003-00830-9 (ebk)

DOI: 10.4324/9781003008309

This work and its open access publication has been supported by the Federal Ministry of Education and Research (BMBF) in the context of its funding of the Käte Hamburger Kolleg/Centre for Global Cooperation Research at the University of Duisburg-Essen (grant number 01UK1810).

Contents

Figures

Tables

Contributors

Olga Cavalli is an internet leader whose work has been fundamental for enhancing a relevant participation of Latin America and the Caribbean in internet governance. She is the Co-founder and the Academic Director of SSIG, the South School on Internet Governance, and ARGENSIG, the Argentina School on Internet Governance. Both schools grant fellowships for attending an intensive training on internet governance, organised in different countries of the Americas. She co-edited the book *Internet Governance and Regulations in Latin America*, published in commemoration of the 10th anniversary of the South School on Internet Governance and available online in three languages. Olga is also an active member of the Internet Society (ISOC), serving as a member of the ISOC Board of Trustees and in the ISOC Foundation Board. She is an active participant in the Internet Corporation for Assigned Names and Numbers (ICANN), where she served as Vice Chair of the Governmental Advisor Committee and Vice Chair of the Generic Names Supporting Organization, among other activities. Olga is a professor at the Economic School of the University of Buenos Aires, and she has a PhD in business direction, a master's degree in business administration, a master's degree in telecommunications regulation, and a degree in electronic and electric engineering.

Jean-Marie Chenou is Associate Professor at the Department of Political Science at the Universidad de los Andes in Bogotá, Colombia, where he has worked since 2016. He holds a PhD in political science from the University of Lausanne (Switzerland) and an MA in international relations from the Université Panthéon-Assas (Paris II). His research focuses on internet governance and the global political economy of the digital age.

Dan Ciuriak is Senior Fellow with the Centre for International Governance Innovation (Waterloo, Canada), where he writes on the economics of the data-driven economy and the international trade aspects of the digital transformation. He is also a distinguished fellow with the Asia Pacific Foundation of Canada (Vancouver), holds a fellowship with the C.D. Howe Institute (Toronto) and has a consulting practice specialising in quantitative trade analysis. Previously, he had a 31-year career with the Government of Canada, retiring as Deputy Chief

Economist at Global Affairs Canada. He is widely published and comments frequently in the media.

Luã Fergus Cruz is a researcher at the Brazilian Institute of Consumer Protection (*Instituto Brasileiro de Defesa do Consumidor*, IDEC). He holds a degree in law from Fluminense Federal University (UFF), having participated, in 2016, in the Padre António Vieira Program at New University of Lisbon (NOVA). In 2019, he was Google Policy Fellow at Foundation for Press Freedom (FLIP), based in Bogotá, Colombia. Before joining IDEC, Luã was a research assistant at the Center for Technology & Society at FGV Law School (CTS-FGV) and CyberBRICS project's Community Manager.

Blayne Haggart is Associate Professor of Political Science at Brock University in St. Catharines, Canada, and Senior Research Fellow, Käte Hamburger Kolleg/Centre for Global Cooperation Research University of Duisburg-Essen, Germany. He recently completed a fellowship at the Weizenbaum Institute for the Networked Society in Berlin, Germany. His current research focuses on the political economy of knowledge governance. He is the author of *Copyright: The Global Politics of Digital Copyright Reform* (University of Toronto Press, 2014) and is co-editor of *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (Palgrave Macmillan, 2019). His work has been published in leading academic journals, including the *Canadian Journal of Political Science*, the *Journal of Information Policy* and *Policy & Internet*.

Lianrui Jia is a postdoctoral researcher in the Department of Arts, Culture and Media at University of Toronto Scarborough. She holds a PhD in Communication and Culture from York University with a dissertation that looks at the tripartite dynamics between state, capital and internet companies in shaping the globalisation of internet industry in China. Her research areas are digital platforms, political economy and internet policy and regulation, with a regional focus on China and Canada. She is interested in the interplay between politics and economy: the role of the state, capital and private sector in shaping the media system and regulatory regime.

Ting Luo is Senior Lecturer of Political Communication at Manchester Metropolitan University (MMU). Before joining the MMU faculty, she was a postdoctoral fellow of the European Research Council–funded research project "Authoritarianism 2.0: The Internet, Political Discussion, and Authoritarian Rule in China" at Leiden University and at Hertie School, Berlin. She received her PhD in government from the London School of Economics. Her research interests include comparative politics with a specialisation on China, digital politics, elections and democratisation.

Aofei Lv is a research associate at the School of Social and Political Sciences, University of Glasgow. Previously, she was a postdoctoral fellow at the University of Amsterdam as part of the European Research Council–funded research

project on "Authoritarianism in a Global Age". She is a comparative political scientist and specialises in Chinese politics, digital politics and public policy. She received her PhD in politics from the University of Glasgow.

Maria Ptashkina is an economics PhD candidate at University Pompeu Fabra, Barcelona, Spain. Her main research interests include macroeconomics, international economics and trade policy. She is a former fellow at the International Center for Trade and Sustainable Development and former delegate from the Russian Federation to the Asia-Pacific Economic Cooperation Forum. Maria is a former member of intergovernmental policy research groups on issues related to international trade and investment (the Group of Twenty, BRICS [Brazil, Russia, India, China and South Africa] and the One Belt, One Road initiative).

Jhessica Reia is currently appointed as Andrew W. Mellon Postdoctoral Researcher in the Department of Art History and Communication Studies at McGill University. Reia holds a PhD and an MA in communication studies from the Federal University of Rio de Janeiro and a BA in public policy from the University of Sao Paulo. Prior to coming to McGill, Reia was a lecturer and project manager at the Center for Technology and Society at FGV Law School from 2011 to 2019. Reia is the BMO Postdoctoral Fellow (2020–2021) at the Centre for Interdisciplinary Research on Montreal, responsible for the project "Smartness after Dark: Understanding Nightlife Governance and Urban Intelligence in Montreal". Reia is a member of the Conseil de Nuit de MTL 24/24 (2020–2022) and former visiting researcher at the McGill Institute for the Study of Canada (2015–2016). Current research interests include urban governance, smart cities, nighttime policy and piracy.

Julia Rone is a postdoctoral researcher at The Minderoo Centre for Technology and Democracy at CRASSH, University of Cambridge. She has a PhD from the European University Institute in Florence with a thesis on mobilisations against free trade agreements. She has taught and supervised at the University of Cambridge, University of Florence, University of Sofia and the Heinrich Heine University in Düsseldorf. In 2018, she was a visiting fellow at the Weizenbaum Institute for the Networked Society in Berlin and the Centre for Advanced Internet Studies in Bochum. As a Wiener-Anspach fellow in 2019–2020, she explored contestations over sovereignty in Belgium, Poland and the UK. She has written on hacktivism, far right media activism and, more recently, on conflicts of sovereignty in the European Union.

Mauro Santaniello is a researcher at the Department of Political and Social Studies of the University of Salerno. His research focuses on internet governance, policy and regulation. He is Adjunct Professor of Digital Policy and Internet Governance and has led research units within several projects on digital democracy in Europe (FIRB 2013), internet governance and democratic innovation (PRIN 2015), and monocratisation in digital policies (PRIN 2017). He is a co-founder of the Internet & Communication Policy Centre. He has published articles about the interplay between digital networks and political,

economic and social processes. Prior to his work in academia, he was a director of communication and technological innovations in the Italian public administration, where he designed and implemented policies for digital inclusion, e-participation and e-government.

Jan Aart Scholte is Chair of Global Transformations and Governance Challenges at Leiden University and Co-Director of the Centre for Global Cooperation Research at the University of Duisburg-Essen. His research covers globalisation, global governance, civil society engagement of global politics, legitimacy in global governance, and global democracy. In the internet area, he was an external advisor to the IANA transition in 2014–2016 and currently leads a project on legitimacy in multistakeholder governance at ICANN.

Ilona Stadnik is Assistant Professor at the Saint Petersburg State University, School of International Relations. In 2018–2019, she was a Fulbright visiting researcher at Georgia Institute of Technology, School of Public Policy, the home of the Internet Governance Project. Her research covers international cyber norm-making, Russia–U.S. relations in the cybersecurity field, and global internet governance. Ilona is a regular participant and speaker at major cybersecurity events such as the United Nations Internet Governance Forum (IGF), CyFy conference and the European Dialogue on Internet Governance (EuroDIG). She has written on international cybersecurity regimes and has been invited to contribute to an edited volume of the *Handbook on Cybersecurity*, covering the Russian cybersecurity strategy. Previously, Ilona worked as a researcher for the Institute of World Economy and International Relations of the Russian Academy of Sciences (IMEMO) and PIR Centre.

Niels ten Oever is a postdoctoral researcher with the 'Making the hidden visible: Co-designing for public values in standards-making and governance' project at the Media Studies Department at the University of Amsterdam. He is also a postdoctoral scholar with the Communications Department at Texas A&M University, research fellow with the Centre for Internet and Human Rights at the European University Viadrina, and associated scholar with the Centro de Tecnologia e Sociedade at the Fundação Getúlio Vargas. His research focuses on how norms, such as human rights, get inscribed, resisted and subverted in the internet infrastructure through its transnational governance. While writing his PhD, 'Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure', Niels was affiliated with the DATACTIVE Research Group at the Media Studies and Political Science department at the University of Amsterdam. Previously Niels has worked as Head of Digital for ARTICLE19, where he designed, fund-raised, and set up the digital programme which covered the Internet Engineering Task Force, the Internet Corporation for Assigned Names and Numbers, the Institute for Electric and Electronic Engineers and the International Telecommunications Union. Before that, Niels designed and implemented freedom of expression projects with Free Press

Unlimited. He holds a cum laude MA in philosophy from the University of Amsterdam.

Natasha Tusikov is an assistant professor of criminology at York University in Toronto, a visiting fellow with the School of Regulation and Global Governance (RegNet) at the Australian National University, and a senior fellow at the Centre for Global Cooperation Research at the University of Duisburg-Essen, Germany. Her research examines intersections among crime, technology, and regulation, with a particular focus on regulation by internet intermediaries. Her book, *Chokepoints: Global Private Regulation on the Internet*, was published in 2017 by the University of California Press, and she is co-editor of *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (Palgrave Macmillan, 2019). Prior to her work in academia, she was a strategic criminal intelligence analyst with the Royal Canadian Mounted Police in Ottawa, Canada. Her work has been published in *Surveillance & Society* and *Internet Policy Review*.

Preface and acknowledgements

It would be an understatement to say that French President Emmanuel Macron's speech of 12 November 2018 to the Internet Governance Forum (IGF) in Paris was unexpected. A surprise to delegates until the last minute, it was the first time in 13 years of the IGF that the meeting was addressed by a head of government (joined by no less than United Nations Secretary-General António Guterres – another first).

The content of the speech was no less surprising. Politicians usually use these occasions to compliment those present on the important work that they are doing and to wish them well in their deliberations. Less common is for a politician to tell an audience that they have to rethink their basic principles. Macron made the case for greater state involvement in internet governance – to people who generally embrace a multistakeholder model of governance with limited if any place for government.

We as internet governance researchers realised that we had witnessed something very unusual that required unpacking. Thus sparked the idea for this volume. To be sure, the state has always been part of internet governance, and (as several of this volume's contributors point out) calls to bring the state back into internet governance have a long and august history. Still, the fact that Macron's speech could be surprising and controversial to people who are deeply involved in internet governance suggested to us that it would be worth scrutinising the role of the state. Indeed, governments around the world are revisiting a decades-old consensus, often termed neoliberalism, which has advocated a minimal place for the state in everything from industrial policy to, yes, internet governance.

Two of us editors (Natasha Tusikov and Blayne Haggart) had the opportunity to think deeply about these issues while we were research fellows at the Käte Hamburger Kolleg/Centre for Global Cooperation Research (KHK/GCR21) at the University of Duisburg-Essen in Germany during 2018–2019. As the Centre's inaugural fellows working on internet governance, we decided, in cooperation with GCR21 Co-Director Jan Aart Scholte, to host a two-day workshop in July 2019 on the role of the state in this policy field. The workshop brought together emerging and senior scholars from multiple disciplines, including political science, international political economy, economics, business studies, communication studies, global studies, criminology and technology ethics. Revised papers from the meeting provide the substance of this edited volume.

Projects like this do not happen without the efforts of many people. First off, we are grateful to all of our contributors, who took time out of their busy schedules to share their considerable expertise in the workshop and then patiently to address our many editorial questions over the ensuing 12 months. One of the best things about being in academia is the chance to meet brilliant and knowledgeable people, and this project did not disappoint.

Our thanks also go to the Centre for funding and providing logistical support for the workshop. Our special thanks to Sigrid Quack, Director of the Centre, for supporting the idea and for generously acting as a workshop discussant. Thanks also to Hortense Jongen and Niels ten Oever for their incisive comments as workshop discussants. We further thank Rakchanok Chatjuthamard, Julia Fleck, Freya Köhler, and Tobias Schäfer for ably providing comprehensive administrative support. Our gratitude extends also to Patricia Rinck at the Centre for helping us prepare the book proposal for Routledge.

At Routledge, we are grateful to Rosie Anderson for supporting the volume from the beginning. Thanks also to Judy Dunlop for preparing the index and to the Social Sciences and Humanities Research Council of Canada for partially funding the index.


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Introduction

Return of the state?

Blayne Haggart, Jan Aart Scholte and Natasha Tusikov

The internet and the state: bedfellows or adversaries? This pivotal issue attracts many polarised opinions. For some, the state threatens contemporary society's main space of openness and freedom. For others, the internet threatens contemporary society's main source of order and welfare. Yet for most people, one suspects, the relationship between the internet and the state is ambiguous and uncertain: It is not clear what the connection is and what it should be.

This book mainly addresses this third audience of the undecided majority. The chapters explore arguments across the ideological spectrum and experiences around the world with an overall aim to bring greater precision and depth to the debate about the internet and the state. As its primary guiding questions, the volume asks: (a) In what ways and to what extent do (and might) we see increased state involvement in contemporary internet governance; and (b) under what conditions can that greater government role in the internet be a good or a bad thing? In addressing these questions, the chapters examine issues such as the role of the state vis-à-vis multistakeholder governance of the internet, the various internet policies of authoritarian and democratic governments, and the relationship between (global) capitalism and the state in internet regulation.

The internet was largely born of a state, the United States government, between the late 1960s and the early 1990s. However, the main expansion of the global internet over subsequent decades unfolded with governments mostly as spectators. With time, though, many states have become increasingly uneasy with this uncontrolled (by them) development. Outside of government, too, many citizens have worried about corporate power, fake news, phishing, hacking and online violence in an under-regulated global internet. At the same time, sceptics view increased state intervention in the internet as a slippery slope to inefficiency and oppression. Clearly, 50 years after the internet's invention, the return of the state is very much in question.

Emmanuel Macron, President of France, aptly identified three general lines of approach to the issue in his speech to the Internet Governance Forum (IGF) in November 2018. At one extreme, Macron discerned a so-called "California" model, where strong private global players run the internet with limited democratic accountability. At another extreme, Macron described a "Chinese" model based on authoritarian state control, protectionist support of the domestic internet industry,

DOI: 10.4324/9781003008309-1

and violations of human rights. A third approach, advocated by Macron himself, promotes greater involvement in internet governance from democratic states who enshrine the public interest and human rights (Macron 2018). As this typology indicates, debates over internet governance are not just over who makes and implements rules for the network, but also about the prioritisation of interests and values. The chapters in this book critically examine all of these contending perspectives.

Such a discussion needs to distinguish among four different areas of actual and prospective state regulation of the internet. First, there is the *physical infrastructure* of the internet, including cables, exchange points and devices that connect to the network. How far can and should states control this core framework, including "kill switches" that would allow government to shut down the internet in certain localities or even nationally? Second, there is the *virtual infrastructure* of so-called critical internet resources, comprising numbers (Internet Protocol [IP] addresses and autonomous system [AS] numbers), names (the domain name system [DNS]), and protocols (technical standards that enable data transmission on the internet). What role ought states to have in this field, until now mainly governed through multistakeholder regimes in which governments play little or no role? Third comes *data*, namely, information concerning internet users and their use of the network. How far should states set rules in this area and have access to such material, for example, to catch criminals or to track political opponents? Fourth is the issue of *content*, namely, the texts, images and sounds that pass through the internet. How far should states intervene to govern these flows? Potentially one could come to different conclusions regarding the types and extents of desirable state initiative in these respective four areas.

Given the importance of these issues for contemporary public policy, our book is, unsurprisingly, not the first academic publication concerning the state and the internet. Already in the 2000s several analyses argued against exaggerations about the "global" nature of the internet and urged researchers to "bring the state back in" (Drezner 2004; Goldsmith and Wu 2006). Meanwhile, the World Summit on the Information Society (WSIS), held in 2003 and 2005, prompted various academic reflections on the place of the state in emergent multistakeholder governance of the internet (Kleinwächter 2007; Drake and Wilson 2008; Mueller 2010). Well before Macron, several scholarly writings already distinguished different models of internet governance that accord varying roles to the state (Solum 2009; Fung et al. 2013; O'Hara and Hall 2018). More recent publications have examined the role of the state in general (Kohl 2017); state encroachments in internet freedom (Powers and Jablonski 2015; Polyakova and Meserole 2019); government shutdowns of the internet (Ruggiero 2012; Freyburg and Garbe 2018); possible state-induced fragmentation of the internet (Mueller 2017); and the role in internet governance of particular states such as Brazil, China and the United States (Carr 2015; Fraundorfer 2017; Griffiths 2019; Knight 2014).

This volume builds on this literature, but also adds at least four distinctive contributions to knowledge on the state and the internet. First, the book includes both searching theoretical explorations and detailed empirical studies on this subject. Second, the theoretical perspectives span diverse disciplines and approaches. Third, the empirical studies encompass circumstances around the world, including

China, Europe, Latin America, North America and Russia – and by authors from those respective regions. Fourth, the volume considers all four main aspects of internet governance: physical and virtual infrastructure, data and content. Thus, while this book by no means aspires to a final word on questions of the state and the internet, it makes a uniquely wide-ranging contribution to the debate.

The rest of this introductory chapter sets the stage for our contributors' explorations of the state's role in internet governance by highlighting two of the book's recurring themes: namely, the state's relationship with multistakeholder governance and the distinction between authoritarian and democratic states with respect to internet governance. The introduction concludes with an overview of the individual chapters as well as general questions about the role of the state in global digital capitalism.

The state and multistakeholder governance

One key long-running debate concerning the role of the state in internet governance has revolved around the multistakeholder principle. The growth of the global internet has coincided with the rise of a new so-called multistakeholder format of global governance. Until the 1990s, global policy emanated almost exclusively from multilateral institutions such as the United Nations (UN), with states as the sole members. Over the past quarter-century, however, much global governance has turned to the multistakeholder principle, under which policymaking transpires through deliberations among representatives of the various groups – especially nonstate actors – who "have a stake" in the issue at hand (Hocking 2006; Raymond and DeNardis 2015; Lundsgaarde 2016; MSI 2017). Multistakeholder governance can involve academics, activists, entrepreneurs, technicians and others in decision-making along with (and sometimes even without) governments. These cross-sectoral apparatuses are now widespread across many issue areas, including environment, corporate social responsibility, disaster relief, health and food security (Scholte 2020).

Multistakeholder designs have found particular traction in internet governance (Flyverbom 2011; Waz and Weiser 2012; Doria 2014; Sahel 2016). They have become especially prominent in regulating the internet's virtual infrastructure, through bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN, for the DNS), the Internet Engineering Task Force (IETF, for protocols) and the Regional Internet Registries (RIRs, for numbers) (Antonova 2008). In these venues, policy develops through consultations mainly among businesspeople, engineers and civil society activists. In contrast, states generally take a peripheral role in these processes, with only an advisory role at ICANN and no formal status whatsoever in the IETF and the RIRs. The multistakeholder principle also underpins the deliberative IGF that convenes annually under the auspices of the UN, as well as in various regional and national venues (Malcolm 2008; Epstein 2013; Epstein and Nonnecke 2016). Some proponents of multistakeholderism have proposed that this largely nongovernmental approach to governing the internet could further apply to the regulation of content, data and exchange points (Wagner and Mindus n.d.).

The multistakeholder approach – and in particular its general marginalisation of the state – has attracted considerable controversy. For its supporters, multistakeholderism provides a more participatory, effective, expert, flexible and fair way of making and implementing rules for the internet and other policy fields (Khagram 2006; Doria 2014; Strickling and Hill 2017; Dodds 2019). Backers affirm that this new model of governance avoids much of the incompetence, inefficiency and rigidity that comes with state-led regulation of the internet. Advocates of multistakeholder governance therefore reacted warily to Macron's aforementioned speech, which they interpreted as a state-oriented broadside against a well-functioning nongovernmental alternative (Badii 2018; Fattal 2018).

Yet critics maintain that multistakeholder governance (of the internet and in general) is deeply flawed. Sceptics underline that, in practice, parties participate very unequally: The multistakeholder approach favours power and privilege, especially of big corporations and dominant countries, while marginalising weaker players in world politics (Carr 2015; Cheyns and Riisgaard 2014; Gleckman 2018; Hofmann 2016; Winseck 2019). Indeed, accounts have often highlighted the prominent role of a hegemonic state (the United States government) in sponsoring the early development of ICANN and the IETF (Carr 2015, 2016; Powers and Jablonski 2015, Chapter 5). Opponents of multistakeholderism often assert that intergovernmental multilateralism offers more voice to peripheral countries and better protects the global public interest. These doubters therefore urge a transfer of responsibilities for global internet governance to state-centred bodies such as the International Telecommunication Union (ITU).

Three chapters in the present volume – by Santaniello, Cavalli and Scholte, and ten Oever – engage directly with this ongoing debate around multistakeholderism and multilateralism in internet governance. Santaniello observes that multistakeholderism emerged as a compromise between neoliberalism (which privileges private-sector actors and free-market policies) and sovereigntism (which treats internet governance as the sole purview of the state). Cavalli and Scholte, writing from an insider's perspective as active participants in ICANN proceedings, identify key strengths and weaknesses of multistakeholder governance. In particular, they question the current regime's ability to effectively address questions of the public interest, given that the predominant stakeholder groups at ICANN mostly prioritise commercial and technical concerns. Similarly, ten Oever regards multistakeholderism as an attempt to depoliticise internet governance; however, as he underlines, the focus on technical expertise is itself a political move that promotes certain values over others. Our four authors do not see the core question as "states – in or out," but rather as the nature of state involvement in multistakeholderism, particularly in taking internet governance objectives beyond mere technical connectivity.

The great divide? Authoritarian and democratic states

Since early days of the internet, debates on its governance have substantially revolved around questions of liberty and oppression. Indeed, advocates of

multistakeholderism have regularly maintained that a "bottom-up" approach with governments on the sidelines helps to keep the internet "open and free." In 1996 John Perry Barlow, libertarian co-founder of the Electronic Frontier Foundation, famously echoed sentiments of the American Revolution in his "Declaration of the Independence of Cyberspace":

> Governments of the Industrial World . . . I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. . . . In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. . . . These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers.
>
> (Barlow 1996)

The subsequent quarter-century has seen such arguments continually replayed, including for example in Macron's previously cited distinction between "California" and "Chinese" models of internet governance. These issues have become still more pointed with current debates around the future of the liberal world order: Will internet governance promote a society built on liberal democracy and human rights or will internet regulation be part and parcel of a systemic turn to authoritarianism across the planet?

As noted already, direct state involvement in internet regulation is often considered to be a tool primarily of authoritarian governments, with its spread to democratic states often seen as a harbinger of digital authoritarianism. Certainly, autocratic leaders have embraced new ways to control information flows and monitor their populations on the internet. China is the paradigmatic case of state control over the internet, with its Great Firewall, bans on popular US-based platforms like Facebook, and complex system of online censorship, often enacted in partnership with private companies (see Luo and Lv, this volume). Also typically placed in the authoritarian camp is Russia, particularly as the Russian government develops plans for kill switches that could shut down the internet in the event of external threats or internal unrest (see Stadnik, this volume).

Internet shutdowns through kill switches are a blunt tool that authoritarian states employ to control the flow of information. Access Now, a nongovernmental advocacy group, defines internet shutdowns as "an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information" (#KeepItOn 2019, 2). For example, governments in Sub-Saharan Africa have routinely used internet shutdowns to restrict information during elections via text messaging and apps (see Freyburg and Garbe 2018). Access Now's global tracking of internet shutdowns finds, unsurprisingly, that authoritarian governments are world leaders in shutdowns, particularly Venezuela, Yemen, Iraq, Algeria and Ethiopia (#KeepItOn 2019).

Meanwhile, democratic states have also explored and, in some cases, actually used internet shutdowns to control information within their borders. For instance, in 2010 US policymakers discussed the possibility of an internet kill switch for domestic traffic, although the proposals eventually went nowhere (Ruggiero 2012). In a paradigmatic example of worries of "digital authoritarianism" – the importation into democracies of perceived undemocratic internet governance practices – India tops Access Now's global list for 2019 of countries that have shut down the internet (#KeepItOn 2019). The government of India suspended the internet in multiple cities, including parts of New Delhi, as protests grew against a new citizenship law seen as anti-Muslim, and also cut off the internet to the Muslim-majority region of Kashmir for many months (Mohan 2020).

Yet, as several contributors to this volume point out, focusing exclusively on binary divisions between authoritarian and democratic states is not always conducive to understanding actually existing internet governance. Consider the question of what drives the behaviour of online platforms in China and the US. Despite operating in different political environments, platforms in both countries have commercial practices that prioritise the accumulation and monetisation of users' personal data (Fuchs 2016; Jia and Winseck 2018; Jiang and Fu 2018; Liang et al. 2018). As Jia points out in her contribution to this book, platforms operating within the authoritarian Chinese internet follow a fundamentally market-based logic. This situation places certain limitations on how the authoritarian Chinese government can treat those companies, given that the state has tied its own fortunes to their well-being. As Jia additionally notes, these companies' need for capital and for access to global markets further constrains the government's scope for action.

Given that market forces structure internet activity in both democratic and authoritarian countries, it may be important to situate the internet as being deeply embedded in larger forces of global capitalism. Taken collectively, the chapters in this volume suggest the need to look beyond the usual authoritarianism-versus-democracy framing of the debate. Rather, the market and capitalism structure policies and limit possibilities for authoritarian and democratic governments alike. In particular, the internet involves new forms of commodification (e.g., of protocols, data and online content) that elicit new lines of regulation that involve both state and nonstate actors.

Arguments in summary

As just indicated, in assessing the nature and desirability (or not) of state involvement in internet governance, contributors to this volume recurrently come back to issues such as multistakeholder arrangements and the relationship between capital and state in internet governance. Individual chapters in the three parts of the book also explore a variety of more specific issues that arise in the respective contexts under consideration. We wind up this introduction with a chapter-by-chapter preview of the insights to come.

The first part of the book considers the state's role in internet governance from a macro systemic perspective. In Chapter 1, Mauro Santaniello examines trends

and transformations of internet governance at the national, regional and global levels. In particular, he highlights four types of internet governance: neoliberalism, sovereigntism, multistakeholderism and constitutionalism. The models vary regarding the actors that they include in internet policymaking and regarding the degree of coercion assigned to decisions. As a key consideration for internet governance, Santaniello examines whether a state's constitution adequately protects individual freedoms and rights while limiting private power. Constitutions that do not do so may be vulnerable to see the internet captured by nationalist, authoritarian and populist forces.

In Chapter 2, Olga Cavalli and Jan Aart Scholte examine how macro questions concerning the state and multistakeholder governance of the internet played out in the so-called IANA stewardship transition of 2014–2016. This process saw formal oversight of the virtual infrastructure of the global internet pass from the US government to an "empowered community" of stakeholder representatives. The chapter traces the long and heated debates regarding the role of the state in multistakeholderism at ICANN that accompanied the transition process, with a particular focus on the question of ICANN's approach to "public interest" issues.

In Chapter 3, Niels ten Oever argues that internet governance should be understood as a regime complex that encompasses both a private-led multistakeholder aspect and a state-driven multilateral aspect. The private multistakeholder dimension of the regime, he argues, prizes interoperability and interconnection above all other objectives, while states and the multilateral dimension pursue myriad other goals. Thus the conflict between the two approaches can be understood as a conflict of prioritised values within a single regime complex rather than as an existential conflict between private and public governance.

In Chapter 4, Dan Ciuriak and Maria Ptashkina round off Part 1 with a discussion of the changing role of the state in an emerging data-driven economy. In contrast to the laissez-faire orthodoxy that has reigned over recent decades, the move to an economy that places intangibles such as data at its centre will almost by necessity prompt increased state intervention in data regulation and economic governance more generally.

Part 2 of the book shifts attention from global circumstances towards the domestic conditions of authoritarian countries. Two chapters focus on China and one on Russia. Each contains a degree of detailed empirical analysis that is uncommon in English-language texts.

In Chapter 5, Lianrui Jia critically assesses interactions among the state, capital and domestic companies in China's strategic effort to transform the country into a cyber superpower. The Chinese government, Jia notes, faces a balancing act between its need to maintain tight political control over the internet to ensure political stability and its efforts to expand markets to ensure the flow of international capital which is essential to the prosperity of capitalist Chinese internet companies. Jia explores these issues more closely by examining the use by Chinese internet companies of the controversial variable interests entity (VIE). This instrument allows companies to circumvent China's foreign ownership rules in order to access much-needed sources of international capital.

In Chapter 6, Ting Luo and Aofei Lv explore the tensions between China's control of politically sensitive content and its more hands-off treatment of non-sensitive content, especially when the latter relates to technology-driven economic development. Luo and Lv use the lens of "fragmented authoritarianism" (Lieberthal and Oksenberg 1988) to understand the Chinese government's oscillation between centralisation and decentralisation in its approach to internet governance. Specifically, this chapter shows how the Chinese government is selective in its internet governance: Priority areas (in terms of Party survival) receive centralised attention, while governance of non-priority areas is fragmented among multiple government agencies with conflicting agendas and interests, which the authors describe with the Chinese metaphor "nine dragons run the water."

In Chapter 7, Ilona Stadnik shows that limits to authoritarian state power over the internet also figure in Russia. The government in Moscow declares ambitions not only to monitor content and control data, but also to create a "Runet" that the authorities could, if they wanted, disconnect from the global internet. However, a range of technical, economic and political circumstances work against these aspirations, and in practice internet users in Russia continue to work with online services based outside the country and beyond the reach of the Russian state.

Part 3 of the book focuses on internet governance as practiced by democratic states. In Chapter 8, Julia Rone assesses efforts by the European Union to counter online disinformation. She considers the concept of digital sovereignty in terms of the state's capacity to control critical technical infrastructure and the flow of information within its borders. Rone highlights that, while both authoritarian and democratic states face capacity issues with respect to internet governance, democratic states face the additional need to maintain democratic legitimacy. Rone also argues that "the return of the state" applies rather narrowly to big and powerful states, particularly since smaller states have limited ability effectively to regulate large global internet companies.

Like Ciuriak and Ptashkina, Jean-Marie Chenou seeks in Chapter 9 to assess internet governance in the context of the regulation of digital capitalism. Adopting a framework based on the varieties of digital capitalism (VoDC), the chapter examines this issue in several Latin American countries. Chenou finds that these states' specific regulation of digital capitalism (in areas such as data, taxation and labour laws) reflects their particular institutional and historical context.

In Chapter 10, Jhessica Reia and Luã Fergus Cruz round off Part 3 by considering the smart city as the "last mile" of internet governance. Here the focus is not on the national government, but on how the internet is deployed as infrastructure in cities. Focusing on the Brazilian smart-city experience in the Bolsonaro era, Reia and Cruz critically assess the power dynamics between state and nonstate actors and reflect upon the implications of different – or absent – regulatory frameworks for data governance in smart cities. In contrast to the progressive international image that Brazil has on other issues of digital governance, the Brazilian smart-city agenda is dominated by commercial interests, with relatively few openings for civil society groups to promote smart-city policies in the public interest.

In the book's conclusion, the editors draw together insights from the nine chapters in wider reflections on the current and prospective nature of state involvement in internet governance. We suggest that, while useful to an extent, casting debates in terms of multilateralism-versus-multistakeholderism and authoritarianism-versus-liberalism also draws attention away from some important underlying dynamics. These include the hegemonic role of the United States in constructing the private internet governance regime, the somewhat ironic sidelining of civil society in multistakeholder governance processes, and the extent to which internet governance is shaped within the context of an increasingly powerful global digital capitalism. Taken together with the preceding chapters, the conclusion highlights the need for researchers and policymakers to ask not whether the state should be involved in internet governance – it always has been – but how the state can be most constructively engaged in internet governance, with full respect for democratic accountability and human rights.

References

Antonova, Slavka. 2008. *Powerscape of Internet Governance: How Was Global Multistakeholderism Invented in ICANN?* Saarbrücken: VDM.

Badii, Farzaneh. 2018. "IGF18: Deliver Us From Multilateral Internet Governance." *Internet Governance Project (blog)*. 28 November. www.internetgovernance.org/2018/11/28/igf18-deliver-us-from-multilateral-internet-governance/. Accessed 11 August 2020.

Barlow, John Perry. 1996. *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium: Journal of International Studies* 43 (2): 640–659. https://doi.org/10.1177/0305829814562655.

———. 2016. *US Power and the Internet in International Relations: The Irony of the Information Age*. New York: Palgrave Macmillan.

Cheyns, Emmanuelle, and Lone Riisgaard. 2014. "Introduction to the Symposium." *Agriculture and Human Values* 31 (3): 409–423. https://doi.org/10.1007/s10460-014-9508-4.

Dodds, Felix. 2019. *Stakeholder Democracy: Represented Democracy in a Time of Fear*. Abingdon: Routledge.

Doria, Avri. 2014. "Use [and Abuse] of Multistakeholderism in the Internet." In *The Evolution of Global Internet Governance: Principles and Policies in the Making*, edited by Roxana Radu, Jean-Marie Chenou, and Rolf H. Weber, 115–138. Heidelberg: Springer.

Drake, William J., and Ernest J. Wilson. 2008. "Multistakeholderism, Civil Society, and Global Diplomacy: The Case of the World Summit on the Information Society." In *Governing Global Electronic Networks: International Perspectives on Policy and Power*, edited by William J. Drake and Ernest J. Wilson, 539–582. Cambridge, MA: MIT Press.

Drezner, Daniel W. 2004. "The Global Governance of the Internet: Bringing the State Back In." *Political Science Quarterly* 119 (3): 477–498. https://doi.org/10.2307/20202392.

Epstein, Dmitry. 2013. "The Making of Institutions of Information Governance: The Case of the Internet Governance Forum." *Journal of Information Technology* 28 (2): 137–149. https://doi.org/10.1057/jit.2013.8.

Epstein, Dmitry, and Brandie M. Nonnecke. 2016. "Multistakeholderism in Praxis: The Case of the Regional and National Internet Governance Forum (IGF) Initiatives." *Policy & Internet* 8 (2): 148–173. https://doi.org/10.1002/poi3.116.

Fattal, Kahled. 2018. "Has President Macron Thrown Multistakeholderism Under the Bus at UN IGF 2018 Paris?" *CirclID*. 13 November. www.circleid.com/posts/20181113_has_president_macron_thrown_multistakeholderism_under_the_bus/. Accessed 11 August 2020.

Flyverbom, Mikkel. 2011. *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham: Edward Elgar Publishing.

Fraundorfer, Markus. 2017. "Brazil's Organization of the NETmundial Meeting: Moving Forward in Global Internet Governance." *Global Governance* 23 (3): 503–521. https://doi.org/10.1163/19426720-02303010.

Freyburg, Tina, and Tina Garbe. 2018. "Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa." *International Journal of Communication* 12: 3896–3916.

Fuchs, Christian. 2016. "Baidu, Weibo and Renren: The Global Political Economy of Social Media in China." *Asian Journal of Communication* 26 (1): 14–41. https://doi.org/10.1080/01292986.2015.1041537.

Fung, Archon, Hollie Russon Gilman, and Jennifer Shkabatur. 2013. "Six Models for the Internet + Politics." *International Studies Review* 15 (1): 30–47. https://doi.org/10.1111/misr.12028.

Gleckman, Harris. 2018. *Multistakeholder Governance and Democracy*. Abingdon: Routledge.

Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Griffiths, James. 2019. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed.

Hocking, Brian. 2006. "Multistakeholder Diplomacy: Forms, Functions and Frustrations." In *Multistakeholder Diplomacy: Challenges and Opportunities*, edited by Jovan Kurbalija and Valentin Katrandjiev, 13–29. Geneva: DiploFoundation.

Hofmann, Jeanette. 2016. "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice." *Journal of Cyber Policy* 1 (1): 29–49. https://doi.org/10.1080/23738871.2016.1158303.

Jia, Lianrui, and Dwayne Winseck. 2018. "The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization." *International Communication Gazette* 80 (1): 30–59. https://doi.org/10.1177/1748048517742783.

Jiang, Min, and King-Wa Fu. 2018. "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?" *Policy & Internet* 10 (4): 372–392. https://doi.org/10.1002/poi3.187.

#KeepItOn. 2019. "Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019." *#KeepItOn*. www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf. Accessed 11 August 2020.

Khagram, Sanjeev. 2006. "Possible Future Architectures of Global Governance: A Transnational Perspective/Prospective." *Global Governance* 12 (1): 97–117. https://www.jstor.org/stable/27800600.

Kleinwächter, Wolfgang, ed. 2007. *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment*. Berlin: Marketing für Deutchland.

Knight, Peter T. 2014. *The Internet in Brazil: Origins, Strategy, Development, and Governance*. Bloomington: AuthorHouse.

Kohl, Uta, ed. 2017. *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*. Cambridge: Cambridge University Press.

Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain. 2018. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure." *Policy & Internet* 10 (4): 415–453. https://doi.org/10.1002/poi3.183.

Lieberthal, Kenneth, and Michel Oksenberg. 1988. *Policy Making in China: Leaders, Structures, and Processes*. Princeton, NJ: Princeton University Press.

Lundsgaarde, Erik. 2016. *The Promises and Pitfalls of Global Multi-Stakeholder Initiatives*. Copenhagen: Danish Institute for International Studies.

Macron, Emmanuel. 2018. *IGF 2018 Speech by French President Emmanuel Macron*. Speech presented at the Internet Governance Forum Annual Meeting, Paris, France. 12 November. www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron. Accessed 11 August 2020.

Malcolm, Jeremy. 2008. *Multi-Stakeholder Governance and the Internet Governance Forum*. Perth: Terminus.

Mohan, Pavithra. 2020. "Kashmir's Internet Shutdown Is Splintering India's Democracy." *Fast Company*. 3 March. www.fastcompany.com/90470779/how-the-internet-shutdown-in-kashmir-is-splintering-indias-democracy. Accessed 11 August 2020.

MSI. 2017. *The New Regulators? Assessing the Landscape of Multi-Stakeholder Initiatives*. Berkeley, CA: Institute for Multi-Stakeholder Initiative Integrity and Duke Human Rights Center.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

———. 2017. *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Cambridge: Polity.

O'Hara, Kieron, and Wendy Hall. 2018. *Four Internets: The Geopolitics of Digital Governance*. Centre for International Governance Innovation. https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance.

Polyakova, Alina, and Chris Meserole. 2019. *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago, IL: University of Illinois Press.

Raymond, Mark, and Laura DeNardis. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (3): 572–616. https://doi.org/10.1017/S1752971915000081.

Ruggiero, Scott M. 2012. "Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch." *Science and Technology Law Review* 15 (2): 241–269.

Sahel, Jean-Jacques. 2016. "Multi-Stakeholder Governance: A Necessity and a Challenge for Global Governance in the Twenty-First Century." *Journal of Cyber Policy* 1 (2): 157–175. https://doi.org/10.1080/23738871.2016.1241812.

Scholte, Jan Aart. 2020. *Multistakeholderism: Filling the Global Governance Gap?* Research review prepared for the Global Challenges Foundation. https://globalchallenges.org/multistakeholderism-filling-the-global-governance-gap/. Accessed 30 November 2020.

Solum, Lawrence B. 2009. "Models of Internet Governance." In *Internet Governance: Infrastructure and Institutions*, edited by Lee A. Bygrave and Jon Bing, 48–91. Oxford: Oxford University Press.

Strickling, Lawrence E., and Jonah Force Hill. 2017. "Multi-Stakeholder Internet Governance: Successes and Opportunities." *Journal of Cyber Policy* 2 (3): 296–317. https://doi.org/10.1080/23738871.2017.1404619.

Wagner, Ben, and Patricia Mindus. n.d. "Multistakeholder Governance and Nodal Authority – Understanding Internet Exchange Points." Unpublished paper. https://uu.diva-portal.org/smash/get/diva2:783243/FULLTEXT01.pdf.

Waz, Joe, and Phil Weiser. 2012. "Internet Governance: The Role of Multistakeholder Organizations." *Journal on Telecommunications & High Technology Law* 10 (2): 331–349. https://scholar.law.colorado.edu/articles/149.

Winseck, Dwayne. 2019. "Internet Infrastructure and the Persistent Myth of U.S. Hegemony." In *Taking Knowledge Seriously: Toward an International Political Economy Theory of Knowledge Governance*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 93–120. New York: Palgrave Macmillan.

Part 1

Internet governance

The bird's-eye view


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1 From governance denial to state regulation

A controversy-based typology of internet governance models

Mauro Santaniello

Introduction

During the inaugural ceremony of the 2018 Internet Governance Forum (IGF) in Paris, French President Emmanuel Macron unsettled the audience, and more generally the internet community, with an unprecedented speech on internet-related policy issues. Macron's presence marked the first time ever that a head of state had opened the Forum in the plenary assembly's 13 years of existence. Unusual till then for the IGF, the president also made his speech in the presence of the Secretary-General of the United Nations, António Guterres, laying out an extensive, informed set of policy proposals.[1] In his speech, Macron broke with the most recent European "conservative" tradition, which was fundamentally in agreement with the US Government's attempt to preserve the international regime of internet governance that emerged from the privatisation process of the 1990s. Macron called for "a movement of reform" in global internet governance in general and more state regulation of the internet in particular. More specifically, Macron argued for the need for "new forms of multilateral cooperation" in internet governance, as opposed to both the Californian model of internet governance "of complete self-management" that is fundamentally "not democratic" and the Chinese model, in which the state is "hegemonic" and individual rights are not guaranteed.[2]

These new forms of cooperation, in Macron's view, should be based on democratic regulation and would be consistent with the values of the founders of the internet, which, according to his narrative, are currently endangered. In Macron's words, "the internet we take for granted is under threat" on three levels: On the network level, it is threatened by "state-orchestrated and criminal cyber attacks"; on the content level, it is menaced by "hate speech," "dissemination of terrorist content," and "authoritarian regimes who exploit these opportunities to penetrate our democracies"; and on the level of data governance, "it is threatened by giant platforms which risk to no longer being simple gateways but gatekeepers, controlling members' personal data." State-backed and criminal attackers, authoritarian regimes and the giant US-based online platforms constitute together the villains in Macron's narrative, with France and, above all, Europe the heroes standing in defense of the free internet.

DOI: 10.4324/9781003008309-3

Macron's speech – its location, its content, its rhetorical style – was presented and received as a discursive turning point in the European approach to internet-related policy issues, reviving the debate over alternative global internet governance models. On the one hand, it represented a change in strategy by a relevant European state actor, which can be fully understood only by taking into account the historical evolution of this field of policy, its main controversies, and dynamics among its actors and coalitions. On the other, it was an attempt to delineate a new governance model for the internet and to build a new discursive coalition around it.

In order to historically contextualise Macron's speech and to better understand its political significance for the global governance of the internet, this chapter will (a) briefly reconstruct the historical development of the main political controversies about internet governance in the international arena; (b) draw, on these controversies, a typology of archetypical global internet governance models; and (c) situate Macron's initiative and the current European approach to internet regulation against these models, highlighting their relevance for international relations in the field of internet governance, as well as global trends, rifts and conflicts emerging from the unresolved tensions between state and non-state actors in internet policymaking.

This chapter identifies two main controversies concerning the institutional design of international venues of internet-related policymaking, namely the controversy related to the extent to which these venues are open and decision-making is inclusive of all interested stakeholders and the controversy about the implementation of decisions made in the venue, in particular the level of enforceability and coercion of its policy outputs. These controversies are conceptualised as analytical dimensions whose intersection helps us to deductively characterise four different ideal-typical models of internet governance: neoliberalism, sovereigntism, multistakeholderism and constitutionalism. Each model is discussed and outlined with its main attributes and its underlying ideology. Then, this typology is used to assess Macron's speech, statements from other European political leaders, and their overall relevance for the global governance of the internet. The analysis shows, among other things, that while on the level of principles and values Macron's proposal is clearly based on a liberal-democratic approach rooted in constitutional theory, on the level of concrete policy proposals his words seem to embrace a less inclusive model focused more on the exercise of national sovereignty than on fundamental rights protection. Also, both Macron's speech and statements from other European politicians clearly testify a turn to state regulation in the European internet governance, one that is mainly addressed to digital platforms rather than traditional issues such as the management of infrastructure and the administration of critical resources. It is concluded that a new stage of structural changes and political struggles seems to be started at the international level around internet-related issues and that it is still hard to understand where these transformations are heading. The aim of this chapter is to provide some conceptual coordinates to better situate and analyse ongoing power reconfigurations and actors' repositioning in the global internet governance, building on the historical development of

the policy field but also abstracting single disputes of the past into a more general level of analysis able to catch long-term trends.

Internet governance forums: from governance denial to state regulation

The early internet, Arpanet, was built by what political scientists call a "policy community" (Heclo and Wildavsky 1974; Rhodes 1990, 1997); that is, a network of stable relations between a restricted number of actors, sharing a common set of values, beliefs, experiences, specialist languages and career paths (Hogwood 1987), relatively isolated from the general public and other institutional networks (Rhodes 1986), and characterised by a low level of internal conflict due to the fact that each participant, even within a hierarchical distribution of power and resources, is engaged in a positive-sum game (Rhodes and Marsh 1992). Arpanet's policy community was "a rather close-knit and trusted network of researchers and scientists from the same cultural background with a shared set of values and beliefs" (Ziewitz and Brown 2013, 11). This community was abundantly supported by public funds (Hafner and Lyon 1996), mainly from the US Department of Defense through its Advanced Research Project Agency (ARPA), and the National Science Foundation (NSF). Members of the community made decisions about design and functioning of Arpanet by means of a deliberative principle known as "rough consensus and running code" (Clark 1992), based on an informal decision-making process aimed at finding practical solutions to be easily implemented (Bradner 1999). This model of governance, which has been defined as "ad hoc governance" by the sociologist Manuel Castells (2001, 31) and as a "technical regime" by the political scientist Jeanette Hofmann (2007, 77), has been operating since the end of the 1960s. In the second half of the 1990s, the US government decided to transfer the operational control over the internet from the technical community of engineers and computer scientists based in US universities to the private sector, as well as to replace the oversight role of the US Department of Defense with that of the US Department of Commerce (Mueller 2002; Goldsmith and Wu 2006). The business leadership in internet development, configuration and management was institutionalised through a set of public policies adopted in the second half of the 1990s. For example, in 1995, the original backbone of the internet, the National Science Foundation Network (NSFNET), was commercialised. As well, the 1996 US Telecommunications Act liberalised the US communications market, allowing media corporations to compete with telecommunications operators, and vice versa, paving the way for the consolidation of big media companies through mergers and acquisitions (Mouritsen 2002). The Telecommunications Act was paralleled, at the international level, by the World Trade Organisation (WTO) Agreement on Basic Telecommunications Services. This agreement, which entered into force on 1 January 1998, called upon member governments to liberalise their domestic telecommunications markets and to open them to global competition.

Furthermore, in 1997, the US administration of Bill Clinton issued its Framework for Global Electronic Commerce, which established the principle that "the

private sector should lead . . . the development of a global competitive, market-based system to register Internet domain names" (Clinton 1997). The presidential order that accompanied the framework also instructed the Department of Commerce (DoC) to "make the governance of the domain name system private and competitive and to create a contractually based self-regulatory regime" (ibidem). In the same years, the US government actively worked to support the privatised nature of the internet governance regime, preventing the technical community from establishing a Geneva-based organisation that, together with the World Intellectual Property Organisation (WIPO), the International Trademark Association (ITA) and the UN International Telecommunications Union (ITU), would exercise control over the Domain Name System (DNS). On 5 June 1998, the DoC's National Telecommunications and Information Administration (NTIA) issued its own "Statement of Policy on the Management of Internet Names and Addresses," known as the White Paper, sanctioning the basis for the establishment of a new corporation for the administration of the DNS, the Internet Corporation for Assigned Names and Numbers (ICANN), which was effectively founded on 18 September 1998.

These policies, aimed at privatising, commercialising, deregulating and liberalising the internet, were mirrored by domestic and international pushes to strengthen digital-copyright protection. In 1996, WIPO's World Copyright Treaty (WCT) and World Performances and Phonograms Treaty (WPPT) ensured legal protection for and enforcement of rules related to digital rights management (DRM) copyright-protection regimes, paralleled in the United States by the 1998 Digital Millennium Copyright Act (DMCA). As a result of these actions, by the end of the 1990s, the United States had constructed an internet self-governance regime at the domestic and international levels, based upon the ideological pillars of property rights and global economic competition, that molded digital communications networks – the internet, in short – into a global market of interrelated services.

As a consequence of these changes, private corporations and nongovernmental entities came to play a central role in internet policymaking, "not only in carrying out their core functions but also as actors responding to events on a larger political stage" (DeNardis 2014, 12). "Profit-seeking entities became co-creators of standards and norms and, in certain cases, held discretionary power for law enforcement, be it for criminal investigations or for the protection of intellectual property rights" (Radu 2019, 76).

The replacement of the previous technical regime with this new private order occurred within a wider political context dominated by the neoliberal credo of business self-regulation. Despite the crucial role of the US government, first in financing the initial development of the internet and then in directing a regime change towards privatisation, the self-regulation model was rhetorically represented as being in open opposition to any kind of governmental regulatory interference. Indeed, a prominent argumentation in the 1990s-era public debate over internet development was what William Drake has labeled "internet governance denial," which conceives of "governance" as a concept semantically too close to that of government, and, as such, as a dangerous idea that could have opened

the doors to "state-centric approaches that would be fundamentally out of synch with and damaging to the Internet" (Drake 2004, 2). State action, in this vision, had to be limited in enabling economic competition, in creating a pro-market legal environment, in protecting property rights, and in fostering entrepreneurship, innovation and private investment. Hence, a neoliberal model of internet governance to all effects.

At the beginning of the 2000s, the new internet private order, established under the auspices of the US government, was facing hostile actions coming from two different directions. The first was from a set of initiatives advanced by a number of other national governments, including both US rivals and allies. In 2003, China, supported by a large group of developing countries, asked for an international treaty for the internet and the establishment of an Intergovernmental Internet Organisation (Kleinwaechter 2009). The European Union, Brazil, South Africa and many other allied governments launched similar initiatives in the same period, calling for an internationalisation of internet governance, including "the management of the Internet's core resources, namely, the domain name system, IP addresses and the root server system" (European Commission 2005). Similarly, the ITU conducted intergovernmental efforts to regain authority for national governments (Kleinwaechter 2004) and became a crucial venue of internet policy-making at the international level.

The second strand of criticism against the US-centred private order was driven by a galaxy of nongovernmental organisations demanding "the consolidation and enhancement of democratic process at all levels from local to global and the democratic management of international bodies dealing with ICTs [Information and Communication Technologies], e.g. ICANN, IETF [Internet Engineering Task Force], ITU" (ALAI et al. 2002).[3] Also, beginning at the end of 1990s, a growing and diverse set of initiatives were being proposed by multiple sources to anchor the development of the internet and its governance arrangements to democratic principles and rights protection (Padovani and Santaniello 2018). Declarations, charters, bills of rights and laws concerning internet-related rights and democratic governance principles were elaborated by civil society associations, intergovernmental organisations, national parliaments, political parties, technical bodies, academics and some private companies. The term "digital constitutionalism" – which has recently emerged to label a field of studies at the crossroad among law, political science and sociology – refers to this "constellation of initiatives that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet" (Redeker, Gill and Gasser 2018, 303).

These requests for reform from both governments and non-state actors led to the establishment of the World Summit on the Information Society (WSIS), a multiphase process set by the United Nations through the ITU in 2003. The WSIS process triggered the institutionalisation of a new internet governance model, the multistakeholder model, based on the idea of a broad participation from different stakeholders, including the private sector, national governments, intergovernmental organisations, civil society and technical and academic communities. The institutionalisation of multistakeholderism in internet governance

was accomplished by a set of international agreements, including the 2003 Geneva Declaration of Principles, the 2003 Geneva Plan of Action, the 2005 Tunis Commitment, and the 2005 Tunis Agenda for Information Society, that established new participative principles and new global policy venues, such as the Working Group on Internet Governance (WGIG)[4]; the WSIS annual meetings[5]; the 2015 WSIS+10 review process[6]; and, above all, the annual IGF, whose first meeting was held in Athens in 2006.

As a specific instance of the multistakeholder model, the IGF and its institutional design represented a compromise between the calls for a wider participation in internet governance and the irrevocable willingness of the US government to prevent this participation from questioning the US-centred private order. Indeed, instead of being configured as a fully empowered decision-making centre and replacing ICANN in the governance of the DNS, as was proposed by several options presented by the WGIG (2005), the IGF was designed as a "forum for multistakeholder policy dialogue" (WSIS 2005, art. 72), addressing a variety of issues, from access to digital divide, from security to human rights protection, from youth participation to capacity building, from digital sovereignty to stakeholders' participation, from ICT for development to standard setting procedures and norms. The IGF was designed with "no oversight function," "no involvement in day-to-day or technical operations of the internet": It was "constituted as a neutral, non-duplicative and non-binding process" (ibidem, art. 77). As Mathiason (2009, 126) puts it: "The Internet Governance Forum was, in many ways, a compromise between those who wanted a vigorous, authoritative and intergovernmental institution to oversee the internet and those who wanted no oversight at all." The WSIS process did not solve these conflicts, but it did embed them within this new venue, the IGF. The IGF came to be shaped by those unresolved tensions, involving a contest between two factions (Mueller 2010). On one side, "forum hawks" conceived of the IGF as the preliminary stage of the establishment of an intergovernmental mechanism for internet governance, be it an international framework convention or a "more traditional intergovernmental arena" (Mueller 2010, 11). "Forum 'doves' on the other hand emphasised those aspects of the mandate that were purely educational or informational. They were keen to prevent the IGF from becoming a starting point for disturbing the status quo" (Mueller 2010, 11).

These tensions escalated over time, and actors started to frame the issues at stake within a geopolitical perspective, with representatives of top-level national governmental institutions intervening directly in the internet governance process. For example, after a formal reprimand by then-US Secretary of State Condoleezza Rice and then-US Secretary of Commerce Carlos M. Gutierrez ten days before the second phase of the WSIS in November 2005, the European Union realigned itself with the US position and suspended its political initiative aimed at the internationalisation of internet governance. Meanwhile, other national governments begun to openly question the usefulness of the IGF itself. In 2010, China and the Group of 77[7] threatened to oppose a renewal of the IGF's five-year mandate (Brousseau and Marzouki 2012, 380). In 2012, at the ITU's World

Conference on International Telecommunications (WCIT) in Dubai, a majority of 89 member states, led by the Russian and Chinese governments, approved the new International Telecommunications Regulations (ITRs), which went unsigned by Western countries and were fiercely opposed by the US Congress (US Senate 2012), internet companies and a number of civil society organisations (Chenou and Radu 2014).

Western opposition to the new ITRs was based on some provisions concerning the role of national governments in subject matters such as networks security and robustness (Art. 5A), unsolicited bulk electronic communications (Art. 5B) and suspension of telecommunications services (Art. 7). At a more profound political level, the formal recognition of the WSIS outcomes within an international treaty like the new ITRs (Resolution n. 3) seemed to challenge the non-binding nature of the multistakeholder model and to advance an intergovernmental, rather than a multistakeholder, approach to internet policymaking. The discussion at the WCIT-12 and the signature of the new ITRs signalled that the multistakeholder governance model that had structured internet governance for the past decade was no longer the unquestioned hegemonic model and was open to challenge (Lewis 2014). The rules, moreover, were agreed to in a process that inverted the power balance and governing process of the ICANN institutional setting. At the WCIT, as in most *international* governance fora, national governments were solely responsible for making decisions via formal votes, while business, technical community and civil society played a consultative role. In contrast, at ICANN, it is governments that have a consultative role, via the Governmental Advisory Committee (GAC) which is able only to advise the ICANN Board, on which it has no voting members.

By shifting internet-related policy processes from a venue devoted primarily to policy dialogue (the IGF) to an effective decision-making institution (the WCIT), the coalition, led by the Russian and Chinese governments, successfully implemented a strategy of "venue shopping" (Baumgartner and Jones 1993), in which actors seeking to make a substantive policy change are able to relocate decision-making to a new policy arena. In doing so, they can take advantage of a change of the setting of participating actors, as well as of "the adoption of new rules, and the promotion of new policy images, or understandings, of an issue" (Pralle 2003, 234).

In 2013, Edward Snowden's disclosure of documents authored by the National Security Agency (NSA), unveiling electronic mass surveillance programs led by the US government, further exacerbated these geopolitical tensions and rifts. US rivals used the scandal as an evidence of bad faith and a demonstration of the need for a change in the global internet governance. Some US-allied governments, themselves targeted by espionage, took a suspicious attitude towards Washington, starting judicial and parliamentary investigations, as well as new legislative processes. In Brazil, for example, the Snowden revelations provided a successful push for the passage of the 2014 Brazilian Civil Rights Framework for the internet, known as the "Marco Civil da Internet," a national law aimed at protecting citizens' rights and limiting the exercise of power in and through the internet.

The NSA revelations also cost the US Government to lose the general support of the US-based technical community that authored the so-called 2013 Montevideo Statement on the Future of Internet Cooperation. The statement "expressed strong concern over the undermining of the trust and confidence of internet users globally due to recent revelations of pervasive monitoring and surveillance" and "called for accelerating the globalisation of ICANN and the [Internet Assigned Numbers Authority (IANA)] functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing."[8] The document was signed by all the leaders of the key organisations responsible for the coordination and administration of the global infrastructure of the internet, including ICANN. On 30 September 2016, after a long debate and an articulated policy process, the oversight function of the DoC's NTIA over ICANN was ended as the effect of the so-called IANA stewardship transition, a process that completed the privatisation of the DNS started in the 1990s.

These events form, in broad terms, the background against which Macron gave his 2018 speech. In this context, the speech stands as a turning point in the ongoing debate about the proper role of governments in internet governance because of its clear call for more state regulation in global internet governance, for its goal of having Europe be a key player in global internet governance, and for the prefiguration of a democratic internet governance model set against both the Californian and the Chinese models. It represents a relevant novelty also for the setting chose by Macron for his political initiative: an IGF facing, on the one hand, ICANN's private management of the internet critical resources and, on the other, ITU's revived interventionism at the intergovernmental level. Macron was explicitly asking for the IGF to reform itself toward producing more concrete outcomes: "[T]his Forum now needs to produce more than just debate and reflection. It needs to reform, to become a body producing tangible proposals."

A typology of internet governance models

As the previous section illustrates, the history of internet governance has been characterised by two main governance controversies centred on the form and status of international internet-focused policy venues. The first controversy relates to who is allowed to enter the venues, who can participate in the policymaking, and whose interests are represented and taken into account. The second controversy substantially relates to the level of enforceability of policymaking's outputs or, in other terms, to the level of coercion to be assigned to decisions made in the venue of policy.

This section builds a typology of internet governance models on these two controversies in order to conceptualise the political space within which actors coalesce and struggle to advance their own policy preferences. While the typology proposed in this chapter is not the first attempt to classify different models of internet governance, it offers a sharper picture of the key fractures that shape the political space of internet governance, as well as a clear connection between each model and its underlying political ideology. The aim of this new typology

is to overcome some limits of previous classificatory efforts. For example, Solum (2009) has proposed a taxonomy of five models that focus on the nature of the institutions in question: i) spontaneous ordering; ii) transnational institutions or international organisations; iii) code and architecture; iv) national governments and law; v) market regulation. However, Solum's taxonomy presents three main conceptual flaws. First of all, his first model (spontaneous ordering), following Hofmann, Katzenbach and Gollatz (2017, 1418), cannot be considered to be a form of governance, since the latter is more appropriately defined as "reflexive coordination," emerging "when routine coordination fails" and a conflict arises. Second, his second model – "transnational institutions or international organisations" – refers, in fact, to two different, even antithetical models. Third, and most importantly for our discussion, transnational institutions, international organisations, code, law and market should not be considered as different governance models, but rather as different types of governance mechanisms. Indeed, at least theoretically, each of them could be both employed in combination with other mechanisms and adapted to different models of governance.

Another well-known modelling of political approaches to internet governance is the typology presented by Milton Mueller in his 2010 book, *Networks and States*. Mueller's typology is based on two axes. The first one, the nation-state axis, counterposes a system based on "existing, national political institutions" to one which "favours creating or evolving new, transnational institutions around the global space for human interaction the network creates" (Mueller 2010, 255). Mueller's second axis, the network-hierarchy axis, reflects the difference between, on the one hand, the preference for a hierarchical system, within which "governance emerges from adherence to rules enforced by an authority, [and] where adherence is obtained by force if necessary," and, on the other hand, free networking characterised by "peaceful forms of association and disassociation" (Mueller 2010, 257). For many aspects, Mueller's typology is similar to what we are going to propose in these pages, above all for his second axis which catches, more or less, the dimension we are referring to as public coercion. That said, Mueller's first axis is focused on the role of the nation-state as opposed to that of new transnational institutions, while the history of internet governance would suggest to take into account a wider spectrum of possible actors in the policymaking process. In other words, it is not sufficient to understand whether an actor prefers old, formal institutions rather than new transnational bodies as the leaders of internet development. Instead, an understanding of preferences about interests' representation within old and new arenas is essential in order to get a clear picture of the whole range of political views in the internet governance field.

Turning back to our typology, it is grounded on two dimensions of conflict that we have named inclusiveness and coercion. The inclusiveness of policy venues concerns what global governance studies refer to as "input legitimacy" (Sharpf 1999), a political criterion focused on meaningful participation of affected interests in relevant decision-making (Dingwerth 2007). The term inclusiveness is taken from Robert Dahl's typology of political regimes, where it points at the dimension of "the right to participate," which distinguishes full democracies (or "polyarchies")

from "competitive oligarchies" and "autocracies" (Dahl 1973). Inclusiveness relates to participation and its institutional conditions. In the case of internet governance, the debate is structured along a continuum. At one extreme is the exclusivist option, whose proponents argue that policymaking should be limited to only one kind of stakeholder – for example, only governments or only businesses – who should be allowed to make decisions without any significant contribution from other actors. At the other is the inclusive option: Decision-making is legitimised via much broader participation. Actors' inclusiveness preferences are distributed between these two ideal extremities. Historically, inclusiveness is the dimension that has been institutionalised by the WSIS process into the new UN venues of policy dialogue that it created: the WGIG, the WSIS meetings, and the IGF.

In the previous section, we argued that UN-based internet governance venues produced by the multistakeholderist turn to participation of the early 2000s generally lack legally binding outcomes and any effective instrument of implementation. As DeNardis and Raymond put it: "[I]nternational gatherings, as 'talk shops,' potentially have an agenda-setting and framing function but realistically have limited influence over policymaking in practice" (DeNardis and Raymond 2013, 8). In terms of institutional design, these venues, and above all the IGF, were designed as "cross-scale linkages" (Heikkila, Schlager and Davis 2011) providing space for dialogue, deliberation, and learning, not as decision-making centres. This feature – the lack of coercion in multistakeholder processes – is the source of the second controversy which has traditionally characterised the internet governance arena. Indeed, we have already noted that a number of actors – both state and non-state – were unsatisfied with the WSIS outcome because of this lack of any mechanism to reform global internet governance post-WSIS. This second controversy echoes one of the axis of another well-known typology in political science, "the applicability of coercion" in Lowi's typology of public policies (Lowi 1972). Actors' policy preferences about coercive outcomes, in our case, vary from the extreme of an informational policy dialogue without coercion to the other extreme of legally binding agreements and resolutions.

By crossing these two controversial dimensions about global internet-related policymaking – inclusiveness and public coercion – we get four ideal-typical models of internet governance (Table 1.1): i) digital neoliberalism; ii) digital sovereigntism; iii) digital multistakeholderism; and iv) digital constitutionalism.

Digital neoliberalism has been the dominant model of internet governance throughout the 1990s. The model postulates a low level of inclusiveness, with the

Table 1.1 A typology of internet governance models

		Inclusiveness	
		Low	*High*
Public coercion	**High**	Sovereigntism	Constitutionalism
	Low	Neoliberalism	Multistakeholderism

private sector entitled to make decisions, and a level of public coercion next to zero. The role of public policy within this model is confined to initiatives aiming at deregulating markets, protecting property rights, fostering private investments and pushing public administrations towards sharing their own databases in order to make them available for private exploitation (open data). As for the management of internet resources, according to this model, public policy should have no concrete outcome. The main source of legitimacy here is economic competition, and the evaluation of processes, structures and actors' performances is based on the criterion of efficiency. The rationale at the base of this model is economic. Governance is denied. Decision-making is preferred to happen within private-led venues of policy, such as ICANN.

Digital sovereigntism shares a preference for the exclusivist option with the neoliberal approach. In this case, however, the leading stakeholder group is not that of business operators, but rather national governments. Sovereigntism differs from neoliberalism on the axis of coercion, in that it envisages legally binding laws and international treaties as public policy outcomes. The role of public authorities is wider than that preferred by the neoliberal model, including policies for cybersecurity and law enforcement, as well as a public policymaking for internet critical resources that is not limited to Lowi's constitutive policy type (Take 2012) but goes so far as to include regulation of day-to-day technical and operational matters. The model is based on a geopolitical rationale, and the preferred governance mechanism is constituted by bilateral or multilateral negotiations and agreements.

Table 1.2 Attributes of internet governance models

	Neoliberalism	*Sovereigntism*	*Multistakeholderism*	*Constitutionalism*
Governance	Denial	Multilateral	Multistakeholder	Popular
Rationale	Economic	Geopolitical	Technical	Political
Basic principle	Hands-off	State-authority	Do-no-harm	Guarantism
Source of legitimacy	Competition	National sovereignty	Participation	Fundamental rights
Criterion of evaluation	Efficiency	Independence	Continuity	Democracy
Public policy goals	Deregulation, IP protection, investments, data disclosure	Law enforcement, cybersecurity, critical resources	Development, digital divide, capacity building	Fundamental rights protection, public interest representation, promotion of equality
Public policy outcomes	No direct outcome	Legally binding laws and international treaties	Policy dialogue	Legally binding principles and rights
Global policy venues	ICANN	ITU, WCIT	IGF	UN, international courts

Legitimacy is based on national sovereignty; state authority is the basic principle of governance; and state independence is the general criterion of evaluation for governance mechanisms and arrangements. Preferred venues of policies, at the international level, are the ITU, the WCIT and intergovernmental agencies, while at the national level, there is a clear preference for the leadership of governments above parliamentary, business and civil society initiatives.

Digital multistakeholderism, as we argued earlier, emerged as a compromise between the first two models. It shares with the neoliberal model a preference for a low level of coercion by public authorities, but it postulates a high level of inclusiveness on the other hand. According to this feature, all relevant stakeholder groups should be involved in policymaking, towards an ideal of "participation on an equal-footing." In this model, public policy authority is usually diverted from internet critical resources and proper internet governance and moved towards developmental goals: digital divide, capacity-building, ICT for development and other like issues. The preferred policy outcome is an informal policy debate, legitimated by participation, developed around a technical rationale where expertise and epistemic communities play a crucial role and self-limited by a principle of continuity known as the do-no-harm principle. The multistakeholderists' preferred venue of policy is the IGF.

Digital constitutionalism is another form of reaction against the institutionalisation of a neoliberal internet governance model that emerged at the end of the 20th century. It is a model that extends the multistakeholderist formulation of participation virtually to all the people and shares with the sovereigntist model a basic call for public coercion. Indeed, the highest level of coercion is required in this model, in the forms of national laws and constitutional provisions, or as integration of the international human rights law. Digital constitutionalism is based on the idea of a popular governance, and legitimation is derived from the protection of fundamental rights according to the principle of *guarantism*, which envisages the universal guarantee of fundamental rights protection. Governance arrangements, from this model's perspective, are evaluated alongside all the dimensions of the quality of democracy: the rule of law, electoral accountability, interinstitutional accountability, electoral and political competition, citizens' participation, responsiveness, compliance with individual rights and equality (Morlino 2003, 2014). The political rationale of this model is clear in the kind of public policy it postulates: one that is oriented towards the protection of fundamental rights, the advancement of the public interest and the promotion of equality and is aimed at the establishment – and enforcement – of legally binding principles and rights. The preferred venues of internet policymaking in this model are the UN General Assembly, international courts and processes of international conventions as well as, at the national level, parliaments and the judiciary.

The degree of institutional inclusiveness and coercion are highly controversial issues in the debates over the establishment and elaboration of the global venues of internet policymaking. They may be considered as core controversies in internet governance since they relate to constitutive policies and institutionalisation processes in this field, and they are general so as to be able to catch specific

controversial issues. For example, some scholars have identified five high-profile instances that indicate a process of rising contentiousness in internet governance: i) the escalation of conflict over the IANA functions and other critical internet resources; ii) state-promoted alternative arrangements in interconnection governance; iii) tensions related to technical infrastructure issues such as IPv4 depletion, net neutrality and the resurgence of proprietary protocols; iv) the increasing co-opting of the infrastructures of internet governance to achieve objectives which are not related to the fundamental functioning of the internet, such as intellectual property protection or national security; and v) the state erosion of the original normative basis of the internet (Bradshaw et al. 2014). All of these controversies are fundamentally related to issues of inclusiveness and coercion of relevant decision-making (be it ICANN, ITU, WSIS or IGF) and imply a political battle among several kinds of actors (businesses, national governments, international organisations, civil society associations or epistemic communities), each one seeking to select and shape internet policy venues according to its own interests, political strategies and policy preferences.

Concluding this section, the combination of the axis related to public coercion with one concerning the inclusiveness of global venues of internet policy, as proposed in the typology presented earlier, seems to provide a useful conceptual tool to map political forces and spaces in the current internet governance ecosystem and to be general enough to accommodate different, more specific, controversial issues.

Using this inclusivity-coercion typology, the next section will assess Macron's project of a new approach to internet-related policymaking and, more generally, the hypothesis of a turn to state regulation in Europe as well as worldwide.

Macron, Europe, and the turn to regulation in the global internet governance

The European Union, and European countries, have always played a regulatory role in internet governance. However, European regulation has historically followed a neoliberal approach, which is particularly evident in the 2010 Digital Agenda for Europe and the 2015 Digital Single Market Strategy, as both promote an approach to digital policy clearly oriented towards competition, entrepreneurship and proprietary rights (Giannone and Santaniello 2018). At the international level, following the EU's withdrawal from the reform movement within the WSIS process at the end of 2005, the Union has remained aligned with the US positions on the axis of coercion and has kept on supporting the non-binding nature of outcomes from international policy venues. On the inclusiveness axis, the European Union has been oscillating between supporting the neoliberal model, that is, recognising business as the primary force in internet governance, and the multistakeholder model in arenas such as the 2015 WSIS+10 review process where the EU asked for broader participation in internet governance arrangements and institutions (Santaniello 2018).

Viewed from this historical vantage point, Macron's speech presented a doubly significant novelty. The first involved his choice of the multistakeholder IGF as

the institutional setting of his call for greater state regulation and his attempt to mobilise the forum, or at least some of its constituencies, towards a new political project based around state regulation rather than policy debate. The second novel aspect of his speech could be found in his request for the IGF to move from being a talk shop towards the pursuit of more concrete outcomes, which amounted to a call to reform the IGF itself. These proposed policy transformations could easily be seen as threatening the very foundations of the WSIS compromise that, as we have seen, is based on the informative nature of the IGF and its outcomes. That said, it is interesting to note that while Macron's speech may have seemed to be proposing a far-reaching revolution, its actual focus may have been somewhat more limited. Crucially, Macron did not mention internet critical resources, ICANN or the DNS in his broadside against the current state of internet governance. Instead, he focused on platform regulation, reflecting the growing importance of internet companies as centres of decision-making, which stands in contrast with the decreasing relative relevance of organisations involved in the management of internet protocols, root servers, domain names and addresses (van Eeten and Mueller 2012).[9] Even when addressing threats to the internet's infrastructure, Macron spoke about cybersecurity – that is, attacks over the network – rather than any potential threat emerging from centralised routing systems or resources. In highlighting cyberattacks, Macron was focusing on an issue in which the right of the state to regulate has been uncontested since the early 2000s, from both a sovereigntist and neoliberal perspective (Birnhack and Elkin-Koren 2003). Moreover, in the field of cybersecurity, even the US government, which is the leader of the neoliberal coalition, has recently turned towards more sovereigntist political preferences and policy options, as exemplified in the debate over the future of 5G networks and the role that companies such as Huawei should have in constructing them. In short, in these actions it is quite clear geopolitical priorities are overturning the principle of global, free-market competition.[10]

At the time of writing of this chapter, it is still impossible to determine whether a turn in the European strategies away from multistakeholder governance and towards a more state-centric approach is likely to emerge with respect to critical resources. It is clear enough that, in Macron's speech, we can hear a call for a turn to state regulation as for digital platforms. In this context, Macron's speech should be seen as a part of a broader and developing discourse, one that seems, for the moment, to be more focused on the platform giants than on core internet functions. A few months before the 2018 IGF, on 23 May 2018, Macron had already expressed a clear point of view on the matter when he convened many representatives of global internet companies for a discussion about regulation and international governance of the internet. On that occasion, the French president welcomed his guests at the Elysee Palace, ironically stating "there is no free lunch" and making clear that he wanted tougher regulations and for internet companies to contribute more to society, especially through taxation (Pennetier and Rosemain 2018). Facebook CEO Mark Zuckerberg seemed to echo the president's stance when, a couple of weeks after the Christchurch mosque shootings in New Zealand in March 2019, he published an op-ed in the *Washington Post* arguing

that "we need a more active role for governments and regulators . . . we need new regulation" (Zuckerberg 2019). Throughout Europe, Zuckerberg's op-ed was met with scepticism from across the ideological divide, but scepticism related to whether Zuckerberg was serious about such regulation, rather than questioning the need for state regulation itself. Zuckerberg critics included German Justice Minister Katarina Barley ("promises aren't enough. In [the] future we will have to regulate companies like Facebook much more strictly" [Reuters 2011]), then-European Justice Commissioner Věra Jourová ("Facebook has to look first and foremost at itself. If they want to, they can embrace a real change already now" [Stolton 2019]), then-Dutch MEP Marietje Schaake ("he has lost a lot of trust . . . nobody sees it at face value anymore . . . if Facebook indeed cares so much about the rule of law, which I think every company should, they can begin respecting it today" [Euronews 2019, 36:20]), and then-British MEP Claude Moraes ("Facebook are adopting a strategy which says 'we know that the European Union, one of the three big regulators in the world, can now adopt anti-trust, monopoly, tax-type regulation. But Facebook doesn't want to get into that. . . . He wants to stay in the soft area" [Euronews 2019, 37:40]).

More recently, then-United Kingdom Prime Minister Theresa May, introducing the Online Harms White Paper on 8 April 2019, stated: "[W]e are putting a legal duty of care on [social media companies] to keep users safe, and if they fail to do so, tough punishments will be imposed. The era of social media firms regulating themselves is over."[11] All these pro-regulation, high-level political statements represent a turn to regulation in European internet governance. This turn involves more than just lawmaking, as in new legislative initiatives such as the EU's General Data Protection Regulation and Copyright Directive, or the increasing importance of regulatory bodies and national agencies in enforcing competition laws, consumer protection provisions and communication policy. These statements about Zuckerberg highlight the extent to which the turn to state regulation of the internet is now, in Europe, also a political discourse. It is, however, a highly selective discourse, focused on the levels of content and data, and particularly on digital platforms, depicted as instruments of both anti-democratic forces (hate speech, fake news, terrorist content) and powerful actors practicing data surveillance (Facebook, Google, Amazon, etc.). Crucially, this discursive turn to internet regulation does not include the oldest issue of the internet governance field, the management of the DNS.

Turning back to Macron's speech and following our inclusiveness-coercion typology, what kind of internet governance model is he proposing? In condemning the "Chinese model" and "the California form of internet," Macron is distancing himself from the low-inclusiveness sovereignist and neoliberal models, respectively. Instead, his speech embraces principles of constitutionalism (high levels of inclusivity and public coercion). Such an approach is ranked as more inclusive than the multistakeholder model, basing its legitimacy not only on stakeholders' participation ("this new path where governments, along with internet players, civil societies and all actors are able to regulate properly") but also on a wider principle of democratic representation ("the condition for democratically elected

governments respecting the rule of law to protect their people"). Moreover, Macron's speech is also imbued with normative narratives, in which traditional state-based mechanisms of democratic lawmaking and law enforcement serve the protection of citizens' rights. These rights (individual freedoms, data protection, cultural diversity, democratic representation), understood as universal rights, are the basic ideas in Macron's discourse and delineate a liberal-democratic form of digital constitutionalism.

That said, one can also discern a second strand in Macron's speech that seems to echo a sovereignist discourse (low levels of inclusion, high levels of public coercion). In the parts of his talk where he addressed practical courses of action, the French president highlights security issues and the need for content regulation, while also standing against anonymity and internet neutrality and in favour of domestic copyright holders facing the unregulated power of transnational platforms. Even those parts of his speech that touch on taxation issues are not framed by talk about the global redistribution of wealth in the internet economy as one would expect from a constitutionalist approach encompassing economic and social rights. Rather, he presents the issue using a nationalist, somehow populist frame: "to ensure fairer taxation so that our peoples are not the sole taxpayers" and "to prevent the effects of domination and hegemony of certain players." Finally, his proposals for concrete reforms to the IGF envisage a "new collegial method," in which the IGF has "to become a body producing tangible proposals." National governments would then legislate and regulate to implement these proposals: "[W]ho better than these governments can set the law?" The risk here is that, without any agreed structural linkage between the forum's deliberations and national legislators, each government would cherry-pick legitimising arguments from the IGF according to its own contingent politics. The result, again, would be much closer to the low inclusiveness of sovereigntism than the high degree of inclusiveness of a constitutionalist approach.

Overall, Macron's model shares with the sovereigntist and the constitutionalist models high levels of public coercion; the shape and direction of any eventual institutional reforms will determine whether its levels of inclusiveness will be closer to sovereigntism's low levels or constitutionalism's high levels. For Macron's model of internet governance to differentiate itself from the sovereigntist approach and be classified as a truly constitutionalist project, it must involve the formalised, guaranteed, and balanced involvement of multiple interests in the decision-making process. In other words, it requires the constitutionalisation of multistakeholder participation. The question about which internet governance model Macron actually has in mind – a sovereigntist or constitutionalist one – is, at the moment of writing, still open. This analysis makes clear that possibilities for an institutionalisation of a democratic approach to global internet governance depend on a process of constitutionalisation that, while limiting private power and protecting digital rights with legally binding mechanisms anchored to democratic national constitutions, is also able to constrain public power, regulating participation at the highest normative level, and preventing governments from embracing the sovereigntist temptation to be the only decision-maker in internet policymaking.

Finally, it is worth noting that this turn to state regulation in internet governance is not unique to the European Union and its member states. Many other countries have either passed or proposed internet governance regulations (Kang and Satariano 2019).

However, what indeed marks Macron's speech as something different from other legislative and political initiatives is the all-encompassing strategy of reform it advances for the global governance of the internet, which is aimed at greater state regulation. By naming the American and Chinese models as an internet governance dichotomy, and promoting an European alternative to them, the French president produced a coherent frame of political action which substantially diverges from sporadic, even if increasingly frequent, initiatives. However, it remains to be seen whether Macron's project will be able to involve the entire European Union or at least some other member states – as the reactions to Zuckerberg's op-ed suggest – or whether its effects will be limited to a national, albeit important, French initiative. Of course, the unity of European states would be a decisive factor for the success of a new model of global internet governance, in the case it was a sovereigntist model – which would endanger geopolitical relations between Europe and the USA and would subvert the multistakeholderist internet order – or it was a constitutional one – which would offer an appealing alternative to what Macron defines the Californian and the Chinese models.

Conclusion

The inclusiveness-coercion typology presented in this chapter provides us with a useful way to distinguish among various models of internet governance. In the case of Macron's speech, it highlights that his proposal is at least somewhat at war with itself, at times supporting a highly inclusive constitutionalist form of internet governance, at others a less-inclusive, but just as coercive, form of sovereigntism. Moreover, a close reading of his speech also highlights the extent to which certain areas of internet governance – namely, the global platforms – are singled out for criticism, while others – namely, the technical infrastructure – are largely ignored. This speech, and other interventions by high-level European politicians strongly suggests that if a turn to state regulation is observable in European internet governance, it is mainly focused on digital platforms. However, the fact that the self-identified champion of this turn, or its main policy entrepreneur, Emmanuel Macron, decided to take a stance in favour of a new internet governance model at the IGF – which, as we have seen, was born within a controversial political space related to the management of the Domain Name System – may yet prefigure the rising of new systemic approaches that will also affect traditional internet governance issues.

That said, a single speech, although politically relevant, is not sufficient to assess Macron's claim that his grand project of reform is aimed at a democratic, rights-based model of internet governance, let alone whether its vision will come to fruition. Future analysis will allow us to discern and evaluate what is going on in this field at the European level and what kind of impact it will have on the global

governance of the internet. For the moment, it is worth noting that Macron's claims have been acknowledged to some degree at the level of the United Nations. The UN High-Level Panel on Digital Cooperation (UNSGdigicoop), established by the Secretary-General in July 2018, in its report issued in June 2019, addressed a series of shortcomings of the current IGF. Above all, it highlighted "the lack of actionable outcomes" (United Nations 2019, 24) by the IGF (which is, recall, a UN entity) and proposed some institutional reforms that mirror Macron's proposal. These high-level calls for the IGF's institutional reengineering represent a political attempt to turn the forum from an arena of governance, understood as reflexive coordination, to an arena of regulation, understood as a "process involving the sustained and focused attempt to alter the behaviour of others according to identified purposes with the intention of producing a broadly identified outcome" (Black 2001, 142).

The nature of internet governance, never completely static, will continue to change and adapt in the coming years. The typology offered in this work, based on historical controversies around constitutive policies of internet governance, can help to provide a conceptual framework to assess these ongoing transformations in internet governance. Beyond this point, further research is needed to keep theory in line with evolving scenarios and to monitor and observe current events, which are crucial for the future of both the internet and democracies.

Notes

1 At the following meeting of the IGF, held in Berlin in November 2019, this novel ceremonial convention was confirmed with the speeches of the Secretary-General of the United Nations and German Chancellor Angela Merkel.
2 Macron's speech is available online at www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron (accessed 30 September 2019).
3 The Internet Engineering Task Force (IETF) is an open international community dealing with internet standards.
4 The WGIG was initiated by the UN Secretary-General in 2003 with the objective of developing a common understanding of internet governance and identifying relevant public policy issues and the roles of involved stakeholders.
5 The World Summit on Information Society of Tunis in 2005 agreed upon the institutionalisation of an annual WSIS meeting to monitor and evaluate progresses on the objectives stated in the Tunis Agenda.
6 The Tunis Agenda, endorsed by the General Assembly in resolution 60/252, envisaged an overall review process of the WSIS outcomes, which was effectively conducted in 2015.
7 The Group of 77 (G-77) is an intergovernmental organisation within the UN system, made of developing countries signatories of the "Joint Declaration of the Seventy-Seven Developing Countries." The G-77 was established in 1964 and initially included seventy-seven members. To date, the G-77 has 135 member states.
8 The Internet Assigned Numbers Authority (IANA) is one of the very first internet-specific institutions. IANA functions refer to activities aimed at managing and ensuring the global uniqueness of internet identifiers: internet protocol addresses (IP), domain names and protocol parameters.
9 Indeed, the commercial success of digital platforms such as search engines and social media are raising the importance of their own (proprietary) naming and addressing

systems in the general context of internet content localisation and traffic routing, to the detriment of traditional IANA functions. Another factor that pushes towards the decreasing relevance of controversies around the DNS is the inflation of the domain name space as the result of an expansive policy in the creation of new Top Level Domains (Thomas 2011).

10 On 15 May 2019, US President Donald Trump, with the "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," paved the way to ban US tech companies from using Huawei technologies and from doing business with the Chinese telecom supplier and phone manufacturer. Notwithstanding the fact that the ban may be understood within the ongoing trade war between the USA and China, the White House, soon followed by other Western countries, clearly gave a national security frame to this unilateral initiative.

11 Teresa May, Twitter post, 8 April 2019, 4:18 a.m., https://twitter.com/theresa_may/status/1115167134496251905, accessed 4 August 2020.

References

ALAI, APC, ALER, CPSR, CONGO, CREIS, DigIT Africa/ITVision, FAWCO, GLOCOM, GreenNet et al. 2002. "Putting People First in the Information Society. A Statement on Wsis Content and Themes, Endorsed by 22 Ngos and Civil Society Entities." *Statement at the WSIS Geneva Phase PreCom-1*. www.itu.int/wsis/docs/pc1/statements_content/cs_group.doc.

Baumgartner, Frank R., and Bryan D. Jones. 1993. *Agendas and Instability in American Politics*. Chicago: University of Chicago Press.

Birnhack, Michael D., and Niva Elkin-Koren. 2003. "The Invisible Handshake: The Reemergence of the State in the Digital Environment." *Virginia Journal of Law & Technology* 8 (6): 1–57. https://dx.doi.org/10.2139/ssrn.381020.

Black, Julia. 2001. "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World." *Current Legal Problems* 54 (1): 103–146. https://doi.org/10.1093/clp/54.1.103.

Bradner, Scott. 1999. "The Internet Engineering Task Force." In *Open Sources: Voices from the Open Source Revolution*, edited by Chris DiBona, Sam Ockman, and Mark Stone, 47–52. Sebastopol, CA: O'Reilly & Associates, Inc. www.oreilly.com/openbook/opensources/book/.

Bradshaw, Samantha, Laura DeNardis, Fen Hampson, Eric Jardine, and Mark Raymond. "The Emergence of Contention in Global Internet Governance." *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2014*. http://dx.doi.org/10.2139/ssrn.2809835.

Brousseau, Eric, and Meryem Marzouki. 2012. "Internet Governance: Old Issues, New Framings, Uncertain Implications." In *Governance, Regulations and Powers on the Internet*, edited by Eric Brousseau, Meryem Marzouki, and Cécile Méadel, 368–397. Cambridge: Cambridge University Press.

Castells, Manuel. 2001. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press.

Chenou, Jean-Marie, and Roxana Radu. 2014. "Global Internet Policy: A Fifteen – Year Long Debate." In *The Evolution of Global internet Governance. Principles and Policies in the Making*, edited by Jean-Marie Chenou, Roxana Radu, and Rolf H. Weber, 3–19. Berlin: Springer.

Clark, David D. 1992. "A Cloudy Crystal Ball – Visions of the Future." In *Proceedings of the Twenty-Fourth Internet Engineering Task Force*, edited by Megan Davies, Cynthia Clark, and Debra Lagare, 540–543. Reston: Corporation for National Research Initiatives.

Clinton, William J. 1997. *The Framework for Global Electronic Commerce*. https://clinton-whitehouse4.archives.gov/WH/New/Commerce/read.html.

Dahl, Robert A. 1973. *Polyarchy: Participation and Opposition*. New Haven, CT: Yale University Press.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

DeNardis, Laura, and Mark Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance." *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013*. http://dx.doi.org/10.2139/ssrn.2354377.

Dingwerth, Klaus. 2007. *The New Transnationalism. Transnational Governance and Democratic Legitimacy*. New York: Palgrave McMillan.

Drake, William J. 2004. "Reframing Internet Governance Discourse: Fifteen Baseline Propositions." In *Internet Governance: A Grand Collaboration*, edited by Don MacLean, 122–161. New York: United Nations Information and Communication Technology Task Force.

Euronews. 2019. "Raw Politics in Full: Brexit Votes, First-Time Politicians and Facebook Regulation." *YouTube Video*. 1 April. https://youtu.be/VkbRAfkcO-o. Accessed 4 August 2020.

European Commission. 2005. *Towards A Global Partnership in the Information Society: The Contribution of the European Union to the Second Phase of the World Summit on the Information Society (WSIS)*, COM(2005) 234 final.

Giannone, Diego, and Mauro Santaniello. 2018. "Governance by Indicators: The Case of the Digital Agenda for Europe." *Information, Communication & Society* 22 (13): 1889–1902, https://doi.org/10.1080/1369118X.2018.1469655.

Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Hafner, Katie, and Matthew Lyon. 1996. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Touchstone Books.

Heclo, Hugh, and Aaron Wildavsky. 1974. *The Private Government of Public Money. Community and Policy inside British Politics*. London: Palgrave Macmillan.

Heikkila, Tanya, Edella Schlager, and Mark W. Davis. 2011. "The Role of Cross-Scale Institutional Link- Ages in Common Pool Resource Management: Assessing Interstate River Compacts." *Policy Studies Journal* 39 (1): 121–145. https://doi.org/10.1111/j.1541-0072.2010.00399.x.

Hofmann, Jeanette. 2007. "Internet Governance: A Regulative Idea in Flux." In *Internet Governance: An Introduction*, edited by Ravi Kumar Jain Bandamutha, 74–108. Dehradun: Icfai University Press.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2017. "Between Coordination and Regulation: Finding the Governance in Internet Governance." *New Media & Society* 19 (9): 1406–1423. https://doi.org/10.1177%2F1461444816639975.

Hogwood, Brian W. 1987. "The Tangled Web – Networks and the Territorial Dimension of Industrial Policy." *Political Studies Association Conference Paper*.

Kang, Cecilia, and Adam Satariano. 2019. "Regulators Around the World Are Circling Facebook." *The New York Times*. 25 April. www.nytimes.com/2019/04/25/technology/facebook-regulation-ftc-fine.html.

Kleinwaechter, Wolfgang. 2004. "Beyond ICANN vs ITU?" *The International Communication Gazette* 66 (3–4): 233–251. https://doi.org/10.1177/0016549204043609.

Kleinwaechter, Wolfgang. 2009. "The History of Internet Governance." *Internet Governance*. 20 October. https://web.archive.org/web/20110717120454/www.intgov.net/papers/35.

Lewis, James A. 2014. "Internet Governance: Inevitable Transitions." In *Organized Chaos. Reimagining the Internet*, edited by Mark Raymond and Gordon Smith, 119–132. Waterloo: Centre for International Governance Innovation.

Lowi, Theodore J. 1972. "Four Systems of Policy, Politics, and Choice." *Public Administrative Review* 32 (4): 298–310. https://doi.org/10.2307/974990.

Mathiason, John. 2009. *Internet Governance: The New Frontier of Global Institutions*. Oxon: Routledge.

Morlino, Leonardo. 2003. *Democrazia e democratizzazioni [Democracy and democratisations]*. Bologna: Il Mulino.

Morlino, Leonardo. 2014. *Democrazia e mutamenti. Attori, strutture, processi [Democracy and changes. Actors, structures, processes]*. Rome: LUISS University Press.

Mouritsen, Russell H. 2002. "Telecommunications Act of 1996: Relationships to Functional Theory." *Perspectives. Electronic Journal of the American Association of Behavioral and Social Sciences* 5.

Mueller, Milton. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: MIT Press.

Mueller, Milton. 2010. *Networks and States. The Global Politics of Internet Governance*. Cambridge: MIT Press.

Padovani, Claudia, and Mauro Santaniello. 2018. "Digital Constitutionalism: Human Rights and Power Limitation in the Internet Eco-system." *The International Communication Gazette* 80 (4): 295–301. https://doi.org/10.1177/1748048518757114.

Pennetier, Marine, and Mathieu Rosemain. 2018. "Macron Tells Global Tech CEOs: 'There Is No Free Lunch.'" *Reuters*. 23 May. www.reuters.com/article/us-france-tech/there-is-no-free-lunch-macron-tells-tech-giant-ceos-idUSKCN1IO1V6.

Pralle, Sarah B. "2003. Venue Shopping, Political Strategy, and Policy Change: The Internationalization of Canadian Forest Advocacy." *Journal of Public Policy* 23 (3): 233–260. https://doi.org/10.1017/S0143814X03003118.

Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford: Oxford University Press.

Redeker, Dennis, Lex Gill, and Urs Gasser. 2018. "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights." *The International Communication Gazette* 80 (4): 302–319. https://doi.org/10.1177/1748048518757121.

Reuters. 2018. "Facebook Must Face Stricter Regulation: German Minister." *Reuters*. 26 March. www.reuters.com/article/us-facebook-cambridge-analytica-germany/facebook-must-face-stricter-regulation-german-minister-idUSKBN1H2231. Accessed 4 August 2020.

Rhodes, Rod A.W. 1986. *Beyond Westminster and Whitehall: The Sub-Central Governments of Britain*. London: Unwin-Hyman.

Rhodes, Rod A.W. 1990. "Policy Networks: A British Perspective." *Journal of Theoretical Politics* 2 (2)): 239–317. https://doi.org/10.1177%2F0951692890002003003.

Rhodes, Rod A.W. 1997. *Understanding Governance*. Buckingham: Open University Press.

Rhodes, Rod A.W., and David Marsh. 1992. "New Directions in the Study of Policy Networks." *European Journal of Political Research* 21: 181–205. https://doi.org/10.1111/j.1475-6765.1992.tb00294.x.

Santaniello, Mauro. 2018. *Internet Public Policy. Politiche pubbliche e governance delle reti digitali [Internet Public Policy. Public policies and governance of digital networks]*. Rome: Aracne Editrice.

Sharpf, Fritz W. 1999. *Governing in Europe: Effective and Democratic?* Oxford and New York: Oxford University Press.

Solum, Lawrence B. 2009. "Models of Internet Governance." In *Internet Governance. Infrastructure and Institutions*, edited by Lee A. Bygrave and Jon Bing, 48–91. Oxford: Oxford University Press.

Stolton, Samuel. 2019. "'Regulation Will Not Solve Facebook's Problems', Commission Says." *Euractiv*. 3 April. www.euractiv.com/section/data-protection/news/regulation-will-not-solve-facebooks-problems-commission-says/. Accessed 4 August 2020.

Take, Ingo. 2012. "Regulating the Internet Infrastructure: A Comparative Appraisal of the Legitimacy of ICANN, ITU and the WSIS." *Regulation & Governance* 6 (4): 499–523. https://doi.org/10.1111/j.1748-5991.2012.01151.x.

Thomas, Jude A. 2011. "Fifteen Years of Fame: The Declining Relevance of Domain Names in the Enduring Conflict Between Trademark and Free Speech Rights." *Journal of Marshall Review of Intellectual Property Law* 11 (1): 1–58.

United Nations. 2019. *UN Secretary-General's High-Level Panel on Digital Cooperation. The Age of Digital Interdependence*. New York: United Nations.

US Senate. 2012. *112th Congress. S. Con. Res.50, 'A Concurrent Resolution Expressing the Sense of Congress regarding Actions to Preserve and Advance the Multistakeholder Governance Model under Which the Inter-net Has Thrived'*. Washington: Government Printing Office. www.congress.gov/bill/112th-congress/ senate-concurrent-resolution/50.

Van Eeten, Michel J.G., and Milton Mueller. 2012. "Where Is the Governance in Internet Governance?" *New Media & Society* 15 (5): 1–17. https://doi.org/10.1177/1461444812462850.

Working Group on Internet Governance (WGIG). 2005. *Report of the Working Group on Internet Governance*. https://www.wgig.org/docs/WGIGREPORT.pdf. Accessed 4 September 2020.

World Summit on the Information Society (WSIS). 2005. *Tunis Agenda for the Information Society*. www.itu.int/net/wsis/docs2/tunis/off/6rev1.html. Accessed 4 August 2020.

Ziewitz, Malte, and Ian Brown. 2013. "A Prehistory of Internet Governance." In *Research Handbook on Governance of the Internet*, edited by Ian Brown, 3–26. Cheltenham: Edward Elgar.

Zuckerberg, Mark. 2019. "The Internet Needs New Rules. Let's Start in These Four Areas." *The Washington Post*. 30 March. www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504–521a-11e9-a3f7–78b7525a8d5f_story.html. Accessed 4 August 2020.

2 The role of states in internet governance at ICANN

Olga Cavalli and Jan Aart Scholte

Introduction

In 2003 and 2005, the United Nations (UN) convened the World Summit on the Information Society (WSIS) in Geneva and Tunis, respectively. These meetings aimed to "develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake" (ITU n.d.). One of the key issues involved the participation of different stakeholders in the governance of the internet. WSIS concluded that internet governance must involve the "full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities" (WSIS 2005; see also Kleinwächter 2004; O'Siochru 2004).

Putting this principle into practice has remained a contentious issue in internet governance (Doria 2014; Savage and McConnell 2015; Hofmann 2016). The debate is often framed as a contest between multilateralism and multistakeholderism: between a governance arrangement where governments dominate (multilateralism) and one where governments are one of several constituencies (multistakeholderism). Different parties have contrasting views on which of these institutional designs is more effective, democratic and fair (see Santaniello, this volume; ten Oever, this volume).

For this edited volume, which focuses on the role of the state in internet governance, this chapter analyses the evolution of the role of governments at the Internet Corporation for Assigned Names and Numbers (ICANN), a key multistakeholder organisation in the internet governance ecosystem. In particular, we address the so-called Internet Assigned Numbers Authority (IANA) stewardship transition of 2014–2016, when ICANN oversaw the transfer of responsibility for certain core technical functions of the internet from the United States government to a global multistakeholder community. One of us (Cavalli) was Vice Chair of ICANN's Government Advisory Committee (GAC) at the time. The other (Scholte) was an unremunerated external advisor on accountability issues. We therefore had privileged positions from which to observe these debates.

Although ICANN has from the start been a multistakeholder organisation, its particular form has altered over time. Specifically, since the IANA transition,

DOI: 10.4324/9781003008309-4

the participation of governments has changed, as the US government no longer has formal oversight over ICANN. Moreover, the ICANN Board can now reject GAC advice with fewer votes than before. This reduced role of the state is important, because ICANN's mission of coordinating a set of critical internet resources involves a wide range of nebulous and politically charged "public interest" matters. For example, recent changes in the privacy regulations of the European Union (EU) affect ICANN, and ICANN's own policies on critical internet resources impact more widely on global and national internet policies. These concerns are even more relevant for developing countries, given that future economy and society are highly dependent on digital technology and connectivity.

This chapter's examination of the role of the state at ICANN develops in five steps. The first section discusses the general principle of multistakeholder governance. The second section elaborates how the multistakeholder principle is put into practice at ICANN. The third section summarises the IANA transition process, while two further sections assess the role of states in post-transition ICANN. We conclude that states generally play a secondary role at ICANN and that this situation can have problematic implications for promotion of the (global) public interest.

Multistakeholder governance

The internet is often referred to as a "network of networks," a collection of communication grids enabled by the TCP/IP (Transmission Control Protocol/Internet Protocol). The internet operates with few centrally defined and managed elements and without a central authority. This complexity has given rise to a particular form of governance in which regulatory tasks are performed variously by the private sector, by the state, by international organisations and by a transnational technical community. In terms of organisational form, some internet governance occurs through international (or multilateral) institutions where states are the sole decision-makers. For example, the International Telecommunication Union (ITU) allocates usage of the wireless spectrum. However, most global internet governance takes place via multistakeholder institutions such as ICANN and the Regional Internet Registries (RIRs), where states are but one of several types of participants in the policy process.

Multistakeholder governance departs from the traditional way of ordering global relations, that is, in a state-to-state (or *inter-national*) format. In conventional international organisations, states (and only states) take the decisions. In contrast, multistakeholder organisations make policy through consensus among different sectoral groups. This alternative model brings new ideas to global governance design, not only regarding internet and related services, but also in respect of ecological issues, corporate social responsibility, health, food security and other policy fields. Multistakeholderism represents an innovation in governance because it allows for joint decision making by different stakeholders and openness to participation by individuals and organisations alike.

Multistakeholder governance brings a new perspective to global negotiations. Rather than a multilateral discussion among different governments,

multistakeholder forums bring in additional stakeholders like the private sector, civil society, academia and the technical community. In a globalised context, multistakeholder governance offers the promise of more effectively recognising and accommodating a plurality of interests (Kurbalija and Katrandjiev 2006; Abbott and Snidal 2009; Tapscott 2014). For instance, the internet impacts significantly on diverse spheres including commerce, defence, culture, personal communications and relations, education and legal issues (Carr 2015).

While multistakeholder governance is by no means unique to internet governance, few other areas have so widely embraced the model (Mueller 2010; Antonova 2011; Flyverbom 2011). In the internet field, multistakeholder governance brings together academic, civil society, commercial, governmental and technical actors across local, national, regional and global scales. This form of internet governance was first articulated in 2003, during the first phase of WSIS, by the Working Group on Internet Governance (WGIG). It declared:

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.
>
> (WGIG 2005)

As this definition suggests, the WGIG saw the three types of actors as having shared responsibilities.

Yet the presence of different types of actors at the table need not entail equal participation and influence of the various stakeholders. For example, global internet companies from developed countries tend to be highly active participants in multistakeholder forums, in contrast to relatively little participation from small and medium-sized enterprises or even from larger companies based in developing economies. Likewise, levels and influence of nongovernmental organisation (NGO) representation tend to vary between one multistakeholder institution and the next. Meanwhile, states have a designated chamber at ICANN (in terms of the GAC), but not in the RIRs or the Internet Engineering Task Force (IETF), where governments are at best invited guests.

Multistakeholderism and states at ICANN

While the internet is largely decentralised in a technical sense, a few key elements are needed to make possible the coordination among the world's networks. These "critical internet resources" include names (the domain name system, DNS) and numbers (IP addresses and autonomous system numbers, ASN). Core information about the names and numbers are contained in the internet's so-called root zone file, which is stored in and operated through thirteen "root servers." Centralised control here is needed to ensure that each name and number on the internet is globally unique. This technical coordination allows the internet to operate as a single worldwide network.

ICANN plays a key role in this respect. It makes policy for the DNS, oversees the implementation of decisions from the IETF and the RIRs, and oversees management of the root zone file. ICANN was created in 1998 on the initiative of the US government, then under the presidency of Bill Clinton. The agency was incorporated as a California-based not-for-profit organisation. ICANN's mission, as defined in its bylaws, includes the important role of keeping a stable and secure operation of the internet based on the coordination of the names and numbers. Thus, ICANN has high importance for the functioning of the internet as a whole.

ICANN's core values clearly express that this coordination of key technical functions must be done for the benefit of the internet community as a whole. In the process, ICANN should carry out its activities in conformity with relevant international conventions and applicable local laws. Moreover, ICANN should ensure that the multistakeholder policy development process is used to ascertain the global public interest – and in ways that are transparent and accountable.

In service of its mission, ICANN develops policy through a consensus-based multistakeholder process. ICANN´s commitments and core values prescribe that these processes "are led by the private sector (including business stakeholders, civil society, the technical community, academia, and end users), while duly taking into account the public policy advice of governments and public authorities" (Core Value 11, in CCWG-Accountability 2016). The aim is to achieve a reasonable balance between the interests of different stakeholders, while also avoiding capture by any of them. That said, the formulation of ICANN core values clearly puts the state in a secondary role behind nongovernmental actors.

ICANN's multistakeholder framework is reflected in its unique organisational structure:

- A 20-member Board of Directors
- Three supporting organisations (SOs)
    - the Generic Names Supporting Organisation (GNSO)
    - the Country Code Names Supporting Organisation (ccNSO)
    - the Address Supporting Organisation (ASO)
- Four advisory committees (ACs)
    - At-Large Advisory Committee (ALAC)
    - Governmental Advisory Committee (GAC)
    - Root Server System Advisory Committee (RSSAC)
    - Security and Stability Advisory Committee (SSAC)

The GNSO addresses policies related to generic top-level domain names (gTLDs such as ".com" and ".amazon"). Over 1200 gTLDs operate in today's internet. As the largest body within ICANN, the GNSO has its own multistakeholder substructure, organised into so-called constituencies. Most of these constituencies have a commercial character, including internet registries (the owners of gTLDs), internet registrars (the retail sellers of gTLDs), internet service providers (ISPs),

intellectual property lawyers and business users of the internet. Beyond business interests, the GNSO also includes a Noncommercial Users Constituency (NCUC) and a Not-for-Profit Operational Concerns Constituency (NPOC). Note that states have no formal role anywhere in the GNSO.

The ccNSO addresses policies related to two-letter country-code top-level domain names (ccTLDs) such as ".ca" and ".in". Currently the internet has over 300 ccTLDs in active use. In contrast to gTLDs, ICANN has no formal authority regarding ccTLDs, whose regulation mainly lies with national agencies in the respective countries. States have a prominent role vis-à-vis ccTLDs as the owners and operators of certain country codes. However, most country codes lie in the hands of quasi-governmental organisations, commercial enterprises, and non-profit associations such as foundations and universities. ICANN only enters the picture to host the ccNSO as a coordinating body for the ccTLD sector.

The ASO brings together representatives from the five RIRs: namely, for Africa, Asia-Pacific, Europe, Latin America and Caribbean, and North America. Governance of internet numbers mainly occurs through the RIRs; however, these bodies come together at ICANN through the ASO in order to discuss global policy issues around numbers and to liaise with ICANN on questions of domain name regulation. ASO members normally come from ISPs and other internet engineering concerns. As in the GNSO, states have no involvement in the ASO.

As for ICANN's advisory committees, states have no official role in the two technical bodies, RSSAC and SSAC. Members of these bodies come respectively from root zone operators and network engineers. Likewise, states have no involvement in ALAC, which gathers individual internet users from across the world, as organised in five regional at-large organisations.

The GAC is the main site of government involvement at ICANN. Started in 1999 with the participation of 17 states and 6 intergovernmental organisations, GAC membership has risen over the years to the current count of 178 states and 38 observers, most of which are intergovernmental organisations (GAC n.d.). GAC seats are normally occupied by civil servants from ministries of communications and (less often) foreign affairs. Since 2012, the GAC has also convened a biennial High Level Government Meeting of (deputy) ministers in conjunction with an ICANN general conference.

The GAC leadership consists of a chair and five (before 2014, three) vice chairs. Until 2014, the GAC chair was elected through informal discussions among GAC members. Since 2014, the GAC membership has officially elected the chair and vice chairs. Between 2012 and 2018, the GAC received secretariat support from a series of external parties, including finally a consulting firm in Australia. Since 2018, GAC secretariat services have come entirely from ICANN's own staff.

The GAC convenes face-to-face at the triannual ICANN meetings. Much significant additional deliberation and decision-taking occurs intersessionally through mailing lists and working groups. The GAC leadership also holds biweekly conference calls. As this degree of activity suggests, the GAC is not a diplomatic talk shop, but a highly engaged policymaking body.

That said, ICANN meetings normally attract only around half of the GAC membership, suggesting that many governments do not prioritise their involvement in this multistakeholder process. Moreover, many members send middle-ranking officials rather than committing senior personnel to ICANN work. Most GAC attendees play a fairly passive role, leaving the main initiative to a core of around two dozen seasoned delegates, disproportionately from the Global North. Poorer states in particular lack the resources to attend and build capacity for more effective participation at ICANN. Many developing-country governments in fact receive financial support from the ICANN organisation in order to attend the meetings. The reluctance of some governments to commit more fully to ICANN also derives in part from the limited influence that they can exert in its processes. ICANN's bylaws place specific restrictions on states' involvement in the governance process. As a consequence of ICANN being legally established as a non-profit entity in the State of California, government representatives cannot be voting members of the ICANN Board. Instead, governments are only represented on the ICANN Board with the GAC chair as a non-voting "liaison" member. The GAC does not appoint a representative to fill the designated seat in the Nominating Committee (NomCom), which selects members of the board and other key decision-taking bodies at ICANN.

As its name suggests, the GAC issues *advice* to the board. The board is required either to adopt GAC advice or to justify its refusal of that advice. However, the board is not bound to follow GAC advice, and the GAC has no legal sanctions available if the board rejects the governments' recommendations. In previous times, GAC advice normally entered the policy process at a late stage, after the other stakeholder groups (principally the GNSO) had crafted the main proposals. More recently, several important ICANN deliberations have involved the GAC at early stages of the policy development process. Thus, while states have a formal role in multistakeholder governance at ICANN – in contrast to the IETF and the RIRs, where governments have no official representation at all – the GAC holds an institutionally weak position. In contrast, governments play a relatively stronger role in other multistakeholder institutions such as the Internet Governance Forum (IGF) at the United Nations, the NETmundial process, and the *Comitê Gestor da Internet no Brasil* (CGI.br) at the national level in Brazil (Epstein 2013; Knight 2014; Fraundorfer 2017).

The IANA transition process

The Internet Assigned Numbers Authority (IANA) is one of the internet's oldest institutions, dating back to the 1970s. IANA is responsible for coordinating some of the key elements that keep the internet running as a single worldwide network. The IANA functions fall into three categories: the previously mentioned DNS and number resources, and the technical standards, or "protocols," that enable transmission of data on the internet.

Management of the IANA functions moved to ICANN upon its creation in 1998, but under contract from the US government, as administered through the

National Telecommunications and Information Administration (NTIA) within the US Department of Commerce (DOC). The US government exercised its formal authority over the IANA functions through a series of arrangements with ICANN: a Memorandum of Understanding (1998–2006); a Joint Project Agreement (2006–2009); and an Affirmation of Commitments (2009–2016). From 1998 to 2016, the US government through NTIA also contracted out responsibility to manage and maintain the root zone file, vesting this task with Verisign, a US-based domain registry company that runs major gTLDs including ".com" and ".net". Thus, although ICANN has had a multistakeholder governance structure from the start, the US government through the contract with the DOC/NTIA had unrivalled influence over core internet functions.

This unique US government role in internet governance was challenged as far back as 2003, when a number of governments at WSIS raised concerns about what they perceived to be the unilateral control by the US government of critical internet resources (DeNardis and Raymond 2013). These objections recurred strongly at the 2012 World Congress on Information Technology (WCIT) (Mueller 2012) and escalated further with the 2013 revelations by Edward Snowden about surveillance practices of the US National Security Agency, which provoked angry rebukes from governments and civil society worldwide (Greenwald 2014).

In response, on 14 March 2014, NTIA announced the US government's intention to transfer its stewardship of the IANA functions to the global internet multistakeholder community. NTIA asked ICANN to convene a process to develop a detailed transition proposal. NTIA also laid down specific conditions that any transition proposal would need to meet. In particular, these requisites specified that NTIA's supervision role should not move to any other government, group of governments or intergovernmental organisation. Moreover, NTIA specified, the proposal should have broad support and follow four principles: to enhance the multistakeholder model; to maintain the security, stability, and resilience of the DNS; to meet the needs and expectations of the IANA services' global customers and partners; and to maintain the openness of the internet (NTIA 2014).

The IANA transition process consisted of two main parts, run in parallel. One, depicted on the left of Figure 2.1, was the handover itself of the IANA functions. For this purpose the multistakeholder community at ICANN convened a Cross Community Working Group (CWG) on Naming Related Functions (i.e., concerned with the DNS). The numbers community formed a Consolidated RIR IANA Stewardship Proposal (CRISP) Team. The IETF addressed protocols aspects through a Planning for the NTIA/IANA Transition (IANAPLAN) Working Group. The CWG, CRISP and IANAPLAN fed their respective proposals into an IANA Stewardship Transition Coordination Group (ICG).

States figured in a mostly secondary role in these bodies. The CRISP and IANAPLAN teams had no government involvement. Fifteen of the 119 members of the CWG (or one in eight) came from the GAC. The GAC also supplied 5 of the 30 ICG members. Some leading nongovernmental players argued for just one GAC seat on the ICG, but a counterargument that won the day maintained that representation of states from several regions was needed.

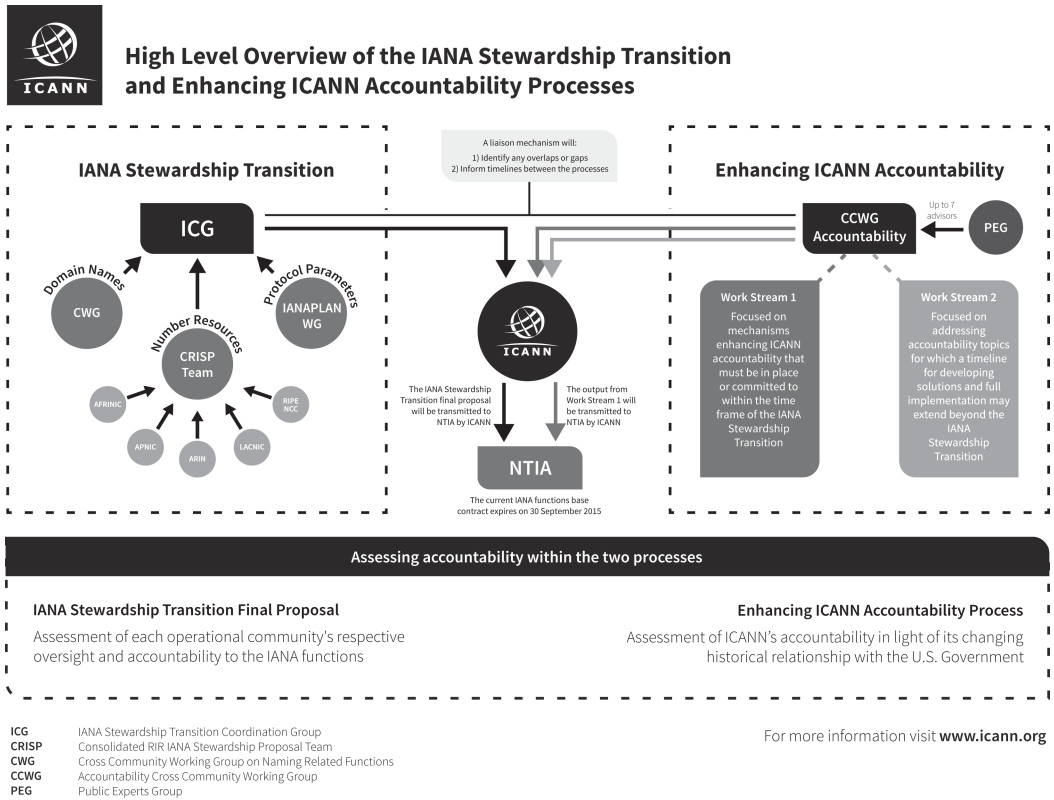


Figure 2.1 Overview of the IANA stewardship transition

Source: ICANN.

The second major part of the IANA transition deliberation, shown on the right of Figure 2.1, concerned the establishment of mechanisms to enhance the accountability of ICANN, given that ICANN would henceforth have greater authority, independent of the US government. Accountability – particularly in situations of marginal state influence – is a long-standing conundrum for multistakeholder governance of the internet (Johnson, Crawford and Palfrey 2004; Koppell 2005; Weber 2009). The IANA handover accentuated these problems all the more, and solutions were not obvious.

The deliberations on ICANN accountability were pursued through a separate Cross Community Working Group (CCWG-Accountability), which divided its tasks into two "work streams." Work Stream 1 focused on proposals for enhancing ICANN accountability in the context of the IANA stewardship transition itself. Work Stream 2 addressed broader accountability issues for ICANN, beyond the IANA functions, such as transparency, diversity and jurisdiction. The CCWG-Accountability was the main venue for debates about the role of the state in ICANN and so forms the focus of much of the following discussion in this chapter.

CCWG-Accountability members were appointed by the different SOs and ACs: five members from ALAC; four members from ASO, five members from ccNSO, five members from GAC, five members from GNSO, two members each from RSSAC and SSAC, an ICANN board liaison, and an ICANN staff representative. Half a dozen independent advisers nominated through a Public Experts Group (PEG) provided external input. Some 200 further individuals participated in the CCWG-Accountability without an ex officio nomination. While the proceedings aimed to reach consensus, actual decision-making was limited to the formally appointed voting members of the working group.

Thus, in line with usual ICANN practice, the CCWG-Accountability treated governments as one stakeholder among several and without any priority. While the GAC is not formally organised into regions, its five nominated members on the working group came respectively from Africa (African Union Commission), Asia-Pacific (Niue), Europe (Denmark), Latin America (Argentina) and North America (USA). Other GAC members active in the CCWG-Accountability proceedings included government representatives from Brazil, France, EU, Iran, Norway, Switzerland, and United Kingdom.

The main IANA transition process lasted for two years. On 10 March 2016, the ICANN Board accepted the overall transition plan developed by the multistakeholder community, as confirmed by the ICG. On 9 June 2016, NTIA announced US government approval of that plan. The official handover of IANA stewardship from NTIA to the multistakeholder community at ICANN was completed on 1 October 2016 (ICANN 2016). Thereafter the CCWG-Accountability continued its Work Stream 2 discussions (i.e., about wider accountability issues) until June 2018.

Work Stream 1: the role of governments in post-transition ICANN

With the October 2016 IANA handover from the US government, ICANN ceased to be formally accountable to a state. That position transferred instead to what

internet governance circles commonly call "the multistakeholder community." In this sense, the IANA transition marked a significant step towards further privatisation of the administration of critical internet resources. Occasional voices (e.g., from governments of the Russian Federation and Saudi Arabia) still suggested that the IANA functions should transfer to the intergovernmental ITU (WSIS+10 2015). However, the overwhelming majority (including the previously sceptical governments of China and India) endorsed the NTIA demand for a global multistakeholder framework of IANA governance. Nor did the ITU intervene in the transition deliberations in any way.

To be sure, as described earlier, states figure in ICANN's multistakeholder community (of SOs and ACs) through the GAC. No one in the transition talks seriously challenged the principle of state involvement in ICANN; yet what precise role would governments play in the post-transition regime? This question, as pursued mainly through the CCWG-Accountability, proved to be one of the most time-consuming and contentious matters in the IANA transition deliberations. Three points stood out in particular, detailed here in turn: the GAC mode of decision-taking; GAC advice to the ICANN board; and GAC's role in the Empowered Community.

GAC decision-taking

Before the IANA transition, the GAC took its decisions on the basis of consensus. As noted earlier, the GAC began with a small membership and quite informal deliberations, so consensus was relatively easier to achieve in the beginning. However, by the time of the NTIA announcement in 2014, the GAC had grown to some 130 members, and the transition attracted the participation of several dozen more governments. In such a situation, consensus in the sense of unanimity can become more challenging. Objections from only one or a few governments could paralyse the GAC decision process.

Reflecting on this challenge, discussions arose during the IANA transition deliberations about shifting GAC decision-taking from consensus to majority rule. Several governments (Argentina, Brazil, France, and the Russian Federation, among others) suggested that the GAC should not be bound by one single rule of decision-making, particularly in respect of potentially controversial topics. It could be the case, they noted, that a single government could block consensus, even if the rest of the GAC held a different position. Such stalemates could prompt some governments to withdraw from ICANN, feeling that their views could have no impact. An exit of states would make ICANN more privatised and less multistakeholder. Moreover, the critics pointed out, consensus is not how governments usually operate in multilateral organisations, where instead majority votes generally prevail.

Opponents of a shift to (some) majority voting in the GAC argued that such a move could make ICANN more susceptible to capture (i.e., assertion of undue influence) by governments. These sceptics, which included the US government and leading US business voices, put forward what was called "Stress Test 18" to assess whether ICANN might fall under state capture through the GAC. A number of governments objected to Stress Test 18, seeing it as singling out the

government stakeholder group with particular suspicion and thereby undermining the collegial spirit of the transition process. However, the US government/NTIA saw Stress Test 18 as both appropriate and a necessary condition to garner US Congressional support for the overall IANA handover (given that the Congress would debate the transition proposal before the DOC/NTIA would approve it). The ensuing arguments were the longest and most heated in the entire transition process. In the end, the GAC accepted retention of the consensus principle (understood as "the absence of any formal objection"), although sixteen states issued a dissenting opinion that these moves would weaken the role of governments in the multistakeholder process at ICANN going forward (GAC Minority Statement 2016). Many additional governments held reservations about Stress Test 18 without signing the open declaration.

GAC and the board

Going into the IANA transition, ICANN followed a practice that, as and when the GAC reached consensus on one or the other advice, the board was bound to consider that recommendation. However, the board was not required to adopt the advice and indeed with a two-thirds majority vote could reject it. In practice, though, such board refusals of GAC views had never happened.

During the IANA transition deliberations a proposal arose in the CCWG-Accountability to lower the threshold for board rejection of GAC advice from two-thirds to three-fifths, or one vote fewer than previously. While this change could seem minor, for the GAC it represented another way to diminish the relevance of government participation in the ICANN multistakeholder model. The reduction was adopted following the discussion of Stress Test 18.

The IANA transition also did not alter the pre-existing situation regarding the position of states in the board itself. As before, the GAC has only a non-voting "liaison" seat on the ICANN Board, and governments have no formal role in the selection of the voting members of the board. Governments also continue to have no official say in the selection process for leaders of the other stakeholder groups. To this extent, state power in post-transition ICANN is indeed heavily constrained.

GAC and the Empowered Community

In contrast, on a third point – the so-called Empowered Community (EC) – the IANA transition arrangements accord states some notable power. The EC is the legal mechanism devised by the CCWG-Accountability through which the stakeholder groups (in the form of the SOs and ACs described earlier) can check the power of the ICANN board and organisation. As something of an "ICANN legislature," the EC has an array of competences, including to reject ICANN and IANA budgets; to reject ICANN operating and strategic plans; to recall the entire ICANN board; to appoint and remove individual ICANN board directors (other than the ICANN President/CEO); and to initiate reviews of ICANN decisions and actions.

Hence, participation in the EC involves pivotal power: Would governments (through the GAC) have a seat at this table? ALAC, ASO, ccNSO, and GNSO all signalled their wish to participate in the EC. In contrast, the technical advisory committees RSSAC and SSAC declined to join the EC, arguing that they had no place in "political" matters of holding the ICANN board and organisation to account. Some (including the US government) expressed scepticism about GAC involvement in the EC, seeing it as an avenue through which governments could exert undue influence in the multistakeholder model. However, the final CCWG-Accountability proposal of February 2016 included full voting GAC participation in the EC.

This outcome is significant inasmuch as it allows the GAC – like any other participating SO and AC – to initiate action on any of the EC powers enumerated earlier. To be sure, the GAC must convince the other four participating stakeholder bodies to support its challenge to the ICANN board or organisation. Equally, though, other SOs and ACs must obtain GAC support of an EC action that they might initiate. In this way, governments have emerged from the IANA transition at the heart of ICANN's principal accountability mechanism.

Still, the CCWG-Accountability proposal does place one key limitation on government involvement in the EC: namely, that the GAC cannot participate in situations where an EC decision challenges a board action based on GAC advice (CCWG-Accountability 2016). This exception, called the "GAC carve-out," thus excludes governments when an EC action challenges the board's implementation of GAC advice. Imagine, for example, that the board would accept GAC advice to deny allocation to a nongovernmental actor of a gTLD that used a term with national or regional significance, such as ".africa" or ".amazon". The GAC would then be unable to participate in an EC deliberation on whether or not to resist such a board decision.

In summary, Work Stream 1 (the handover of the IANA functions) brought several changes to the role of states at ICANN. Most prominently, the transition has ended NTIA oversight of ICANN; at least formally, the US government is now just one member among many at the GAC. The power of governments at ICANN also remains constrained in other important ways: The consensus principle limits GAC decision-taking capacity, and governments lack a vote on the ICANN Board. Moreover, when GAC does manage to reach a consensus position, the ICANN Board can still reject the associated GAC advice with a three-fifths majority vote. More positively for states, the GAC has (with one "carve out" exception) equal and strong standing with other stakeholders in ICANN's EC mechanism. All in all, then, governments are a clearly recognised stakeholder in post-transition ICANN, yet also experience major limitations on their influence. The role of the state at ICANN is therefore anything but settled.

Work Stream 2: long-term issues and the (global) public interest

Once the immediate accountability issues connected with the IANA transition were concluded in early 2016, the CCWG-Accountability turned to other matters

of longer-term concern. This agenda included questions such as the diversity of participants in ICANN processes (by region, gender, etc.); the accountability of SOs and ACs; the accountability of ICANN staff; the development of standards to assess the conduct of ICANN board members; ICANN transparency; jurisdictional issues, especially with respect to settling disputes connected with ICANN; the enhancement of ICANN's ombuds; and human rights. The Work Stream 2 agenda continued for another two years beyond the US government handover of the IANA functions, until ICANN's June 2018 meeting in Helsinki.

Underlying many of these issues are questions of "the public interest," broadly meaning that ICANN should govern the internet in ways that serve all affected people. The internet is a public good: more than a technical infrastructure, more than a commercial opportunity, more than an academic resource, more than a space where individual users can do whatever they please. The internet is a key resource for society as a whole, across the world. Consequently, it is crucial that ICANN commits to promoting the overall good. Work Stream 2 questions of transparency, accountability, diverse participation, ethical leadership and human rights are therefore vitally important as means for ICANN to determine and defend the (global) public interest.

Frequent invocation of the phrase "the public interest" at ICANN indicates that the regime's work involves more than coordination of certain critical technical functions and extends further to a range of public policy matters around the internet. Indeed, ICANN's own latest Strategic Plan 2021–2025 speaks of "coordinating policy development reasonably and appropriately related to these technical functions" (ICANN 2019b). While many at ICANN are concerned that the regime should not pursue "mission creep" beyond its core agenda of technical coordination, widespread opinion now also holds that, say, the subject of human rights is appropriately within ICANN's scope (ten Oever 2018).

As chapters across the present volume repeatedly indicate, technical issues cannot be isolated from normative questions in internet governance. Even something as seemingly bland as internet names and numbers readily becomes political. For example, who gets priority in the allocation of IP addresses, particularly if they become scarce? Should internet numbers remain a public resource, outside the market, or may they be commodified and subject to commercial transactions for profit? Who gets to own ".africa", ".islam" and ".apple"? Does use of ".ps" imply recognition of a State of Palestine? Likewise ".tw" for Taiwan? Does ICANN better register itself under the law of California or that of, say, Switzerland? With such sensitive questions ever present around critical internet resources, it is hardly surprising that the IANA transition quickly became politicised.

The "public interest" concept is supposed to adjudicate such questions and surfaces throughout key ICANN documents. For example, from 2013 to 2014, ICANN convened a Strategy Panel on the Public Responsibility Framework, which underlined "ICANN's responsibility to serve the global public interest" and that "ICANN builds trust through serving the public interest" (ICANN 2014b). The ICANN Strategic Plan 2016–2020, which resulted from an extensive multistakeholder deliberation, affirms that ICANN's goal is to be "a proficient, responsive

and respected steward of the public interest through its commitment to public accountability, openness, and effective cooperation and collaboration" (ICANN 2014a). Public interest also features in the recent statement of Strategic Objectives, which calls on the regime to "develop and implement a global public interest framework bounded by ICANN's mission" (ICANN 2019b). Likewise, ICANN's Accountability Indicators aim to "develop and implement a global public interest framework . . . through . . . increasing the base of internationally diverse, knowledgeable, and engaged ICANN stakeholders" (ICANN n.d.). These widespread references to "the (global) public interest" take ICANN well beyond narrow technical coordination tasks. They highlight that ICANN has a central role as a steward in a more holistic and all-encompassing internet ecosystem.

To be sure, definitions of "the public interest" – let alone "the *global* public interest" – are notoriously nebulous and controversial. Indeed, the phrase often surfaces in documents and discussions without any explicit specification. In a more precise articulation, the Strategy Panel of 2014 defined "the global public interest in relation to the internet as ensuring the internet becomes, and continues to be, stable, inclusive, and accessible across the globe so that all may enjoy the benefits of a single and open internet" (ICANN 2014b). However, it seems somewhat overly optimistic to declare, in the Accountability Indicators, that "the ICANN community's decision and policy-making structures and processes are driven by *a clear understanding* of the public interest" (ICANN n.d., emphasis added). Indeed, elsewhere the statement on Accountability Indicators concedes that there may be "inability to reach consensus on what constitutes public interest and on best practices related to the public interest" (ICANN n.d.).

Many of these conceptual ambiguities and political controversies came out in a workshop on "The Global Public Interest in Critical Internet Resources" that convened at the 2015 Internet Governance Forum in João Pessoa, Brazil (IGF 2015). Participants broadly agreed that defining the public interest was a political negotiation among contending perspectives. The discussion also underlined that formulation of the public interest is not fixed, but varies between societies and adapts over time. Different speakers gave different relative emphases in their conceptions of the public interest to technical, economic, social and cultural dimensions. More technical perspectives associated the public interest with the provision of a stable and secure internet. More economically oriented approaches linked the public interest to the prevention of monopoly and market capture. Workshop contributors from developing countries tended to place equal access and increased participation at the core of the global public interest vis-à-vis the internet. Given these multiple and often conflicting conceptions of the public interest, the workshop underlined the importance of finding ways through these competing interests and needs.

Here, the role of the state becomes crucial. States – particularly democratic states – provide an important – many would say the most important – arena to formulate and implement the public interest. Other stakeholders place their primary focus on narrower objectives: Business mainly aims for commercial success; civil society associations generally advocate on behalf of specific groups; engineers

put their foremost energies into technical problem-solving; and academics seek to construct and communicate knowledge. These other actors are not blind to wider public concerns, as witnessed when firms pursue corporate social responsibility and civil society organisations promote human rights. Yet governments put the public interest squarely first – *and* offer mechanisms for negotiating between contrasting positions. Thus, internet governance without the state risks subordinating the public interest.

In this way the GAC, as the designated site of state involvement, is essential to multistakeholder processes at ICANN. A marginalisation of states at ICANN, and in multistakeholder internet governance more generally, risks underplaying the role of the public interest in internet governance, possibly even losing sight of it altogether. The absence of any systematic role for states at the IETF and the RIRs can be quite worrying in this regard. Can wholly privatised exchanges among business, civil society and technical circles adequately determine the public interest, without involvement from government? States are uniquely positioned as the most legitimate stakeholders when it comes to defining and protecting the public interest. The premise that the private sector can substitute for the state in this regard is problematic.

Seen in this light, the previously described outcomes of the IANA transition are troubling. The consensus principle (which, note, is not required of any other SO or AC at ICANN) makes it harder for governments to bring a view to the multistakeholder table. When the GAC does succeed in arriving at consensus advice, the ICANN Board can reject it with a 60 per cent vote. Nor does the GAC have full voting participation in the ICANN Board in the way of commercial and civil society stakeholders. Moreover, unlike other SOs and ACs, the GAC faces a "carve out" in the EC. Considering these restrictions on government participation together, one can ask whether a generalised scepticism about state regulation in internet governance has had undesirable consequences for the public interest.

A weak state role also opens ICANN to be more easily captured by business interests. While the IANA transition deliberations expended enormous time and energy on fears of government takeover, the increased power of corporate actors implied by the withdrawal of US government oversight attracted comparatively little attention. It is somewhat ironic that all the talk and measures in the CCWG-Accountability against a hypothetical future government capture arguably facilitated an actual and immediate trend in the direction of corporate dominance and possible capture.

These dangers are illustrated in the long-running dispute between the Amazon company and governments of the Amazon river basin regarding the delegation of the gTLD ".amazon". The Amazon corporation applied to ICANN in 2012 for use of this string. Governments of the Amazon region objected to the company's application and in 2013 pressed their case through a GAC advice decided by consensus (with the US government abstaining). The ICANN Board followed this advice and declined to delegate ".amazon" to the company; however, the Amazon corporation persisted to claim its intellectual property rights to the name. After years of unsuccessful attempts to bridge the conflict, and despite the previous

unanimous GAC advice, the board finally decided in 2019 in favour of the company (ICANN 2019a). Amazonian states argued that the company had appropriated their geographical name without their due consent, but to no avail. The commercial interest of the Amazon company trumped the public interest of the communities living in the Amazon region.

Conclusion

This chapter has examined the role of states in multistakeholder internet governance at ICANN, with particular emphasis on shifts in the position of governments during recent years as a result of the IANA stewardship transition. Our analysis has concluded that, while states have become more active in multistakeholder processes at ICANN, they overall still hold a secondary role. It is a larger role than in the IETF and the RIRs, but a smaller role than in the IGF and a number of national arrangements for the governance of internet infrastructure. On balance, the IANA transition leaves the role of the state at ICANN in the balance, which leaves concerns as to how well this core institution of global internet governance can further the public interest.

This diagnosis points towards several possible reforms of ICANN, mainly with the purpose to bring governments on a par of influence with other stakeholders. One step would be to release the GAC from its consensus rule, thereby enabling more government decisions and expanding government participation in ICANN's multistakeholder deliberations. In addition, the GAC seat on the ICANN Board could obtain voting rights, and the NomCom could be permitted, when suitable candidates are available, to suggest government officials to fill open seats on the board. Such measures would help to even the playing field at ICANN between the state and nonstate actors, in the process increasing political space for attention to public interest concerns.

To be sure, states ought simultaneously to upgrade their engagement at ICANN in order to merit such increased influence. For example, more governments could attend and actively contribute to ICANN proceedings. If states demand a seat at the table, then they also need to take it when offered. In addition, many governments could raise their level of representation at ICANN, sending more senior civil servants or ministerial-level delegates. Junior officials are less equipped with information, experience and authority to handle the delicate politics of determining the public interest. Furthermore, states who claim to adjudicate the public interest – whether at ICANN or elsewhere – need to be democratically accountable. At present not all governments in the GAC base their policy positions on responsive consultation with their citizens, which undermines their credibility as promoters of the public interest.

However, the state and ICANN also face an underlying problem regarding the *global* public interest that increased government involvement cannot solve. States have *territorial* jurisdictions and represent *territorial* publics; hence, governments generally approach the public interest in relation to their country and its population. Yet the *global* public interest can have a different quality of relating

to people who are spread transnationally across the planet (Scholte 2014). For example, the global public interest of adequate internet access for all humanity is not something that individual states are likely to prioritise ahead of their ideas about national interest. In addition, states may underrepresent nonterritorial parts of "the public," such as persons living with disability and women. In today's more global world, the public is not always equivalent to the nation, and one therefore cannot assume that the state is always an adequate custodian of the public interest in a global sphere such as the internet.

References

Abbott, Kenneth W., and Duncan Snidal. 2009. "The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State." In *The Politics of Global Regulation*, edited by Walter Mattli and Ngaire Woods, 44–88. Princeton, NJ: Princeton University Press.

Antonova, Slavka. 2011. "'Capacity-Building' in Global Internet Governance: The Long-Term Outcomes of 'Multistakeholderism'." *Regulation & Governance* 5 (4): 425–445.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium: Journal of International Studies* 43 (2): 640–659. https://doi.org/10.1177/0305829814562655.

CCWG-Accountability. 2016. *CCWG-Accountability Work Stream 1 Recommendations*. https://community.icann.org/pages/viewpage.action?pageId=58723827. Accessed 22 September 2020.

DeNardis, Laura, and Mark Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance." *Paper for GigaNet Symposium*. https://dx.doi.org/10.2139/ssrn.2354377.

Doria, Avri. 2014. "Use [and Abuse] of Multistakeholderism in the Internet." In *The Evolution of Global Internet Governance*, edited by Roxana Radu, Jean-Marie Chenou, and Rolf H. Weber, 115–138. Heidelberg: Springer.

Epstein, Dimitry. 2013. "The Making of Institutions of Information Governance: The Case of the Internet Governance Forum." *Journal of Information Technology* 28: 137–149. https://doi.org /10.1057%2Fjit.2013.8.

Flyverbom, Mikkel. 2011. *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham: Edward Elgar.

Fraundorfer, Markus. 2017. "Brazil's Organization of the NETmundial Meeting: Moving Forward in Global Internet Governance." *Global Governance* 23 (3): 503–521. https://doi.org/10.1163/19426720-02303010.

GAC. n.d. *Website of the Government Advisory Committee*. https://gac.icann.org/. Accessed 22 September 2020.

GAC Minority Statement. 2016. *Minority Opinion by Olga Cavalli*. https://regmedia.co.uk/2016/03/09/gac-minority-statement-iana.pdf. Accessed 22 September 2020.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Picador.

Hofmann, Jeanette. 2016. "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice." *Journal of Cyber Policy* 1 (1): 29–49. https://doi.org /10.1080/23738871.2016.1158303.

ICANN. 2014a. *ICANN Strategic Plan for Fiscal Years 2016–2020*. www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf. Accessed 22 September 2020.

ICANN. 2014b. *ICANN Strategy Panel on the Public Responsibility Framework*. www.icann.org/en/system/files/files/prf-report-15may14-en.pdf. Accessed 22 September 2020.

ICANN. 2016. "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends." 1 October. www.icann.org/news/announcement-2016-10-01-en. Accessed 22 September 2020.

ICANN. 2019a. *Status Update on .AMAZON Applications – The Next Steps*. www.icann.org/news/blog/status-update-on-amazon-applications-the-next-steps. Accessed 22 September 2020.

ICANN. 2019b. *ICANN Strategic Plan for Fiscal Years 2021–2025*. www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf. Accessed 22 September 2020.

ICANN. n.d. *Accountability Indicators*. www.icann.org/accountability-indicators. Accessed 22 September 2020.

IGF. 2015. *The Global 'Public Interest' in Critical Internet Resources Workshop*. www.intgovforum.org/multilingual/ru/content/2015-11-11-ws-52-the-global-%E2%80%9Cpublic-interest%E2%80%9D-in-critical-internet-resources-workshop-room-1. Accessed 22 September 2020.

ITU. n.d. *Basic Information: About WSIS*. www.itu.int/net/wsis/basic/about.html. Accessed 18 July 2020.

Johnson, David R., Susan P. Crawford, and John G. Palfrey. 2004. "The Accountable Internet: Peer Production of Internet Governance." *Virginia Journal of Law & Technology* 9 (9): 1–33.

Kleinwächter, Wolfgang. 2004. "WSIS: A New Diplomacy? Multistakeholder Approach and Bottom Up Policy in Global ICT Governance." *Information Technology & International Development* 1 (3–4): 3–13.

Knight, Peter T. 2014. *The Internet in Brazil: Origins, Strategy, Development, and Governance*. Bloomington: AuthorHouse.

Koppell, Jonathan G.S. 2005. "'Pathologies of Accountability': ICANN and the Challenge of 'Multiple Accountabilities Disorder'." *Public Administration Review* 65 (1): 94–108. https://doi.org/10.1111/j.1540-6210.2005.00434.x.

Kurbalija, Jovan, and Valentin Katrandjiev, eds. 2006. *Multistakeholder Diplomacy: Challenges and Opportunities*. Geneva: DiploFoundation.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Mueller, Milton. 2012. "ITU Phobia: Why WCIT Was Derailed." *Internet Governance Project, Georgia Tech School of Public Policy*. www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/. Accessed 20 July 2020.

NTIA. 2014. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." *News Release. United States Department of Commerce*. www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions. Accessed 20 July 2020.

O'Siochru, Sean. 2004. "Civil Society Participation in the WSIS Process: Promises and Reality." *Continuum: Journal of Media & Cultural Studies* 18 (3): 330–344. https://doi.org/10.1080/1030431042000256090.

Savage, John E., and Bruce W. McConnell. 2015. *Exploring Multi-Stakeholder Internet Governance*. New York: EastWest Institute.

Scholte, Jan Aart. 2014. "Reinventing Global Democracy." *European Journal of International Relations* 20 (1): 3–28. https://doi.org/10.1177%2F1354066111436237.

Tapscott, Don. 2014. "Introducing Global Solution Networks: Understanding the New Multi-Stakeholder Models for Global Cooperation." *Problem Solving and Governance Innovations* 9 (1/2): 3–46. https://doi.org/10.1162/inov_a_00200.

ten Oever, Niels. 2018. "Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN." *Policy & Internet* 11 (1): 37–60. https://doi.org/10.1002/poi3.172.

Weber, Rolf H. 2009. "Accountability in Internet Governance." *International Journal of Communications Law & Policy* 13: 153–167. https://doi.org/10.5167/uzh-33071.

WGIG. 2005. *Report of the Working Group on Internet Governance*. Chateau de Bossey, June. www.wgig.org/docs/WGIGREPORT.pdf. Accessed 22 September 2020.

WSIS. 2005. *Tunis Agenda for the Information Society*. United Nations. www.itu.int/net/wsis/docs2/tunis/off/6rev1.html. Accessed 22 September 2020.

WSIS+10. 2015. *Submission of the Russian Federation to the World Summit on the Information Society + 10 Final Document*. http://workspace.unpan.org/sites/Internet/Documents/UNPAN94956.pdf. Accessed 5 September 2015.

3 The metagovernance of internet governance

Niels ten Oever

Introduction

Since the mid-1990s, multistakeholder governance, and specifically private internet governance, has been viewed as a governance innovation (Verhulst et al. 2014) and a replacement for intergovernmental telecommunications governance. However, in the 2010s the private internet governance regime, characterised by multistakeholder bottom-up self-regulation (Sowell 2012), started to show some signs of wear and tear, with the increased rule-setting done by states and multilateral bodies. For instance, as described in Chapter 2, several states have felt that they currently have an insufficient stake in the decision-making in the Internet Corporation for Assigned Names and Numbers (ICANN), the body that coordinates the usage of unique identifiers, such as top-level domains and IP addresses, that are foundational for the internet. Other states, such as Russia and China, have gone further by unilaterally proposing and enacting national regulations and creating domestic internet infrastructures in order to better exert influence on the internet, as described in Chapters 5 and 7.

This contest, at its heart, involves a contest between conflicting norms. The private internet governance regime has as its highest value the creation of interoperability and interconnection through industry coordination and norm development. In contrast, the multilateral regime seeks to achieve a number of other goals (including but not limited to maximising state sovereignty, promoting economic prosperity and limiting the spread of harmful and illegal content), through laws, policies, and norm-setting.

The rise of multilateral, or state-focused, internet governance is often seen as being a direct challenge to existing multistakeholder, or private, internet governance (e.g., Mueller 2017). This view sees the state as an (illegitimate) challenger to this private internet governance regime. In contrast, this chapter argues that rather than one regime potentially displacing another, we can better understand transnational internet governance as a regime complex that functionally and effectively consists of two normative regimes, namely a "private internet governance" regime that produces interconnection and interoperation and which is limited in turn by a "multilateral internet governance" regime. These two normative regimes jointly shape the internet as we know it. Both regimes operate with functionally

DOI: 10.4324/9781003008309-5

narrow remits that are shaped by their respective guiding norms. The guiding norms of the private internet governance regime is to increase of interconnectivity and interoperability, whereas the guiding norm of the multilateral internet governance regime is also to ensure the technical infrastructure accommodates national and regional norms and values.

To understand how these two regimes fit together, I employ the concept of "metagovernance." This lens offers us a to functionally differentiate between these two regimes and to analyse how power and influence are exerted in decentralised decision-making environments. Metagovernance, or "the governance of governance" (Jessop 1997), "entails the coordination of one or more governance modes by using different instruments, methods, and strategies" (Gjaltema, Biesbroek and Termeer 2019, 12). The concept of metagovernance allows one to transcend the perspective that sees "governance" as a practice that overcomes government in favour of one that understands the dialectical relationship between the two regimes. In using this concept, I build on the work of Sandra Braman (2020), who first applied the lens of metagovernance to the field of internet governance. Braman provides an excellent overview of the usefulness of the concept for the field, which I seek to validate by showcasing how institutional design and norm regimes serve as tools for metagovernance (Sørensen and Torfing 2009).

The private internet governance regime, which emerged after the privatisation of the internet in the early 1990s, is narrowly aimed at producing voluntary interconnection and interoperation among internet users and transnational corporations. While it has proven to be very successful in these regards, it has proven unable, in its current configuration, to accommodate norms that do not contribute to an increase in interconnection and interoperation, that is, to address other important social-policy objectives, such as privacy and internationalisation. The inability of the private internet governance regime to deal with these issues has sparked the creation of a new regime, namely the multilateral internet governance regime, based on norm-setting by state-based entities. The result has been the emergence of a regime complex that includes both regimes that themselves are a combination of different governance modes – private actors working through voluntary norms on one hand, states working through treaties and laws on the other – that are sometimes in conflict over norms, goals, and methods. These conflicts give the regime complex a dynamic, changing character. Oftentimes these regimes are painted as opposites, but I argue that both fulfill a particular role that cannot be fulfilled by the other regime. The private internet governance regime systematically fails at incorporating structural considerations on its societal impact, especially when these limit interoperability and interconnection. The multilateral internet governance regime, on the other hand, is unable to produce a general-purpose global communication network. The lens of metagovernance helps us to theorise how the interaction of these regimes, in the internet governance regime complex, are producing the internet infrastructure that is the backbone for information societies.

To substantiate this claim, I will first provide definitions of key theoretical terms I use in my analysis. Second, I provide an overview on debates of how internet

governance should be understood. Third, I describe the rise of the private internet governance regime and its guiding norms of interconnection and interoperability. Finally, I describe the pushback to the private internet governance regime, and the rise of the multilateral regime, and how this led to the emergence of a regime complex.

Norms, regime, and metagovernance of the internet infrastructure

The internet infrastructure is designed to function as a network of independent networks. The word "internet" itself is derived from "internetworking," the practice of interconnecting multiple networks (Peterson and Davie 2007, 169). These independent networks, also called Autonomous Systems (AS), are operated by many different kinds of institutions, ranging from internet service providers and telecommunication companies to research institutions and financial companies. For instance, AS2 is the University of Delaware, AS3 is the Massachusetts Institute of Technology, and AS32251 is assigned to the bank BNP Paribas. Furthermore, the internet does not have a central authority, the independent networks that make up the internet are not necessarily limited to one country or continent, and the "rules of the road" (Wu et al. 2007) for the internet are for the most part not binding, but rather voluntary norms that are developed through the private internet governance regime. Norms are "widely-accepted and internalised principles or codes of conduct that indicate what is deemed to be permitted, prohibited, or required of agents within a specific community" (Erskine and Carr 2016, 87). The voluntary technical norms that underpin the guiding norm of interoperability and interconnection on the internet are produced in private internet governance bodies. Examples of such protocols are the Internet Protocol (IP), the Domain Name System (DNS), and the Hypertext Transfer Protocol (HTTP). The dependence on voluntary norms produces in private governance bodies, rather than mandates in laws or treaties that are developed and ratified by nation states, to promote the interconnection of independent transnational networks make the governance of the internet a complex affair that has resulted in a "mosaic" (Dutton and Peltu 2005) or "bricolage" (Radu 2019) of governance institutions.

The internet has grown from being a communication network based in one and then several societies to the point where it now deeply permeates almost every part of every society in the world, a process described as metastisation (Raymond 2019). Typically, when discussing an issue area in global politics, we can speak of "regimes," which produce "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations" (Krasner 1982, 186). However, the internet's ubiquity and pervasive permeation, and the involvement of a wide range of bodies, institutions, and authorities in the governance of the internet, mean that it is more useful and appropriate to speak of internet governance as a "regime complex." A regime complex is "an array of partially overlapping and non-hierarchical institutions that includes more than one international agreement or authority" (Alter and Raustiala 2018, 329). Regime theory allows one to theorise collaboration and conflict within

one issue field and regime complexes help to understand the interrelation between these regimes that might not always directly interact with each other, but all impact a specific area, in this case the internet infrastructure. Because they involve various institutions, or regimes, the metagovernance framework is particularly useful for thinking about regime complexes such as internet governance.

Politically contested definitions: the where, who, and what of internet governance

The internet's infrastructure has become a fundamental part of the critical infrastructure of information societies. This transformation embeds not only a particular technology or communication system within a society but also the norms enshrined in the processes of designing, standardising, and coordinating internet infrastructure. These norms are politically contested, including at the fundamental level of what exactly is "internet governance."

The definition of "internet governance" is itself contested: Struggles over internet governance thus involve debates regarding what internet governance itself means, as there is no authoritative or definitive definition of internet governance. In the words of Hofmann, "definitions of internet governance, either narrow or broad, always implicitly include preliminary decisions about institutions, constellations of actors and forms of authority" (2005, 1). The nature of these "preliminary decisions" and thus the perspectives of key actors can be illustrated by comparing a few definitions of internet governance. The first, and still most used, definition of internet governance was minted during the United Nations World Summit on the Information Society (WSIS) in 2005:

> Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet.
>
> (United Nations 2005)

This definition describes a wide range of actors involved in the process of internet governance, but their involvement is immediately qualified by the addition of the phrase "in their respective roles." While the nature of these roles is not defined explicitly, this definition least indicates that the actors do not engage on equal footing in the process because of their different respective roles. In the negotiations during the development of these definition, governments were the main actors pushing for the inclusion of this qualifier of the respective roles, because they believed a government representative should, for instance, have more weight than a member of a civil society organisation or a company. Nonetheless, this definition does acknowledge that non-governmental actors do have a role to play in the governance of the internet.

The definition of internet governance that was reached at WSIS cemented the idea that internet governance was a multistakeholder effort (Hofmann 2016).

This, however, led to a backlash among several influential internet governance scholars. In response to the definition of civil society and governments as key actors in the practice internet governance, they proposed one that argues that practically speaking, the private sector, in interplay with the networks' users, not civil society and governments, sets the rules in the governance of the internet:

> Internet governance is collective decision-making by owners, operators, developers, and users of the networks connected by Internet protocols to establish policies, rules, and dispute resolution procedures about technical standards, resource allocations, and/or the conduct of people engaged in global internetworking activities.
>
> (Mueller, Mathiason and Klein 2007, 245)

While this definition did not gain much traction, it does foreground the dominant role the private sector plays in private internet governance. In contrast to the previous one, this definition does not mention governments and civil society or their roles or obligations. The authors do so because, for them, "the internet is largely composed of . . . privately owned and administered networks . . . which means that it has less need than many other systems for global governance" (Mueller, Mathiason and Klein 2007, 246). With this statement, these scholars are not just offering an assessment of the current situation but are also making a normative statement. They are claiming, as many after these scholars have done, that internet governance *should* be left to the private sector. This belief dovetails with the idea that sole role of the private internet governance regime is to increase interconnection and interoperability. The definition also implies that governments and civil society might not (or, perhaps, should not) have an active role to play in the governance of the internet.

The centre of the private internet governance regime consists of private, non-state institutions. The governance bodies are not treaty bodies, nor are they international organisations. The internet infrastructure's technical standards and governance bodies, such as the Internet Engineering Task Force (IETF), ICANN, and Regional Internet Registries (RIRs) are dominated by the transnational corporations that design and sell networking equipment, provide services or operate networks. The IETF, ICANN, and the RIRs together set the "rules of the road" (Wu et al. 2007); that is, they produce the preconditions of the interoperability of independent networks by providing the coordination and distribution of unique numbers to all connected networks and devices on the internet, the service that translates human-readable addresses into numbers, as well as the open voluntary protocols that allow these interconnected devices and networks to communicate. The IETF, ICANN, and the RIRs are bodies that have grown and developed in conjunction with the internet and are fully and exclusively dedicated to its coordination and operation. Because these bodies provide the bare minimum of technical preconditions for the internet to function, they are often understood as the core internet governance bodies. Whereas internet governance, or at least the self-regulatory private internet governance regime, is often a synonym for these bodies, these specific institutions are not mentioned in definitions of internet

governance. The institutional configuration of these organisations, such as their processes, procedures, and organisational culture and other affordances, does play a significant role in the shaping on the internet infrastructure. One could understand this as a blind spot in the internet governance definitions provided earlier, because they do not take into account the "mosaic" (Dutton and Peltu 2005), or "bricolage" (Radu 2019), of governance institutions involved in, and traditionally associated with, internet governance, such as the IETF, ICANN, and RIRs. The guiding norms of interconnection and interoperability are also encoded in the bylaws, technical documents, and policy documents. For instance, in the founding document of the RIR for Europe, West Asia (i.e., the Caucasus and Iran) and the Middle East, Reseaux IP Europeans, it reads: "RIPE promotes and coordinates interconnection of IP networks within Europe and to other continents" (RIPE 1992). This is just to illustrate that the private internet governance regime is not a "neutral" meeting platform, if such a thing could exist, but rather a normative regime. The prominent internet governance scholar Laura DeNardis, meanwhile, provides a definition that includes private internet governance bodies but also clearly highlights that internet governance does not stop there and includes the role of technology, states, and international agreements. This definition thus combines the first two definitions but adds institutions, practices, and the role that design of architecture plays:

> the practice of internet governance extends beyond institutions such as the Internet Corporation for Assigned Names and Number and standards-setting organisations to include private industry policies, national policies, international treaties, and the design of technical architecture.
>
> (DeNardis 2014, 19)

Van Eeten and Mueller, for their part, put the centre of gravity of internet governance beyond these institutions to emphasise the influence of the private sector. They argue that "the aggregate effect of decentralised decisions and adjustments made by ISPs . . . have much more profound effects on the evolution and use of the internet than the ICANN" (Van Eeten and Mueller 2013, 727). While it might be true that actors such as internet service providers (ISPs) undertake regulatorily consequential actions, many of the decisions made outside of the aforementioned formal internet governance bodies are still mediated by trust relations and connections that are built at the meetings that are organised by these governance bodies, as convincingly shown by Ashwin Mathew in his work on the governance of internet routing (Mathew 2014). In other words, making the definition of internet governance too inclusive risks reducing its conceptual utility. Hofmann, Katzenbach, and Gollatz offer an escape out of this conundrum by defining governance as "critical moments" when routine activities become problematic and need to be revised, thus, when regular coordination itself requires coordination" (Hofmann, Katzenbach and Gollatz 2016, 1406). This approach helpfully locates internet governance in a combination of practices of reflexive coordination, and thus ensures that not all practices involving the internet infrastructure are understood

as internet governance, but does include a wide array of practices, venues, and actors. That said, while this seems an elegant theoretical solution that includes activities both inside and outside of governance bodies, it does not describe *where* these practices of internet governance take place and *who* undertakes them. This makes internet governance a large, nebulous object with blurry edges that is hard to describe or interrogate, which in turn makes it hard to research larger trends about how the internet infrastructure is being shaped through its transnational governance.

Another way of locating internet governance is by understanding that "[a]rrangements of technical architecture are arrangements of power" (DeNardis 2014, 7). To uncover practices of internet governance is to locate "the politics of this architecture" (DeNardis 2014, 7). To do this, one can trace patterns of ownership, power, and reconfigurations in the internet infrastructure and particularly in the exercise of control (Musiani et al. 2015), which is especially relevant when it comes to control over main "chokepoints" (Tusikov 2016, 36), or "control points" (Choucri and Clark 2018, 168). In addition to large data transit providers that interconnect networks and operate (submarine) cables, content distribution networks and internet exchange points, governance and standard-setting institutions such as ICANN, IETF, and RIRs are prime examples of such points of focus, because these are persistent fields of convergence of coordination, collaboration, and policy development in internet governance. Not only are the formal processes that these bodies facilitate important, but also the building of trust, reputation and personal relations, which is an essential part of these coordination processes, happens to a significant degree at the meetings that these institutions organise (Mathew 2014; Meier-Hahn 2014). While not all internet governance takes place in governance and standard-setting institutions, these are main focus points for coordination and a place where many of the players in inter-networking meet to engage in industry self-regulation, or, in the *parlance* of the field, bottom-up coordination (Sowell 2012). Also, reverberations and responses to significant changes in the internet infrastructures are discussed and sometimes addressed in, through, and by these institutions.

The previous sections show how internet governance definitions are both descriptive and normative and how they include, exclude, or emphasise the role of governments, corporations, civil society, technological design, governance institutions, and reflexive practices. Another approach to internet governance is through how power is exercised through the internet infrastructure. This approach emphasises the role of institutional configuration, epistemic communities, and interpersonal relations that are important building blocks of the private internet governance regime that I will further describe in the following section.

The rise of the private internet governance regime

The commercialisation of the internet at the beginning of the 1990s led to the rise of the private internet governance regime, which one can understand by looking at the relevant arrangements of power. Many expected that the distributed

architecture of the internet and its private governance would lead to perfect markets, free competition, and decentralised structures (Litan and Rivlin 2001; Wu 2018). However, as we now know, this did not happen. Rather, "market concentrations, control, and power struggles are categories to adequately describe the fundamental dynamics of the commercial internet" (Dolata and Schrape 2018, 85). Instead of leading to competition and innovation (Cowhey, Aronson and Richards 2009; Van Schewick 2012; Powers and Jablonski 2015), it actually led to the emergence of internet oligopolies (Mansell and Javary 2002; Smyrnaios 2018), such as Google, Amazon, Cloudflare, Cisco, Huawei, and Juniper. The internet has long had a privatised component; already in the 1980s corporations were connected to the internet, and networks were often produced and maintained by companies such as Bolt Beranek and Newman (BBN), then called Interface Message Processor (IMP), that built the first router. Nonetheless, in these early days the oversight over the development of the internet architecture was still managed through publicly funded agencies and academic institutions. In the 1980s, the internet was also already connected to commercial services, such as mail providers like SprintMail and Compuserve (Kahin 1990), but commercialisation was still limited because commercial traffic was not allowed on the network due to the Acceptable Use Policy (AUP) that governed the internet backbone, which was funded by the National Science Foundation (NSF).[1]

However, the growth of the use of the internet by the end of the 1980s and beginning of the 1990s seriously congested the internet backbone that was run by the NSF. Several options were explored to increase the capacity of the internet and the backbone. Of the different options, such as establishing national research networks, commercialisation of the internet backbones was perceived as the best option to scale the network (Kahin 1990; Chinoy and Salo 1997), which fitted with the "end of history" (Fukuyama 2012) sentiment that was en vogue in that period, which translated in a limited role of government and a belief in neoliberal market economies. The decision to pursue commercialisation led to the creation of the Commercial Internet Exchange, which overcame the limitations set by the AUP because there was no longer a central backbone funded by public money. This alleviated a burden on public funding and replaced it with private capital, which resulted in the commercialisation and further privatisation of the internet (Frischmann 2001). Some understand this as the retreat of government from internet governance, which fits into a straightforward story implicit in the Mueller definition and argument mentioned earlier in which state and civil society interests (beyond maximising interoperability) are treated as illegitimate. Others, however, have argued that this has actually led to the galvanisation of the power of the United States, through the dominance of the American companies (e.g., Carr 2015). I build on the thinking of Madeline Carr by interpreting the de-funding of the backbone by the US government as an act of metagovernance – that is, "the coordination of one or more governance modes" via different methods and strategies. From this perspective, the US government did not retreat from internet governance. Instead, it engaged in governance by other means, in this case, outsourcing the growth of the internet to the private sector through the establishment

of a transnational private internet governance regime. This decision spurred the formal institutionalisation of the IETF, RIRs, and ICANN. Commercialisation of the internet was not a retreat from governmental control, but a transition from direct governance to indirect governance through norm-setting and institutional design. Industry was tasked with meeting particular US goals of increasing interconnection between independent networks, without incurring direct costs for government. And so it did, but with consequences that were not directly foreseen.

Norms in the private internet governance regime

The commercialisation and the privatisation of the internet that started at the end of the 1980s led to the formal institutionalisation of the private internet governance regime with the official institution of RIRs, the IETF, and ICANN. These bodies were supposed to coordinate interconnection between independent networks following voluntary standards. A popular saying among IETF engineers captures the single-minded focus on this mission: "The IETF is not the protocol police." (Among RIR network operators the equivalent saying is, "We are not the routing police.") However, these sayings fail to identify who actually *is* the protocol or routing police. The answer, it turns out, is surprisingly simple: There is no police, at least if one thinks of police in terms of a restricting authority. The private internet governance regime is not aimed at limiting or restricting interconnection; to the contrary, and true to the private regime's embedded norms, it is aimed at creating more interconnection and interoperability. The private internet governance regime does not create limitations but creates incentives for cooperation among competitors (Meier-Hahn 2014). The participants in these bodies do what they describe as acting "for the good of the internet" (Mathew 2014), and this dominant norm translates in an increase in network capacity, meaning higher bandwidths and lower latency, for more interoperable devices. This norm benefits certain groups: network operators, vendors, and service providers (Powers and Jablonski 2015) through a network effect. More interconnected networks, and interconnection among networks, produces an increase in value for all interconnected networks (Lemley 1997). Within this normative framework, within the private internet governance regime, debates centre not on *whether* more interconnection and interoperation should be created: This is taken as a given. Rather, they focus on *how* this should happen. The private internet governance regime is an instrument for the increase of data traffic through the production of interconnection and interoperability between transnational corporations.

Other norms that are often professed in internet governance, such as openness and decentralisation, are deprioritised when they come in conflict with the prevailing normative framework of interconnection and interoperability. The distributed design of internet governance was supposed to prevent centralised decision-making as much as possible, to ensure that no one party or group would have significant sway over another. The sedimentations of these design choices can be found in the formalisation of the policy and specification development processes in these bodies that all have been organised around the principle of

openness (Russell 2014; ten Oever 2021 forthcoming). Openness here should be understood as the public availability of process and outcome documents, discussion archives, as well as participatory decision-making. This has led to drawn-out, specialised, highly proceduralised, and resource-intensive processes. Ironically this "openness" design has had the effect of closing down these decision-making processes for everyone who has not been initiated into the processes and vocabulary of this environment because it leads to a torrent of often interrelated documents, emails, calls, and meetings in which one can participate. This flood of information can be hard to navigate, as it takes not only experience to filter the information based on relevance but also expert knowledge to understand the content. For example, the guide to abbreviations used in internet governance that is produced regularly by the not-for-profit DiploFoundation, currently runs to 34 pages and over 150 abbreviations (DiploFoundation n.d.). Because of the need for expert knowledge of technologies and processes in order to effectively participate, compounded with the resources and time needed to acquire this knowledge and participate in these meetings and conversations, the practice of open and distributed internet governance revolves around a relatively small group of experts that form a global elite (Scholte 2017) that regularly attend internet governance meetings that take place several times per year in large hotels and conference venues on different continents. While the bodies might have different areas of operations, and different institutional configurations, the number of people actively partaking in decision-making in these bodies is quite small, and the number of organisations they represent is significantly smaller and getting smaller every year due to consolidation in the market. Thus, the open decision-making process in the private internet governance regime has not led to more openness, but it has facilitated private self-coordination for the production of more interoperation and interconnectivity.

Governmental requests and the rise of the multilateral internet governance regime

When governments largely delegated the scaling of the internet to the private sector (while holding some indirect involvement and oversight), the internet could grow without governments worrying about the economic and financial overhead costs and risks for themselves. However, when this private governance regime was optimised for its intended purposes of increasing interconnection and interoperation, it came with significant consequences for the ability of governments to influence this regime.

Private internet governance can be largely understood as an example of normative industry self-coordination that is optimised through the institutional configuration of distributed bodies to increase interconnection and interoperability between networks and devices. When the private internet governance regime is expected or requested to perform other roles that do not fit with the underlying norms of increasing connectivity and interoperability, it regularly fails to deliver, for instance, when the private internet governance regime is asked to consider the societal impact of their policies and technologies. This becomes glaringly clear when governments make requests to the private internet governance regime to inscribe or encode social

or legal norms which might not increase interconnectivity or interconnections. Such conflicts between two normative systems is typical within regime complexes. I will provide four recent examples of this in the internet governance regime complex. These examples demonstrate that when states have concrete policy objectives they seek to pursue by means of the internet infrastructure, the private internet governance regime resists their requests because states' requests were in conflict with their norm for increasing interconnection and interoperation.

WHOIS and GDPR

An interesting example where internet governance was unable to accommodate the needs of states started with ICANN's lack of response to the formal requests of the European Commission to limit access to the private information of registrants of websites via the publicly available WHOIS registry. The WHOIS registry is a service that everyone can access to look up the contact information, often including the physical address, of the person or entity who registered a domain name. For the European Commission, this presented a violation of the right to privacy of domain registrants and European privacy laws (Perrin 2018), as they documented in their letters to ICANN in 2006 and 2007 (Article 29 Data Protection Working Party 2006, 2007). ICANN never responded to these letters. Only when the European Commission developed its own rules, namely the Europe-wide, enforceable, General Data Protection Regulation in 2016, ICANN started a process to devise an alternative to the existing WHOIS registry.

For the private internet governance regime, embodied in ICANN in this example, the WHOIS registry was understood as an artefact that enabled interconnection and interoperability. This was actually one of the reasons that the WHOIS registry was invented in the internet's early years: to be able to find the contact information connected to a malfunctioning network. The European Commission found that the WHOIS registry violated the privacy of website owners. The private internet governance regime prioritised here interconnection and interoperability – they emphatically did not want different WHOIS systems for different parts of the world – over the norms of the European Commission.

Snowden revelations of US mass surveillance

Another example that shows how internet governance bodies are bad interfaces for government policies was the response to the Snowden revelations by the IETF. In response to the revelations of widespread American state surveillance, the IETF adopted a document called "Pervasive Monitoring Is an Attack" (Farrell and Tschofenig 2014). At the same time, the Internet Architecture Board, a prominent committee of the IETF, adopted a statement urging "protocol designers to design for confidential operation by default" (Morgan 2014), which heralded a widespread use of encryption in protocols to thwart the US government's ability to continue its surveillance practices. These documents by themselves were reminiscent of a document released in May 2000, in which the IETF stated that

it would not standardise interfaces for wiretapping or interception technologies in the technologies they develop and standardise (Internet Architecture Board and Internet Engineering Steering Group 2000). With these actions, the IETF went straight against requests by and perceived needs of the United States government, namely the ability of law enforcement agencies and other government services to access private internet communications.

The IETF has made it clear, time and again, that they do not want to facilitate the weakening of encryption or the construction of back doors to provide access to law enforcement agencies to data streams. One of the main arguments offered by the IETF is that a weakening of protocols would provide access not only to law enforcement agencies but also to others, which would weaken trust in the network. That would in turn negatively impact interconnectivity. The US government, as well as other governments, however, has never ceased asking and looking for such capabilities.

Chinese draft law and verification service providers

US government and European Commission requests are not the only ones that are denied by the private internet governance regime. In 2006, the Chinese government published draft legislation (Creemers 2016) which contained a provision that would mandate all internet domain names in China to be registered through government-licensed service operators. Verisign, the world's largest domain registry, developed a proposed technical standard[2] to implement verification service providers through the Extensible Provisioning Protocol (EPP). EPP is the protocol that is used by domain registries and registrars to register domains. This would have added the possibility of verification service providers to acknowledge that someone's identity has been verified. The verification service provider would check whether someone, based on their identity, would be allowed to register a specific domain.

Permissionless innovation – the ability to develop and implement protocols and services without having to ask for permission – has been one of the principles underlying the internet's interconnectiveness and interoperability. When one is asked to register in the WHOIS registry upon registering a domain, your identity is not verified, and receiving it does not depend on *who you are* or whether you are allowed to have that domain. The Chinese government's proposal would have gone against this policy. And even though American company Verisign, the registry of the largest top-level domain in the world, was eager to enter this market and create a technical norm to accommodate that proto-legal norm, there was a significant amount of criticism in the IETF working group which caused Verisign to discontinue the work on the proposed standard.

Schengen routing

A final example is the proposal that has been brought up by several governments and which has been resisted by engineers and network operators time after time: internet routing based on geographical borders, such as Schengen routing (Dönni et al. 2015). The proposal prescribes that internet traffic originating from and destined for

a certain country, or group of countries, would stay within that territory. Time and again, it has been argued that the internet does not recognise geographical borders (Mueller 2017). This is not because it is a technological or social impossibility to make this happen, but it is rather a design choice made primarily by network operators. Networks could be limited to one jurisdiction, and routing rules could be developed to preferably or exclusively route internet traffic among specific networks in a specific jurisdiction. This possibility, however, has been repeatedly rejected by network operators and network equipment vendors in the private internet governance regime because this could lead to less internet interconnection and interoperability between networks. This illustrates perfectly how norms requested by the multilateral internet governance regime for technical infrastructure to accommodate national or regional social and legal norms get resisted by the private internet governance regime because it hampers interconnection and interoperation.

In each of these four examples, the private internet governance regime resisted the introduction of norms by governments in the internet infrastructure. This shows that the bodies that make up the private internet governance regime produce interconnection and interoperation and support norms favouring these outcomes. States, rather, seek to introduce limitations to fit the network (and its inherent normative biases) to their particular norm regimes, which must address other policy issues beyond maximising interconnection. The inability, or unwillingness, of the private internet regime to accommodate these requests by nation states has led to the rise of a multilateral internet governance regime. The private internet governance regime and the multilateral internet governance regime jointly make up the transnational internet governance regime complex. In the multilateral internet governance regime, states seek to align the technical infrastructure with national and regional social and legal norms.

This attempt by state governments to contest interoperability norms has led scholars such as Milton Mueller, one of the co-authors of the second internet governance definitions cited earlier, to argue that there is a misalignment between internet governance and national sovereignty (Mueller 2017). According to Mueller, internet governance produces (or, rather, should produce) one global internet, while nation states seek to apply rules based on their own limited territorial reach.

Mueller's argument is worth unpacking, because it gets to the heart of what it means, from a metagovernance perspective, to see internet governance as a regime complex of sometimes-overlapping institutions and regimes, rather than as a unidimensional regime that converges around one single set of norms (in this case, related to interoperability). While Mueller sees states' actions as a challenge to an existing internet governance regime, these state actions can also be understood as a next step in the "process of defining, delimiting, and inscribing space" in cyberspace, involving a "process of deterritorialisation and reterriorialisation" (Lambach 2019, 2–3). However, the limited normative scope of a private internet governance regime, supporting and focusing exclusively on the norms of increased interconnection and interoperation, means that states are unable to realise their public-policy objectives via the regime as it currently exists.

Unable to work through the narrow interconnection-focused regime, we have seen actions such as the introduction of the General Data Protection Regulation of the European Commission (Kulesza 2018; Perrin 2018) and the Russian "sovereign internet" regulation (Stadnik 2019; this volume). Such moves are new milestones in the governance of the internet infrastructure, since they could form the beginning of a trend in state-based rule-setting on internet infrastructure, which is inherently different from the private "multistakeholder" internet governance regime. A similar trend in states engaging in intergovernmental initiatives for norm-setting for the internet can also be observed in initiatives such as the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and the United Nations Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security. These multilateral efforts should also be understood as inherent part of the emerging multilateral internet governance regime. In contrast to Mueller's interpretation of this emerging regime as a threat to privatised internet governance, a metagovernance approach highlights that it, together with the private internet governance regime, make up an internet governance *regime complex*.

From this perspective, we can understand the internet governance regime *complex* as follows. The private internet governance regime is guided by the norm of creating more interconnection and interoperation. The multilateral internet governance regime, on the other hand, serves to shape the internet to the norms of states and limits interconnection and interoperation. These two regimes should not be understood as opposing forces, but rather as two different parts of the internet governance regime complex. Aside from being composed of distinguishable parts, such as the Internet Governance Forum on the multilateral side and the IETF on the private governance side, they do not focus on different areas. If they did, we would be able to classify them as sub-regimes. Instead, these two regimes have different purposes, while they both seem to design and optimise the internet infrastructure to function according to their respective objective, namely the increase in interconnection and interoperability or the accommodation of technical norms to local norms, which makes these different regimes instruments of metagovernance.

The private internet governance regime's features and limitations are the product of a "mobilisation of bias," through which "some issues are organised into politics while others are organised out" (Schattschneider 1975, 71). In this case, the interconnection and interoperation norms are organised in. They lie at the heart of the private internet governance regime and the internet's technical standards: "The goal is connectivity, the tool is the Internet Protocol"; "connectivity is its own reward" (Internet Architecture Board 1996, 1). Crucially, this private regime was shaped in this manner by governments, most significantly the US government, via processes of commercialisation and privatisation. This perspective helps to restore governments into the internet-governance picture. The limitation of interoperation and interconnection by governments through the multilateral internet governance regime should be understood as an internet governance practice and not as something that is misaligned with internet governance. It is solely misaligned with (parts of) the private internet governance regime.

Discussion

States' (particularly the United States') decision to commercialise and privatise the internet's infrastructure led to the emergence of the private internet government regime and, later, the multilateral internet governance regime. The commercialisation of the internet was not an example of the retreat of government, but rather a transition from direct governance to a process of metagovernance through the dialectics between two normatively limited regimes: one focused on interconnectivity and the other on other norms. Efforts by governments to govern the internet through the multilateral internet governance regime, irrespective of how they are framed or the goals that are claimed, limit the increase in interoperation and interoperability of the private internet governance regime but rather seek the technical infrastructure to accommodate to social and legal norms.

The metagovernance heuristic used in this chapter is not solely an analytical lens to allow us to discern the functional differentiation between the regimes of the internet governance regime complex. It also offers the practical opportunity to explore why some norms get embedded in policies and technologies and why some are not. This brings about possible reflections on the societal impact of the development of technological norms through this regime complex. The social and legal impact of the internet has been a topic of discussion since its early inception. In her analysis of early technical internet standards documents, the so-called RFC-series, Braman shows how norms, privacy, security, rights, and freedoms have been part and parcel of early technical discussions about the internet (2011, 2012). There also exists an extensive literature on the norms and values that have been embedded in the internet infrastructure (Orwat and Bless 2016; Shilton 2018; Zittrain 2008), and scholars have also asked whether the internet infrastructure should be designed to accommodate different value systems (Clark et al. 2005), or rather have specific values embedded in them, for instance through the use of value-sensitive design approaches (Brown, Clark and Trossen 2010; Friedman, Kahn and Borning 2008). There also have been calls to encode specific sets of values in the internet infrastructure (Cath and Floridi 2017) or at least consider the implications of policies and technical proposals structurally on their societal impact (Morris and Davidson 2003). Despite all this, norms beyond interoperability and interconnectivity have never been operationalised through the private internet governance regime.

The heuristic of metagovernance allows us to make a functional differentiation between the private and the multilateral internet governance regimes. This differentiation highlights the tools of metagovernance, such as norms and institutional design, that are used to structure these regimes and fundamentally make the internet work in the way it does. The differentiation also helps to explain why the private internet governance regime does not take the structural impact of technology on society into account.

The lack of structural evaluation of the societal impact of technological norms in the private internet governance regime is not because existing institutions lack the capacity to evaluate and implement policies and frameworks supporting different norms or because there is a lack of interest among various individuals involved in the internet governance regime complex. Rather, as I noted earlier, norm evaluation is happening, but it occurs through the lens of the embedded and guiding

norm of the specific regime. In the case of the private internet governance regime, this is the norm of interconnection and interoperation. Proposed new voluntary norms are evaluated against these deeply enshrined and institutionally and infrastructurally embedded norms that guide the community of the bodies that make up the private internet governance regime. Freedom of speech and freedom of expression are rights that are widely supported within the private internet governance regime because expression fits very well with increasing interoperation and interoperability. On the other hand, the operationalisation of the right to privacy, such as in the case of WHOIS and the GDPR or Schengen routing, or the right to nondiscrimination, is more likely to be enacted through the limitation of interconnectivity and interoperation through the multilateral internet governance regime. This is because privacy requires data minimisation, and Schengen routing implies limited interoperation between networks.

Conclusion

Existing definitions and understandings of internet governance largely focus on stakeholder groups, institutions, and practices. In this chapter I have sought to show how one can make effective functional differentiations between governance regimes within the internet governance regime complex, using the lens of metagovernance. By understanding these regimes through their embedded norms, one obtains a higher-level view to the vast field of internet infrastructure and its governance. Subsequently, one is able to interrogate the respective regimes using their own respective norms. This shows that the governance of the internet infrastructure is by no means monolithic, nor is it random. Insight in the two norm regimes that make up the regime complex provide one with the ability to understand how power and control are exercised in this global network, namely through deeply embedded guiding norms, bound to norm regimes that transcend individual internet governance bodies and instruct the behaviour of those who engage in it. This analysis has also shown that the resurgence of the nation state through the rise of the multilateral internet governance regime is a direct consequence of the inability of the private internet governance regime to accommodate social and legal norms that do not increase interconnection and interoperability.

Notes

1 The Acceptable Use Policy. GENERAL PRINCIPLE:
(1) NSFNET Backbone services are provided to support open research and education in and among US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Use for other purposes is not acceptable.
UNACCEPTABLE USES:
(10) Use for for-profit activities, unless covered by the General Principle or as a specifically acceptable use.
(11) Extensive use for private or personal business.

Source: www.livinginternet.com/doc/merit.edu/acceptable_use_policy.htm, accessed 28 November 2019.

2 For the Verification Code Extension for the Extensible Provisioning Protocol, see https://tools.ietf.org/html/draft-ietf-regext-verificationcode-06, Accessed 29 November 2019.

References

Alter, Karen J., and Kal Raustiala. 2018. "The Rise of International Regime Complexity." *Annual Review of Law and Social Science* 14 (1): 329–349. https://doi.org/10.1146/annurev-lawsocsci-101317-030830.

Article 29 Data Protection Working Party. 2006. *European Commission. Letter to ICANN Board of Directors Chairman*. 22 June. www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf. Accessed 29 November 2019.

Article 29 Data Protection Working Party. 2007. *Subject: Comments on the GNSO Whois Task Force Preliminary Task Force Report on Whois Services of 22 November 2006; and on the Draft ICANN Procedure for Handling Whois Conflicts with Privacy Law of 3 December 2006*. European Commission. Letter to ICANN Board of Directors Chairman. 12 March. 22 June. www.icann.org/en/system/files/files/schaar-to-cerf-12mar07-en.pdf. Accessed 29 November 2019.

Braman, Sandra. 2011. "The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979." *The Information Society* 27 (5): 295–310. https://doi.org/10.1080/01972243.2011.607027.

Braman, Sandra. 2012. "Privacy by Design: Networked Computing, 1969–1979." *New Media & Society* 14 (5): 798–814. https://doi.org/10.1177/1461444811426741.

Braman, Sandra. 2020. "The Irony of Internet Governance Research: Metagovernance as Contextpractices." In *Research Methods in Internet Governance*, edited by Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, and Francesca Musiani. Cambridge, MA: MIT Press.

Brown, Ian, David D. Clark, and Dirk Trossen. 2010. "Should Specific Values Be Embedded in the Internet Architecture?" In *Proceedings of the Re-Architecting the Internet Workshop*, 10:1–10:6. ReARCH'10. New York: ACM. https://doi.org/10.1145/1921233.1921246.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium* 43 (2): 640–659. https://doi.org/10.1177/0305829814562655.

Cath, Corinne, and Luciano Floridi. 2017. "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights." *Science and Engineering Ethics* 23 (2): 449–468. https://doi.org/10.1007/s11948-016-9793-y.

Chinoy, Bilal, and Timothy J. Salo. 1997. "Internet Exchanges: Policy-Driven Evolution." In *Coordinating the Internet*, edited by Brian Kahin and James H. Keller, 325–345. Cambridge, MA: MIT Press. http://dl.acm.org/citation.cfm?id=275025.275053.

Choucri, Nazli, and David D. Clark. 2018. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA: MIT Press.

Clark, D.D., John Wroclawski, Karen R. Sollins, and Robert Braden. 2005. "Tussle in Cyberspace: Defining Tomorrow's Internet." *IEEE/ACM Transactions on Networking* 13 (3): 462–475. https://doi.org/10.1109/TNET.2005.850224.

Cowhey, Peter F., Jonathan D. Aronson, and John Richards. 2009. "Shaping the Architecture of the US Information and Communication Technology Architecture: A Political Economic Analysis." *Review of Policy Research* 26 (1–2): 105–125. https://doi-org.proxy.library.brocku.ca/10.1111/j.1541-1338.2008.00371.x.

Creemers, Rogier 2016. "Internet Domain Name Management Rules (Opinion-seeking Revision Draft)." *China Copyright and Media*. 25 March. https://chinacopyrightandmedia.

wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/. Accessed 4 August 2020.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

DiploFoundation. n.d. *Internet Governance Acronym Dictionary*. Version 3.0. www.diplomacy.edu/sites/default/files/IG_Acronym_glossary_2019.pdf. Accessed 27 November 2019.

Dolata, Ulrich, and Jan-Felix Schrape. 2018. *Collectivity and Power on the Internet: A Sociological Perspective*. SpringerBriefs in Sociology. Springer International Publishing. www.springer.com/de/book/9783319784137.

Dönni, Daniel, Guilherme Sperb Machado, Christos Tsiaras, and Burkhard Stiller. 2015. "Schengen Routing: A Compliance Analysis." In *Intelligent Mechanisms for Network Configuration and Security*, edited by Steven Latré, Marinos Charalambides, Jérôme François, Corinna Schmitt, and Burkhard Stiller, 100–112. Lecture Notes in Computer Science. Cham: Springer International Publishing.

Dutton, William H., and Malcolm Peltu. 2005. "The Emerging Internet Governance Mosaic: Connecting the Pieces." *SSRN Scholarly Paper ID 1295330*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=1295330.

Erskine, Toni, and Madeline Carr. 2016. "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." In *International Cyber Norms: Legal, Policy & Industry Perspectives*. Tallinn: NATO CCD COE Publications.

Farrell, Stephen, and Hannes Tschofenig. 2014. "RFC7258 – Pervasive Monitoring Is an Attack." *RFC – Series*. IETF. https://tools.ietf.org/html/rfc7258.

Friedman, Batya, Peter H. Kahn, and Alan Borning. 2008. "Value Sensitive Design and Information Systems." In *The Handbook of Information and Computer Ethics*, edited by Kenneth Einar Himma and Herman T. Tavani, 69–101. Hoboken: John Wiley & Sons.

Frischmann, Brett. 2001. "Privatization and Commercialization of the Internet Infrastructure." *Science and Technology Law Review* 2: 1–25. https://doi.org/10.7916/stlr.v2i0.3537.

Fukuyama, Francis. 2012. *The End of History and the Last Man*. New York: Penguin.

Gjaltema, Jonna, Robbert Biesbroek, and Katrien Termeer. 2019. "From Government to Governance . . . to Meta-Governance: A Systematic Literature Review." *Public Management Review* 1–21. https://doi.org/10.1080/14719037.2019.1648697.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2016. "Between Coordination and Regulation: Finding the Governance in Internet Governance." *New Media & Society* 19 (9): 1406–1423. https://doi-org.proxy.library.brocku.ca/10.1177%2F1461444816639975.

Hofmann, Jeanette. 2005. "Internet Governance: A Regulative Idea in Flux." *SSRN Scholarly Paper ID 2327121*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2327121.

Hofmann, Jeanette. 2016. "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice." *Journal of Cyber Policy* 1 (1): 29–49. https://doi.org/10.1080/23738871.2016.1158303.

Internet Architecture Board. 1996. *RFC1958 – Architectural Principles of the Internet*. https://tools.ietf.org/html/rfc1958.

Internet Architecture Board, and Internet Engineering Steering Group. 2000. "RFC2804 – IETF Policy on Wiretapping." *RFC – Series*. IETF. https://tools.ietf.org/html/rfc2804.

Jessop, Bob. 1997. "Capitalism and Its Future: Remarks on Regulation, Government and Governance." *Review of International Political Economy* 4 (3): 561–581. https://doi-org.proxy.library.brocku.ca/10.1080/096922997347751.

Kahin, B. 1990. "RFC1192 – Commercialization of the Internet Summary Report." *RFC-Series*. IETF.

Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36 (2): 185–205. https://doi-org.proxy.library.brocku.ca/10.1017/S0020818300018920.

Kulesza, Joanna. 2018. "Balancing Privacy and Security in a Multistakeholder Environment. ICANN, WHOIS and GDPR." *The VISIO Journal* 49. http://4liberty.eu/balancing-privacy-and-security-in-multistakeholder-environment-icann-whois-gdpr/.

Lambach, Daniel. 2019. "The Territorialization of Cyberspace." *International Studies Review* vix022: 1–25. https://doi.org/10.1093/isr/viz022.

Lemley, Mark A. 1997. "The Law and Economics of Internet Norms." *Chicago-Kent Law Review* 73 (4): 1257.

Litan, Robert E., and Alice M. Rivlin. 2001. "Projecting the Economic Impact of the Internet." *American Economic Review* 91 (2): 313–317.

Mansell, Robin, and Michele Javary. 2002. "Emerging Internet Oligopolies: A Political Economy Analysis." In *An Institutionalist Approach to Public Utilities Regulation*, edited by E. Miller and W. J. Samuels, 162–201. East Lansing, MI: Michigan State University Press.

Mathew, Ashwin J. 2014. *Where in the World Is the Internet? Locating Political Power in Internet Infrastructure*. Berkeley, CA: University of California Press. www.ischool.berkeley.edu/research/publications/2014/where-world-internet-locating-political-power-internet-infrastructure.

Meier-Hahn, Uta. 2014. "Internet Interconnection: How the Economics of Convention Can Inform the Discourse on Internet Governance." In *GigaNet: Global Internet Governance Academic Network, Annual Symposium*. https://dx.doi.org/10.2139/ssrn.2809867.

Morgan, Cindy 2014. *IAB Statement on Internet Confidentiality*. Internet Architecture Board. 14 November. www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/.

Morris, John, and Alan Davidson. 2003. "Policy Impact Assessments: Considering the Public Interest in Internet Standards Development." *SSRN Scholarly Paper ID 2060656*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2060656.

Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Hoboken: Wiley.

Mueller, Milton, John Mathiason, and Hans Klein. 2007. "The Internet and Global Governance: Principles and Norms for a New Regime." *Global Governance* 13 (2): 237–254.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. 2015. *The Turn to Infrastructure in Internet Governance*. 1st ed. New York: Palgrave Macmillan.

Orwat, Carsten, and Roland Bless. 2016. "Values and Networks: Steps toward Exploring Their Relationships." *ACM SIGCOMM Computer Communication Review* 46 (2): 25–31. https://doi-org.proxy.library.brocku.ca/10.1145/2935634.2935640.

Perrin, Stephanie E. 2018. *The Struggle for WHOIS Privacy: Understanding the Standoff Between ICANN and the World's Data Protection Authorities*. PhD Thesis. https://tspace.library.utoronto.ca/handle/1807/89738.

Peterson, Larry L., and Bruce S. Davie. 2007. *Computer Networks: A Systems Approach*. New York: Elsevier.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: University of Illinois Press.

Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford: Oxford University Press.

Raymond, Mark. 2019. *The Metastasization of the Global Cyber Regime Complex and the Creation of Critical Governance Infrastructure*. Presented at the International Studies

Association, Toronto, March. www.isanet.org/Conferences/Event-Detail/mid/6587/EventID/11827/ItemID/111384?popUp=true.

RIPE. 1992. "RIPE Terms of Reference." *RIPE NCC*. 29 November. www.ripe.net/publications/docs/ripe-001. Accessed 5 August 2020.

Russell, Andrew L. 2014. *Open Standards and the Digital Age*. Cambridge: Cambridge University Press.

Schattschneider, Elmer E. 1975. *The Semi-Sovereign People: A Realist's View of Democracy in America*. Boston, MA: Wadsworth, Cengage Learning.

Scholte, Jan Aart. 2017. *Complex Hegemony: The IANA Transition in Global Internet Governance*. Presented at the Giganet Annual Symposium, Geneva. https://igf2017.sched.com/event/CRB7/the-12th-annual-symposium-of-the-global-internet-governance-academic-network-giganet.

Shilton, Katie. 2018. "Engaging Values Despite Neutrality: Challenges and Approaches to Values Reflection during the Design of Internet Infrastructure." *Science, Technology, & Human Values* 43 (2): 247–269. https://doi.org/10.1177/0162243917714869.

Smyrnaios, Nikos. 2018. *Internet Oligopoly: The Corporate Takeover of Our Digital World*. Bingley: Emerald Publishing Ltd.

Sørensen, Eva, and Jacob Torfing. 2009. "Making Governance Networks Effective and Democratic through Metagovernance." *Public Administration* 87 (2): 234–258. https://doi-org.proxy.library.brocku.ca/10.1111/j.1467-9299.2009.01753.x.

Sowell, Jesse H. 2012. "Empirical Studies of Bottom-up Internet Governance." In *Proceedings of the 40th Research Conference on Communications, Information, and Internet Policy*. Arlington, VA: Telecommunications Policy Research Consortium.

Stadnik, Ilona. 2019. "Internet Governance in Russia – Sovereign Basics for Independent Runet." In *TPRC47 Proceedings*. Washington, DC: TPRC. https://papers.ssrn.com/abstract=3421984.

ten Oever, Niels. 2021 Forthcoming. "'This Is Not How We Imagined It' – Technological Affordances, Economic Drivers and the Internet Architecture Imaginary." *New Media & Society*.

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. Berkeley, CA: University of California Press.

United Nations. 2005. "Tunis Agenda for the Information Society." *World Summit on the Information* Society. WSIS-05/TUNIS/DOC/6(Rev.1)-E. 18 November. www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Van Eeten, Michael J.G., and Milton L. Mueller. 2013. "Where Is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–736. https://doi-org.proxy.library.brocku.ca/10.1177%2F1461444812462850.

Van Schewick, Barbara. 2012. *Internet Architecture and Innovation*. Cambridge: MIT Press.

Verhulst, Stefaan G., Beth S. Noveck, Jillian Raines, and Antony Declerq. 2014. "Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem." *Centre for International Governance Innovation*, December. www.cigionline.org/publications/innovations-global-governance-toward-distributed-internet-governance-ecosystem.

Wu, Tim. 2018. *The Curse of Bigness: Antitrust in the New Gilded Age*. New York: Colombia Global Reports.

Wu, Tim, David Gross, Esther Dyson, Michael Froomkin, A.A. Dyson, and A.A. Gross. 2007. "The Future of Internet Governance." In *Proceedings of the ASIL Annual Meeting* 101: 201–213. https://doi.org/10.1017/S0272503700025660.

Zittrain, Jonathan. 2008. *The Future of the Internet – And How to Stop It*. New Haven, CT: Yale University Press.

4 The data-driven economy and the role of the state

Dan Ciuriak and Maria Ptashkina

Introduction

The digital transformation of the global economy is driving profound changes in terms of how we produce goods and services, the ways in which we govern ourselves, the distribution of wealth, and thus the sources of social influence and political power. In the era of rapid technological change that started with the Industrial Revolution, we have witnessed economies and societies continuously transformed based on ownership of the essential factor of production of the day and command of the economic rents that flow to that factor. The emergence of the data-driven economy (DDE) with the digital transformation in which data is the essential factor of production thus signals the transition to a new era. This chapter contends that this transition has profound implications for the role for the state. By extension, it argues that current international institutions and fora are insufficient for regulating data and the plethora of issues to which it is giving rise, necessitating new international rules.

Understanding the functioning of the DDE, which is powered by the data generated by the myriad daily routines of digitally connected individuals and machines, entails recognising the implications for economic and social change that come with the emergence of such an economy. Modern technology enables the "datafication" of virtually every aspect of human social, political, and economic activity. The ubiquitous devices that capture data include computers and cellphones connected to the internet and social media platforms, fitness trackers, security cameras in buildings, satellites tracking position, sensors in pipelines, and chips in smart equipment of all sorts, from cars to tractors to refrigerators. While, originally, the main growth of data was in areas related to personal use of the internet, the area where data accumulation is now truly exploding is in the Internet of Things (IoT) – machines talking to machines. The IoT is rapidly expanding to encompass all sectors of the economy as companies seek to exploit the capabilities of this new age. With ubiquitous monitoring, it is only a modest exaggeration to say that if it moves, it is measured.

Ever more powerful technology is being developed to exploit these new data assets. This includes scaling up computing power, specialised computer chips, and "deep learning" techniques based on neural networks that mimic the brain to train

DOI: 10.4324/9781003008309-6

artificial intelligence (AI) for inference and prediction. These new technologies allow the exploitation of previously unattainable information to power innovation across a rapidly growing set of "use cases" or applications. These technologies are disrupting existing markets and reshaping industries (e.g., the emergence of a "personal mobility" sector that promises to subsume and displace several industries, such as automobile manufacture, rental fleet management, and taxi service) as well as introducing new industries altogether (e.g., data analytics and a service industry for data storage and processing, such as cloud computing, software as a service, and so forth). New to production is machine knowledge capital, which competes with human capital the way robots compete with physical labour, complementing technologies that increase efficiency, and reduce costs for established industries through business and production process innovation.

The new economic and social environments stemming from the transition to a DDE (and data-driven society) are generating novel demands for governance and state intervention. This expanded role for the state not only pushes back against decades of economic orthodoxy that advocated for minimal governmental intervention in economic activity but entails a ramping up of government regulatory capacity and brings states into new rivalries with geo-economic and geopolitical overtones.

In this chapter, we review the economics of the digital era and trace the implications for the role of the state as economic agent, as regulator, and as the agent of power projection internationally to capture global rents. We make the case for the role of the state in the age of data and identify new regulatory challenges, including the geopolitical and geo-economic dimensions that have been set in sharp relief by the trade and technology disputes between the United States, the global data hegemon, and China, a state with the technological and economic capacity to challenge that role. We draw conclusions for international economic governance, focusing in particular on the rules-based system under the World Trade Organization (WTO), specifically laying out digital policy considerations for updating this central international economic-governance institution for the age of data.

Background: conceptualising the role of the state in the age of data

Economic eras, from feudalism to the data-driven economy

A scan of economic history suggests that the characteristics of an economy, the social orders that emerge from it, and the role of the state both in domestic governance and in international relations are shaped by the nature of the essential productive assets of the age and the technologies that exploit it. The historic transitions from the land-based economies of the feudal era to the mass production systems of the industrial era and the intellectual property (IP)-based models of the knowledge-based economy (KBE) generated new demands for collective action and created new opportunities for international rent capture, which modified the role of the state.

While change is continuous, we can nonetheless identify reasonably distinct historical economic eras, based on characteristics imbued by, or related to, the nature of the essential and relatively scarce factor of production of the age.[1] Table 4.1 classifies economic eras based on the role of land, machinery for mass production, IP, and data as the critical productive asset of each age and attempts to characterise each in terms of factors that shape the role of the state.

The dating of these eras is necessarily notional and impressionistic, as well as being tied to the transitions in the leading-edge economies; not all regions or countries experience these trends at the same time or to the same degree. For example, while historians date the start of the industrial revolution to as early as 1760 (Toynbee 1884), major innovations that were foundational for the industrial era came later and took some time to make their imprint on the age. Thus, the Watt-Boulton steam engine, while first put on the market in 1776, did not begin to transform transportation until the first decade of the 19th century, which witnessed the advent of the steam-powered railroad in 1804 (Lo 2015) and the steamship in 1807 (Ricci 2012). Similarly, the Luddite revolt against mechanised cotton weaving started only in 1811 (Whitney's iconic cotton gin was patented in 1794). Economic historian Jeffrey Williamson (1984) observes that "Somewhere around the 1820s Britain passed through a secular turning point." The post–Napoleonic War era was different from the preceding age and 1820 thus seems a reasonable dating point for this Zeitenwende.

Similarly, there appears to be an inflection point in the pace of the issue of patents in the United States around 1980, which coincides with the Carter Administration's passage of the Bayh Dole Act of 1980 to incentivise the commercialisation of research by American universities. This serves to demarcate the transition from the industrial age to the KBE in which the capitalisation of intangible knowledge assets starts to dominate.

The transition to a DDE is harder to date because national economic accounts have even yet to reflect the value of data. Concerted efforts to measure the economic value of data and other intangible assets on company balance sheets and national economic accounts date only to the mid-2000s (Corrado et al. 2012). One could date the transition to about this time, when the term "Big Data" was first used in its modern sense (in 2005; Dontha 2017), Yahoo created the Hadoop facility to process big data (also in 2005; Dontha 2017), Google went public (in 2004; Choo, 2005), Facebook debuted its advertising business (in 2007; Facebook 2007), and Apple introduced the iPhone (also 2007; Markoff 2007). However, then came the Great Financial Crisis (GFC) of 2008–2009. As this crisis passed, Google Chairman Eric Schmidt described the state of affairs as follows (Kirkpatrick 2010):

> There were five exabytes of information created by the entire world between the dawn of civilisation and 2003. Now that same amount is created every two days. . . . But the real issue is user-generated content. People are describing enormous amounts about themselves. . . . We can, using AI techniques, predict where you are going to go. . . . All of a sudden, a lot of assumptions we make about daily life are going away.

Table 4.1 Economic characteristics of the DDE compared to previous eras

	Feudalism	*Industrial capitalism*	*Knowledge-based economy*	*DDE*
Time frame	Pre-1820	1820–1980	1980–2010	2010-present
Essential rent-generating productive asset	Land	Machinery for mass production	Intellectual property	Data
Availability of the productive asset	Fixed, but some ability to expand production by including marginal land/irrigation	Expandable through capital investment	Exclusive (time-limited)	Exclusive (indefinite trade secret) when proprietary; shared under "open data" models
Economic institutional framework	Fiefs and the manorial system	Firms that have achieved minimum efficient scale	Firms with technology capabilities	Firms with technology, data, and data analytics capabilities
International relations	Wars of conquest for control of land and its rents	Market expansion through colonies/gunboat "diplomacy"	Rent capture through trade agreements (TRIPS, FTAs)	Rent capture through data clauses (free flow/data localisation)
Pace of innovation	Sporadic	Continuous (driven by knowledge spillovers)	Accelerated (by industrialisation of research and development)	Sharp further acceleration by industrialisation of innovation by machine learning
Scale economies	Limited	Steep	Very steep	Very, very steep
Scope economies	Limited	Marginal	Marginal	Steep
Network effects	None	Certain sectors (telecoms, transport)	Pervasive, due to standards-essential patents	Very powerful in Internet platform sectors
Information for economic agents	Non-key and symmetric	Symmetric with market solutions for asymmetries	Imperfect, but highly transparent and essentially symmetric	Asymmetric

Source: Developed by the authors.

The post-GFC world is different because of the massive expansion of the role of data in the economy. The year 2010 thus appears to be as good a time as any to mark the transition to the DDE (Srnicek 2017; Zuboff 2015).

Across these historical eras, social structures evolved based on the wealth that accrued to the scarce factor of production in the form of "rents" (i.e., above-normal economic returns), as this shifted from the landed gentry of the manorial era, to the urban industrial tycoons of the capitalist era (the "nouveau riche" of their day), to the CEOs of technology companies, and now to those who control data. The location of power also shifted from the manors of rural Europe, to industrial cities, and then to the innovation hubs. The contest for rents shifted from land, to markets, to IP, and now to data. International conflict followed the lines of these contests, shifting from wars of territorial acquisition, to naval control of shipping lanes and ports to dominate markets, to the modern technology wars fought mainly by lawyers (Ciuriak 2020). The age of data has injected additional stimulus to the latter, turning a simmering low-level conflict over IP between the United States and China into a full-blown cold war and technological decoupling and opening up new fronts between erstwhile allies, as the European Union moves to ensure its technological independence from both the United States and China and to recapture its data rents through digital taxes (Ciuriak and Ptashkina 2018). Finally, across these transitions, as shown in Table 4.1, externalities proliferated, expanding the natural role of the state.

Rents, externalities, and the endogenous rise of the state

The role of the public sector is closely linked to externalities. Externalities are the consequences – positive or negative – that occur as a result of our actions and that we tend not to take into account when undertaking these activities. In the absence of externalities, one might be able to think of an economy of individual economic agents making decisions about production and consumption based entirely on their own preferences, capabilities, and the prevailing prices in the market, without reference to the state. This theoretical construct, however, is a poor guide to reality, because complex economies do not exist in a vacuum: They require systems of governance that create enforceable property rights and provide for the myriad other public goods that underpin organised markets, such as transport and communications, public education, health systems, basic utilities, public and national security, courts to settle disputes, and research and development funding (Sykes 2005).

One of the main economic justifications for government is to avoid the underprovision of goods with positive externalities. Such goods and services have "public good" characteristics – i.e., they can be enjoyed by many people at the same time without being used up and it is difficult to exclude people from enjoying their use.[2] Such goods and services will tend to be underprovided by the market because they attract "free riders" (i.e., those who benefit from the good or service without paying for it); the classic example is national defence.

At the same time, there are also "public bads" – things that have negative externalities such as pollution. These require collective action to counter through

regulation and disciplines in instances where private contracting to offset damages (as per the Coase theorem; Coase 1960) would be impractical due to exorbitant costs of contracting.

Since state functions come with a cost, addressing externalities requires collective funding – in other words, taxes. These can only be sustained if there is surplus generated by the economy above subsistence levels. Here, it is useful to recall that the emergence of the administrative state is tied to the emergence of surplus agricultural production (see, e.g., Frangipane 2018, and sources therein), which created the basis for organised markets; writing, which initially, as far as can be determined from archaeology, was confined to commercial ledgers and tax records; money and finance (including the introduction of interest, which created powerful tendencies for wealth concentration and the need for debt collection and enforcement); and civil engineering to create the original infrastructural public goods (irrigation and flood control[3]). These various types of public goods in turn created free rider problems that necessitated taxes and their collectors, as well as defense against acquisitive rent-seekers. In simple terms, surplus (rents) called the state into existence, and the state justified its existence by providing public goods – which is to say, it captured the positive externalities implicit in providing various non-rivalrous goods and services.

Industrialisation, for its part, required the concentration of workforces in cities, which massively expanded externalities – many of them negative ones. Where people living in agrarian settings interact infrequently with others and thus generate few externalities, whether positive or negative, those living in cramped quarters generate externalities in profuse amounts, including the spread of disease and the inevitable friction of people getting in each other's way. The Industrial Revolution thus created new demands for governance while also creating the rents to pay for it through the economic returns to good governance. Cities prospered if they were able to solve the collective action problems of investing in public goods – roads, hospitals, sanitation, education, courts to adjudicate conflicts, and so on.

If governance involves in part the regulation of negative externalities and investment to capture positive externalities, with the scale determined by the scale of rents generated, we have no difficulty in understanding the steep rise in the role of the state in the industrial era. We also see that the scale of the state is in part determined by the investment opportunities in public goods that contribute to rent generation. This emphasises that the "sweet spot" – where the state is appropriately sized and has appropriate roles – is determined by technology, not ideology.

With the emergence of the KBE, which depends on a capital asset (knowledge) that has classic "public good" characteristics and that depends on protection for its monetisation, the role of the state further expanded. This reflects several things: the rising investment opportunities in public good space (witness the public support for research and development in the era of the KBE); the governance problems implicit in the commitment to policing the protection of IP (specialised IP courts, additional resources for customs to combat counterfeit goods, etc.); and, given the powerful concentrative tendencies of the KBE as evidenced by

the steadily rising share of wealth captured by the top percentiles in this era, new requirements to either defend the wealth of the wealthy (the rise of the militarised police state to protect gated communities) or to redistribute the wealth (the rise of populism).

Against the background of this additional narrative, we can surmise that the trajectory for the optimal role of the state implied by the digital transformation is again upward, given that it does the following:

- Introduces a new form of capital that has "public good" characteristics;
- Creates prospects of large rents, which in principle stimulate public investment;
- Creates opportunities for international rent capture to trigger international rivalry; and
- Raises pervasive negative externalities that require governance reform.

In this context, the state does not wither; it adapts and rises. The early returns on the DDE are fully consistent with this expectation. We are seeing states moving to capture rents associated with data, including by mobilising public-sector data and introducing tax reforms that follow the shift of economic activity into the digital realm. We are seeing strategic trade and investment policies being adopted by the major players with skin in the DDE game, including restrictions on the market access of foreign competitors and public investment in support of national champions and in technologies deemed to be strategic. States are also being galvanised into regulatory actions to address the plethora of *Black Mirror* dystopian developments that the digital transformation has set in motion.[4]

With the expectation that the role of the state will expand in the DDE, building on the expansion of its role in the industrial and KBE eras, we turn to the specific implications of the digital transformation for the role of the state as economic agent, as regulator, and as the agent of power projection internationally to capture global rents.

The roles of the state in the age of data

The state as economic agent – industrial policy in the DDE

In recent decades, the prevailing economic orthodoxy has held that government involvement in the economy should be primarily directed to providing economic infrastructure and economic frameworks that facilitate private sector economic activity. This role assignment was reinforced internationally by the General Agreement on Tariffs and Trade (GATT)/WTO Agreement on Subsidies and Countervailing Measures (ASCM). The implicit assumption underpinning this agreement is that government intervention is a distortion rather than a correction to some underlying market failure, such as the presence of positive or negative externalities. In the advanced economies, industrial policy accordingly was designed to support industrial development in general (so-called horizontal or soft industrial

policies), while not attempting to "pick winners" in specific sectors (so-called vertical or hard industrial policies), not least to avoid being challenged under WTO rules.[5] Where rent capture beckoned, typically in new high-technology areas, such as civil aircraft, nanotechnology, solar, and electric cars, governments did not hesitate to intervene, although their support was designed as much as possible to be "horizontal" in nature, consistent with the understood norm.[6] More recently, concerns about secular stagnation and disappointing developmental outcomes, coupled with the success of China's industrial policies in powering its technological advance, have led to widespread consideration of more activist industrial policies.

The DDE puts new pressure on the shaky consensus around industrial policy, for several reasons. First, it is based on a form of capital with public good characteristics. As Haskel and Westlake (2017) (and others) highlight, economic innovation depends on the combining of intangibles, such as data and IP to create new knowledge, goods, and services; the more freely IP and data can flow, the easier it is to make this happen. In other words, data exhibits the positive externalities of a "public good." However, as Haskel and Westlake (2017, 83) note, "If the spillovers of intangibles encourage companies to keep their investments to themselves, or at best to share in a self-interested way, then the synergies of intangibles have the opposite effect" (see also Ciuriak 2018b, 6–7). In theory, at least, these public-good characteristics of intangibles support some degree of public-sector investment.

Second, it introduces new technologies that have general-purpose characteristics but that are being developed in specific use cases, such as machine learning applications for facial recognition or self-driving cars. In other words, while governments may seek to frame support as "horizontal," it is inevitably sector- or product-specific, which can be a problem (as discussed further).

Third, the transition to new technology creates a classic industrial policy coordination problem – for example, investors in electric vehicles will need complementary investments in charging stations while IoT applications will depend upon a publicly funded roll-out of 5G telecommunications systems. This supporting infrastructure needs to be provided and paid for by somebody.

Fourth, the acceleration in the pace of change has necessarily shortened the time horizons for private investors in recovering investment, which means that private-sector capital will not commit to some investments that have social value (Ciuriak 2018b).

Fifth, the strategic competition between the United States and China has motivated these two giant economies to commit public funds in copious amounts to support the critical technologies of the DDE, which in turn means that other countries face marginalisation in the DDE if they do not jump in as well.

Taken together, all these factors support a larger role for public-sector investment and risk-taking. However, this raises a truly thorny issue from the perspective of the rules-based system, since the ASCM frowns on public-sector industrial support that is "specific" to an industry. Absent a cogent theoretical counterpoint to the ASCM, countries that commit public-sector funds to investments to the DDE are doing so against their own better judgements concerning the role of the public sector and are implicitly risking WTO-authorised retaliation. This suggests that the

policies adopted might be poorly framed and generate unnecessary friction; moreover, this heightens the risk that grounds on which a reconciliation of Chinese and Western industrial policies might be based will go unexplored. While intellectual support for a new industrial policy has been provided by economists such as Rodrik (2010) and Mazzucato, Kattel and Ryan-Collins (2020), a new consensus, embedded in international rules, has yet to emerge to fit our new reality.

The state as regulator

As economic activity and social interaction shift progressively online, there will be a commensurate need to transpose the existing body of government regulation for the digital domain. This process will provide a welcome opportunity for housekeeping and taking advantage of digital technology to reduce the cost to government of delivering government services, as well as the cost to the public of accessing those services. This process is well underway through such initiatives as the Digital 9, a group of leading digital nations that is collaborating on digital-policy issues.[7] At the same time, the new economic and social environment generates significant new demands for governance, which points to an expanded role for the state as regulator.

Part of the immediate regulatory challenge will involve governments expanding their capacity beyond that required by the minimalist-state orthodoxy of the past several decades. Particularly important is the analytical capacity to develop regulatory frameworks, a challenge Chenou remarks upon in his chapter in this volume. Governments will need greater receptive capacity for the analytical work done in academia and think tanks, not to mention the advocacy input from business and non-governmental organisations. The acceleration of the pace of change of social and economic systems will place a premium on understanding and managing transitions and turbulence. Another factor is the pervasiveness of change, which will place a premium on the ability to integrate the implications of changes across multiple dimensions (including across multiple economic sectors, as well as social and political dimensions).

One of the more subtle implications of the DDE is the need to retool how governments measure and manage the economy. In the DDE, an important locus for value capture will be within the household. Numerous tasks that previously required time-consuming activity, such as shopping, are greatly facilitated by access to the internet and e-commerce solutions. Improvements in the efficiency of household production are, however, ignored entirely in estimates of gross national product, which captures only activity undertaken by formal firms. By the same token, household welfare, the standard bottom line for policy impact assessment, acquires new dimensions beyond total consumption, including the greater variety of consumer goods and services accessible through e-commerce but also more leisure. As well, households enter into competition with formal firms through business models in the so-called sharing economy, such as ride-sharing and home-sharing, without facing comparable regulatory requirements. Further, the gig economy is now operating at the international level: Digital technologies allow skilled personnel to remotely

operate machinery ranging from construction cranes to robot-assisted open-heart surgery, within and potentially across borders. These business modalities raise a plethora of regulatory issues.

Another general issue is managing markets in a context that gives rise to superstar firms – a consequence of the winner-take-most nature of platform-based business models and the DDE in general (Srnicek 2017; Ciuriak 2018a).The state will need to raise the level of its game to deal with concentration of private-sector power in the hands of the CEOs of superstar firms. With effectively unlimited financial resources showered on them by financial markets supercharged by negative real policy interest rates and exploiting the technology newly developed by tens of thousands of highly trained PhDs around the world, modern tech CEOs have control over resources that Machiavelli's Prince could only dream of, yet they often face few of the checks and balances that circumscribe political power in modern democracies. This reality is set in sharp relief by the Cambridge Analytica scandal, which involved the use of "Canadian technology on an American platform, paid for by Russian and US money to interfere in a British referendum over its future in the European Union" (Balsillie 2019). At the same time, given the advantage to a state of having national champions, the superstar firm model puts the state into strategic trade and investment competition with other states, in a context in which the tools of geo-economics have been unleashed. This reality of domestic tension between government and superstar firms and international alignment of government with superstar firms is captured well by the populist US President Trump domestically railing at the US technology giants as part of the "radical left," but walking out of international negotiations on the apportionment of profit taxes on multinational enterprises because such taxes would target US technology giants (Zuidijk 2020).

The nexus of issues that falls under the "sovereignty" pillar of social choice appears to pose far more demanding challenges in the networked world. Platform companies, such as Facebook and Google, have not handled well the many issues ranging from privacy to hate speech, a conclusion echoed by Rone in this volume. While these companies are likely part of the solution to addressing such challenges as disinformation faced by an increasingly interconnected world, there is also likely to be a stronger role for independent public-sector agencies because of the plethora of temptations for abuse of dominance in a world of dominant firms – ranging from the use of information for political objectives as noted earlier; impairment of competition (Google was found guilty by Germany's competition authority of using its market dominance to favour its affiliated companies; [European Commission 2018]); ethical failures in exploiting private information (Facebook was censured for ethical breaches by the United Kingdom; UK House of Commons 2019); abuse of the system for tax avoidance, which undermines public administration, which itself will become increasingly problematic in a post-pandemic age of elevated public debts (TRTWorld 2020); and leveraging their size and asymmetric information advantage in negotiations with public authorities (e.g., Simon 2018; Wylie 2018).

The DDE also raises at least two entirely new regulatory challenges. The first is the regulation of AI, and the second is the use of AI in regulation.

As regards the former, Ciuriak and Wylie (2018) sketch out the scope of the challenge. One set of challenges relates to the use of AI. Standard setting, whether by international institutions, the private sector, or expert-led bodies, is needed when AI performs mechanical functions. Where it undertakes human cognitive or decision functions, competence regulation would be appropriate. In terms of effects, AI may have a societal impact, such as with regard to surveillance or through distributional impacts. For the former, we will need to develop a tripartite consensus framework with effective democratic oversight over the executive arm of government. With regard to the latter – i.e., distributional impacts raised by the re-allocation of work between humans and machines – we will need to update or rewrite the economic policy framework. Finally, AI has both security and trade implications. Where AI has military applications, cyber-security in defense of sovereignty will become essential, whereas when it intersects with trade and investment, new approaches to international rules will be required in such areas as competition, strategic trade and investment policy, and the role of foreign direct investment in knowledge-based and data-driven sectors.

As regards the use of AI in regulation, we have already seen China introduce AI courts (Japan Times 2019; Zou 2020), the United States deploy several different "risk assessment" tools to help judges determine whether to incarcerate defendants pending trial (Metz and Satariano 2020), and France ban the use of AI for predictive analysis of case law (Connett 2019). Tennis has adopted "shot spot," which allows players to challenge line calls made by human judges but imposes a penalty if a challenged call proves to have been accurate (Bane 2015). Similar systems are also in use in cricket and football (Ahmadi and Sobhani 2014). And even staid baseball is considering having AI systems make ball and strike calls, in the wake of controversies arising in a context where the viewing audience has access to AI calls that often show that umpire calls were inaccurate (Jones and Levy 2017; Bogage 2019). While some of these uses of AI are obviously trivial, they provide interesting examples of alternative modes where humans override AI in some applications and where AI overrides humans in others. Other AI applications raise important questions about accountability and human rights. Although data is often seen as just the facts, such scholars as Safiya Umoja Noble have highlighted the extent to which algorithms and the data upon which they depend continue to reflect racial, gender, and other biases (Noble 2018). Addressing these biases, again, would seem to require high-level political governance and societal consensus.

To summarise, from a regulatory perspective, the rise of the DDE appears to be a time for the state to staff up and lawyer up, at least for the transitional phase during which the rules of the road of the DDE are being established and becoming ingrained in behaviour.

State rivalry and power projection in the age of data – the return of geo-economics

From a global perspective, the rules-based framework under the GATT/WTO is rightly celebrated for imposing discipline on countries tempted to extract terms of

trade gains by raising tariffs on industrial goods. However, it is important to note where it was less successful, namely in restraining strategic trade investment policies when major rent capture opportunities arose in areas ranging from dynamic random-access memories to civil aircraft. Now, at the dawn of the DDE era, similar rent capture opportunities are emerging with respect to the winner-take-most advantages that go with control of significant amounts of economically valuable data (as well as IP). A full-blown trade and technology war has broken out between China and the United States (see, e.g., Segal 2019); again, the WTO framework has been ineffective in containing it (Rudd, Clark and Bildt 2019), even as many analysts express concern about the WTO's very survival (e.g., Gros 2020).

A number of observations can be made on the basis of the early returns from this new conflict concerning the role of the state.

First, the almost casual abandonment of the rules-based system in favour of geo-economic power plays at a time of pervasive technological change that is generating large new sources of economic rent suggests (or at least gives rise to the suspicion) that the survival of the rules-based system for an extended period of time in the postwar period was somewhat fortuitous – a function of the economic conditions of that era. In retrospect, it was the comparative paucity of rents and competitive conditions of the mature industrial economy that made the system suitable for regulation by markets and rules rather than by strategic policy. This leads to the conclusion that the rules-based system under the WTO was a creature of the technological conditions of its age, rather than an optimal end point towards which economic systems naturally evolve – an "end of economic history" in a sense similar to Francis Fukuyama's "end of history."

Second, the role of China's rise in triggering the present rupture serves to underscore that such institutions as the GATT/WTO are also creatures of the political conditions of their age. The original GATT was a Cold War instrument sponsored by the United States as an alternative to the International Trade Organisation (ITO), the intended third part of the Bretton Woods trio alongside the International Monetary Fund and the World Bank. The difference between the GATT and the ITO was that the former excluded the prime geopolitical adversary of the United States at the time, namely the Soviet Union and its allies. With the transformation of the global economy from the industrial/KBE era for which the GATT/WTO was designed and the rise of a new geopolitical adversary in the form of China, the GATT/WTO structure was not suited to address the issues at play in the DDE (since it did not have a regime in force for data flows) and it provided China with recourse against the United States for unilateral actions. Accordingly, the WTO was quickly sidelined by the United States with the simple stratagem of refusing to allow the replacement of members of the Appellate Body that serves as the means by which WTO rulings are enforced (Johnson 2019). International institutions do not reign in hegemonic powers; they exist and serve at their pleasure.

Third, once the contest is engaged, the dynamics suggest there is no going back.

US measures against China have included, besides tariffs on US imports from China, many technology-related measures. Of the latter, some of the most

prominent are as follows: explicit prohibitions on sale of US technology to China (including by foreign firms that use as much as 25 percent US technology in their products); curtailment of Chinese investment in US technology and data assets and forced unwinding of existing such investments (including the gay dating app Grindr; Hale 2020); a "China Initiative" by the US Department of Justice targeting Chinese nationals for scrutiny for alleged technology theft, including the use of extradition treaties to reach Chinese nationals abroad (Cass and Gardner 2020; Department of Justice 2020); a (failed) attempt to exclude Chinese technology experts from participating on international standards-setting bodies (IEEE 2019; Schwartz 2020); directives to US universities to review their technology partnerships with Chinese entities and indeed to withdraw from them on pain of losing US federal government funding (Armstrong, Waldman and Golden 2020; Somerville and Lee 2019); and of course the full-court press on third countries to exclude the Chinese telecom giant Huawei from participating in their roll-out of 5G networks.

For its part, China pulled out all stops to address its technological deficiencies in areas where a US technology ban represents a constraint, accelerating the decoupling. The speed with which this all unfolded reflects the fact that it was foreseen – and in fact had undoubtedly been war-gamed by both sides (for examples of disclosed war games on US–China technology decoupling, see Bryan-Low et al. 2019; Russo 2020). Thus, Huawei had stockpiled critical components and worked to line up alternative suppliers even before the technology war fully broke out. Accordingly, in one redesign cycle, it was able to produce a new, high-end cell phone without US parts. Following a 15 May 2020 extension by the Trump administration of its restrictions from chips to the tools used to make them to cut off these workarounds, China's President Xi Jinping announced a US$1.4 trillion investment programme over the period to 2025 to promote China's technological independence (The Economist 2020). These moves put enormous pressure on global supply chains, potentially to the point of a full technological decoupling between the two economies.

In a world of geo-economic power plays, as opposed to one of governance by multilateral rules, the state becomes a particularly central player, because it alone has the power to divert resources at the national scale into the contest for rents. Whether the state co-opts private interests or private interests co-opt the state is likely a matter of initial conditions and/or the nature of the interests that are touched by the new rent-generating technology. In the case of the DDE, we see both directional impulses: The powerful lobby effort mounted by the US technology giants co-opted the state to press for favourable international rules, while the national security implications of the new digital technologies led the state to coopt the technology giants to collaborate, even in contexts where this created reputational risk for the companies themselves in their global ambitions (Powers and Jablonski 2015).

One can note that the US technology offensive against China was almost entirely unimpeded by the rules developed for the industrial/KBE era. Nor was it reliant on the tools of earlier mercantilist wars – tariffs and gunboats. These are irrelevant in prosecuting the current war. The grounds for conflict have shifted, so have the tools, and so too must the rules to restrict their use.

There is thus a critical need for a rethinking of current institutional frameworks to address the role of data and the nature of the economy to which big data and the technologies that exploit it give rise. The earlier considerations point to the need for a plethora of international rules to smooth out the many points of friction that are likely to emerge as nations individually and at times collectively implement provisional solutions to address negative externalities of data and to secure a foothold in the DDE. Accompanying these international rules should be a vision for a WTO 2.0 that might differ fundamentally from version 1.0. In order to address the issues laid out in this chapter, a potential negotiating agenda for an updated WTO should include a new regime to govern the flow of data across borders, while allowing for a fair sharing of the economic returns generated by data captured within a nation's borders. A key issue here is taxation on income generated by data captured within a jurisdiction. This data regime, furthermore, requires exceptions to accommodate regulations governing use of data to protect sovereignty, particularly as regards maintaining election integrity and constraining surveillance through effective rules on privacy. Other important concerns are competition policy and IP. The DDE sets up a "winner-takes-most" economic environment that raises issues of market access, while IP rules must be updated to address the expansive interpretations of trade secrets, among other issues.[8]

Conclusion: the state and global governance in the age of data

The foregoing discussion considers the implications of the digital transformation for the role of state. The analytical strategy is to focus on the role of data as a capital asset, to compare the characteristics of data as the essential capital asset of its age to its predecessors in previous ages – land, mass production machinery, and IP – and to draw inferences for social and economic ordering from the transition. This narrative provides a basis for considering how the age of data might shape up. In short, the chapter contends that the DDE generates novel and complex demands for governance and public-sector economic engagement, which imply a significantly expanded role for the state.

Scanning economic history through this lens leads to some provocative insights: It suggests that the nature of the essential productive asset of an age shapes economies and societies; that the contest over the rents that accrue to the essential asset orders international relationships; and that the nature of the essential and scarce asset dictates the battleground issues and the choice of weapons. As a corollary, the international institutions called into being to optimise outcomes in any given setting are creatures of their age and the technological conditions that shape it. Political and economic contexts, in other words, matter, a finding echoed by Chenou in his chapter.

There is an appealing simplicity to this construction, as it suggests that the economic and social order is determined by conservation of a relatively scarce and valuable factor of production. This in turn implies that optimisation processes drive the outcome, which in turn predicts that societies that manage the use and regulation of data effectively – that is, find the "sweet spot" between capturing

positive externalities and constraining negative ones – will fare better than those that do not. This immediately points to a promising line of research, focused on one of the questions at the heart of this volume, namely, how should the state's role in economic governance be expanded to best promote the positive externalities and limit the negative externalities created in a DDE?

As the earlier discussion suggests, the digital transformation is generating a wealth of economic framework issues that need to be addressed at both the domestic and international levels. How markets evolve will determine the extent of pressure on regulation, but the economic framework policies developed for the industrial/KBE era do appear to need more than tweaking to support a largely open and highly integrated global digital trading system and a more or less free flow of data. As well, a new détente is required among the major digital economy powers; as argued in Ciuriak (2020), this would be best reached earlier rather than later, based on the expectation that the "race" to dominate the DDE is in fact likely to be over before it is really engaged because of the acceleration of the pace of innovation with the shift of this activity into machine-learning space. The age of data may thus be short-lived. But it promises to be intense and the state is at the heart of it.

Notes

1 While it may seem contradictory to state that data is both being generated in astronomical amounts and remains "scarce," that is the reality in two senses. First, in a distributional sense, shortage of data as a factor of production is often severe in the DDE for both firms and for developing countries, given private control of data by platform firms (Williams 2019). Second, for many use cases that involve complex models, the data required to train algorithms using machine learning within stipulated mathematical criteria can be infinite, meaning there is an insatiable appetite for more data to achieve commercially deployable AI.
2 To put it in economics terms, they are non-rivalrous and non-excludable.
3 Flood control seems to have been a particularly important factor in motivating collective action, given that floods bring both fertile soils as well as devastation. Thus, we see the rise of early civilisations in flood plains, including the Nile, the Tigris-Euphrates, the Ganges, and the Yellow and Yangtze Rivers. The devastating floods of the latter gave rise to the ultimate bureaucracy, the Mandarin administrative state, which tamed the rivers with monumental (for the age) civil engineering endeavours in the form of canals that linked the two river systems.
4 See, for example, the ever-increasing number of platform-regulation proposals and regulations tracked by Winseck and Puppis (n.d.).
5 Harrison and Rodriguez-Clare (2010) and Devarajan and Uy (2009) discuss the horizontal/vertical distinctions, referring to horizontal policies as "soft" industrial policies and vertical policies as "hard" industrial policies.
6 These norms did not, of course, prevent governments from bailing out financial firms deemed "too big to fail" or from saving troubled industrial giants. In these regards, the accepted industrial policy was honoured as much in the breach as in the practice.
7 As of June 2020, the Digital Nations group comprised Canada, Denmark, Estonia, Israel, Mexico, New Zealand, Portugal, the Republic of Korea, the United Kingdom, and Uruguay.
8 These issues are taken up in greater detail in Ciuriak (2019).

References

Ahmadi, Zahra, and Niloufar Sobhani. 2014. "Arbitration Management with Using Artificial Intelligence Technology (the sample: Goal-line Technology in Football)." *Russian Federation Modeling of Artificial Intelligence* 2 (2): 48–58.

Armstrong, David, Annie Waldman, and Daniel Golden. 2020. "The Trump Administration Drove Him Back to China, Where He Invented a Fast Coronavirus Test." *ProPublica* 18 March. www.propublica.org/article/the-trump-administration-drove-him-back-to-china-where-he-invented-a-fast-coronavirus-test. Accessed 4 August 2020.

Balsillie, Jim. 2019. *Six Recommendations for the International Grand Committee on disinformation and 'Fake News'*. Waterloo: Centre for International Governance Innovation. 7 November. https://www.cigionline.org/articles/six-recommendations-international-grand-committee-disinformation-and-fake-news.

Bane, Michael. 2015. "Beyond the Line Call: How Hawk-Eye Can Improve Performance." *The Conversation*. 21 January. https://theconversation.com/beyond-the-line-call-how-hawk-eye-can-improve-performance-35962. Accessed 4 August 2020.

Bogage, Jacob. 2019. "Baseball's Robot Umpires Are Here. And You Might Not Even Notice the Difference." *Washington Post*. 10 July. www.washingtonpost.com/sports/2019/07/10/baseballs-robot-umpires-are-here-you-might-not-even-notice-difference/. Accessed 4 August 2020.

Bryan-Low, Cassell, Colin Packham, David Lague, Steve Stecklow, and Jack Stubbs. 2019. "Hobbling Huawei: Inside the U.S. War on China's Tech Giant." *Reuters*. 21 May. www.reuters.com/investigates/special-report/huawei-usa-campaign/. Accessed 4 August 2020.

Cass, Luke, and Stephen Gardner. 2020. "The China Initiative: Combating Economic Espionage and Trade Secret Exfiltration." *IP Watchdog*. 9 February. www.ipwatchdog.com/2020/02/09/china-initiative-combating-economic-espionage-trade-secret-exfiltration/id=118646/. Accessed 4 August 2020.

Choo, Eugene. 2005. "Going Dutch: The Google IPO." *Berkeley Technology Law Journal* 20 (1): 405–441.

Ciuriak Dan. 2018a. "The Economics of Data: Implications for the Data-Driven Economy." In *Data Governance in the Digital Age*. Waterloo: Centre for International Governance Innovation. 5 March. www.cigionline.org/articles/economics-data-implications-data-driven-economy. Accessed 4 August 2020.

Ciuriak, Dan. 2018b. "Rethinking Industrial Policy for the Data-Driven Economy." *CIGI Paper* 192. Waterloo: Centre for International Governance Innovation. www.cigionline.org/sites/default/files/documents/Paper%20no.192web.pdf. Accessed 4 August 2020.

Ciuriak, Dan. 2019. "World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age." *CIGI Policy Brief 152*. Waterloo: Centre for International Governance Innovation. www.cigionline.org/publications/world-trade-organization-20-reforming-multilateral-trade-rules-digital-age. Accessed 4 August 2020.

Ciuriak, Dan. 2020. "Economic Rents and the Contours of Conflict in the Data-Driven Economy." *CIGI Policy Brief*. Waterloo: Centre for International Governance Innovation. www.cigionline.org/publications/economic-rents-and-contours-conflict-data-driven-economy.

Ciuriak, Dan, and Maria Ptashkina. 2018. "Started the Digital Trade Wars Have: Delineating the Regulatory Battlegrounds." *Opinion*. RTA Exchange. International Centre for Trade and Sustainable Development. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3098982. Accessed 4 August 2020.

Ciuriak Dan, and Bianca Wylie. 2018. "Data and Digital Rights: More Questions Than Answers – But Enumerating the Questions is Essential." *Ciuriak Consulting Commentary*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300263. Accessed 4 August 2020.

Coase, Ronald H. 1960. "The Problem of Social Cost." *Journal of Law and Economics* 3(1): 1–44. https://doi-org/10.1057/9780230523210_6.

Connett, Ian. 2019. "France Resists Judicial AI Revolution." *Above the Law* (blog). Legal Innovation Center. 10 June. https://abovethelaw.com/legal-innovation-center/2019/06/10/france-resists-judicial-ai-revolution/. Accessed 4 August 2020.

Corrado, Carol, Jonathan Haskel, Cecilia Jona-Lasinio, and Massimiliano Iommi. 2012. *Intangible Capital and Growth in Advanced Economies: Measurement Methods and Comparative Results*. New York: The Conference Board. June. www.conference-board.org/publications/publicationdetail.cfm?publicationid=2377. Accessed 4 August 2020.

Department of Justice. 2020. "Information about the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018." *Fact Sheet*. Washington: Department of Justice.

Devarajan, Shanta, and Marilou Uy. 2009. *Is it Worthwhile to Support Industrial Policy?* Paper presented at the DIE Workshop on Industrial Policy in Developing Countries. Bonn. 18–19 November.

Dontha, Ramesh. 2017. "The Origins of Big Data." *Blogpost*, KDNuggets. https://www.kdnuggets.com/2017/02/origins-big-data.html. Accessed 4 August 2020.

The Economist. 2020. "America's Latest Salvo against Huawei is Aimed at Chipmaking in China." *The Economist*. 23 May. www.economist.com/business/2020/05/23/americas-latest-salvo-against-huawei-is-aimed-at-chipmaking-in-china. Accessed 4 August 2020.

European Commission. 2018. "Antitrust: Commission Fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine." *Press Release*. 20 July. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581. Accessed 4 August 2020.

Facebook. 2007. *Facebook Unveils Facebook Ads*. Press Release. 6 November. https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/. Accessed 4 August 2020.

Frangipane, Marcella. 2018. "From a Subsistence Economy to the Production of Wealth in Ancient Formative Societies: A Political Economy Perspective." *Economia Politica* 35: 677–689. https://doi-org/10.1007/s40888-018-0133-3.

Gros, Daniel. 2020. *Will the WTO survive 2020?* Center for Economic and Policy Studies. 7 January. www.ceps.eu/will-the-wto-survive-2020/. Accessed 4 August 2020.

Hale, Kori. 2020. "Grindr's Chinese Owner Sells Gay Dating App Over U.S. Privacy Concerns For $600 Million." *Forbes*. 26 March. www.forbes.com/sites/korihale/2020/03/26/grindrs-chinese-owner-sells-gay-dating-app-over-us-privacy-concerns-for-600-million/#211922d3551c. Accessed 4 August 2020.

Harrison, Ann E., and Andres Rodriguez-Clare. 2010. "Trade, Foreign Investment, and Industrial Policy." In *Handbook of Development Economics*, Vol. 5, edited by Dani Rodrik and M. Rosenzweig. Amsterdam: North Holland.

Haskel, Jonathan, and Stan Westlake. 2017. *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton, NJ: Princeton University Press.

IEEE. 2019. "Compliance with U.S. Trade Restrictions Should Have Minimal Impact on IEEE Members Around the World." *Press Release*. 29 May www.ieee.org/about/news/2019/compliance-with-us-trade-restrictions.html. Accessed 4 August 2020.

Japan Times. 2019. "In Brave New World of China's Digital Courts, Judges Are AI and Verdicts Come Via Chat App." *Japan Times*. 7 December. www.japantimes.co.jp/news/2019/

12/07/asia-pacific/crime-legal-asia-pacific/ai-judges-verdicts-via-chat-app-brave-new-world-chinas-digital-courts/. Accessed 4 August 2020.

Johnson, Keith. 2019. "How Trump May Finally Kill the WTO." *Foreign Policy*. 9 December. https://foreignpolicy.com/2019/12/09/trump-may-kill-wto-finally-appellate-body-world-trade-organization/. Accessed 4 August 2020.

Jones, Meg Leta, and Karen Levy. 2017. "Sporting Chances: Robot Referees and the Automation of Enforcement." *Working Paper*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3293076.

Kirkpatrick, Marshall. 2010. "Google CEO Schmidt: 'People Aren't Ready for the Technology Revolution'." *ReadWrite.com (blog0)*. 4 August. https://readwrite.com/2010/08/04/google_ceo_schmidt_people_arent_ready_for_the_tech/. Accessed 4 August 2020.

Lo, Chris. 2015. "Tracks in Time: 200 Years of Locomotive Technology." *Railway Technology*. 19 May 2015. https://www.railway-technology.com/features/featuretracks-in-time-200-years-of-locomotive-technology-4517022/. Accessed 4 August 2020.

Markoff, John. 2007. "Apple Introduces Innovative Cellphone." *New York Times*. 10 January. https://www.nytimes.com/2007/01/10/technology/10apple.html. Accessed 4 August 2020.

Mazzucato, Mariana, Rainer Kattel, and Josh Ryan-Collins. 2020. "Challenge-Driven Innovation Policy: Towards a New Policy Toolkit." *Journal of Industry, Competition and Trade* 20 (2): 421–437.

Metz, Cade, and Adam Satariano. 2020. "An Algorithm That Grants Freedom, or Takes It Away." *New York Times*. 6 February. www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html. Accessed 4 August 2020.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: University of Illinois Press.

Ricci, Tom. 2012, 14 May. *Robert Fulton: Biography*. American Society of Mechanical Engineers. https://www.asme.org/topics-resources/content/robert-fulton. Accessed 4 August 2020.

Rodrik, Dani. 2010. "The Return of Industrial Policy." *Project Syndicate*. 12 April. www.project-syndicate.org/commentary/the-return-of-industrial-policy?barrier=accesspaylog. Accessed 4 August 2020.

Rudd, Kevin, Helen Clark, and Carl Bildt. 2019. "Former World Leaders: The Trade War Threatens the World's Economy." *The New York Times*. 11 October. www.nytimes.com/2019/10/11/opinion/china-trade.html. Accessed 4 August 2020.

Russo, Federica. 2020. "War Game Analyzes Future US-China Relationship." *Asia Times*. 18 June. https://asiatimes.com/2020/06/war-game-analyzes-future-us-china-relationship/. Accessed 4 August 2020.

Schwartz, Ari. 2020. "Standards Bodies Are Under Friendly Fire in the War on Huawei." *Lawfare (blog)*. 5 May. www.lawfareblog.com/standards-bodies-are-under-friendly-fire-war-huawei. Accessed 4 August 2020.

Segal, Adam. 2019. "Year in Review 2019: The U.S.-China Tech Cold War Deepens and Expands." *Council on Foreign Relations*. 18 December. www.cfr.org/blog/year-review-2019-us-china-tech-cold-war-deepens-and-expands. Accessed 4 August 2020.

Simon, Scott. 2018. "Amazon Deal in New York Creates Some Unlikely Allies." *National Public Radio*. 17 November. www.npr.org/2018/11/17/668766759/opinion-amazon-deal-in-new-york-creates-some-unlikely-allies. Accessed 4 August 2020.

Somerville, Heather, and Jane Lanhee Lee. 2019. "U.S. Universities Unplug from China's Huawei under Pressure from Trump." *Reuters*. 24 January. www.reuters.com/article/us-usa-china-security-universities-insig/u-s-universities-unplug-from-chinas-huawei-under-pressure-from-trump-idUSKCN1PI0GV. Accessed 4 August 2020.

Srnicek, Nick. 2017. *Platform Capitalism*. Cambridge: Polity Press.

Sykes, Alan O. 2005. "The Economics of WTO Rules on Subsidies and Countervailing Measures." In *The World Trade Organization: Legal, Economic and Political Analysis*, Vol. 2, edited by Patrick F.J. McCrory, Arthur E. Appleton, and Michael G. Plummer. New York: Springer.

Toynbee, Arnold. 1884. "Lectures on the Industrial Revolution." In *England: Public Addresses, Notes and Other Fragments, together with a Short Memoir*, edited by Benjamin Jowett. London: Rivington's.

TRTWorld. 2020. "Will the Pandemic Herald the End of Big Tech's Tax-Free Ride?" *TRT-World*. 22 May. www.trtworld.com/magazine/will-the-pandemic-herald-the-end-of-big-tech-s-tax-free-ride-36541. Accessed 4 August 2020.

UK House of Commons. 2019. "Disinformation and 'fake news': Final Report." *Digital, Culture, Media and Sport Committee, Eighth Report of Session 2017–19*. London: UK House of Commons https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm. Accessed 4 August 2020.

Williams, Sarah. 2019. "Data Scarcity in the Era of Big Data: Learning to Use Data from Private Organizations." *Working Paper, MIT*. http://civicdatadesignlab.mit.edu/files/WilliamsDataScarcity.pdf. Accessed 4 August 2020.

Williamson, Jeffrey G. 1984. "Why Was British Growth So Slow during the Industrial Revolution?" *Journal of Economic History* 44 (3): 687–712.

Winseck, Dwayne, and Manuel Puppis. n.d. *Platform Regulation Inquiries, Reviews and Proceedings Worldwide*. https://docs.google.com/document/d/1AZdh9sECGfTQEROQjo5fYeiY_gezdf_11B8mQFsuMfs/edit#heading=h.drjg9uyede6x. Accessed 4 August 2020.

Wylie, Bianca. 2018. "Sidewalk Toronto: Gaslighting Toronto Residents Backfired – Capacity's Built and Power's Shifted." *Medium*. 16 October.

Zou, Mimi. 2020. "'Smart Courts' in China and the Future of Personal Injury Litigation." *Journal of Personal Injury Law* (forthcoming).

Zuboff, Soshanna. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30: 75 – 89. https://doi.org/10.1057/jit.2015.5.

Zuidijk, Daniel. 2020. "Trump Says Tech Giants Controlled by 'Radical Left,' Vows Action." *Bloomberg*. 16 May. www.bloomberg.com/news/articles/2020-05-16/trump-says-tech-giants-controlled-by-radical-left-vows-action. Accessed 4 August 2020.

Part 2

Internet governance and authoritarian states


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

5 Building China's tech superpower

State, domestic champions and foreign capital

Lianrui Jia

This chapter focuses on and contests the "Chinese model" of internet governance, such as that set forth in the 2018 speech of French President Emmanuel Macron to the Internet Governance Forum, which sees the state completely controlling and driving innovation. As the Chinese internet governance literature notes, there is a well-established consensus that the state plays a dominant role in regulating and monitoring content (MacKinnon 2012; Ruan et al. 2016), in establishing a holistic cyber-sovereignty framework (Zeng, Stevens and Chen 2017; Arsène 2016) and in planning national technology development (Chen 2019). However, research has also shown that various non-state actors have entered the game, not least private Chinese companies like Alibaba, Tencent, and Baidu, as well as technical communities. These non-state actors all play important roles in driving national policies (Vila Seoane 2019; Keane and Wu 2018; Leong 2018), setting technical standards and shaping China's internet governance agenda (Shen 2016; Negro 2019). Given this reality, the more important question is not whether the state is back in the context of Chinese internet governance, but in what capacities is the state back? And how has its role changed over time?

This chapter takes a broad view of internet governance, peeking into blind spots that are often not labelled as "internet governance." As van Eeten and Mueller (2012) argue, a focus on the explicitly institutionalised rules and procedures in clearly defined formal institutional venues such as the Internet Corporation for Assigned Names and Numbers (ICANN), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF) only offer a partial picture of the rules and norms that shape internet governance. Beyond these headline global organisations, the tools and machinery of internet governance are dispersed in areas of telecommunications policies regarding mobile telecoms, trade, market regulation and cyberlaw (van Eeten and Mueller 2012). Focusing only on these formal organisations can lead one to miss other significant political and, importantly, economic arenas in which governance – the setting of formal and informal rules that affect the functioning and use of the internet – occur.

This chapter thus conceptualises internet governance as "governance that shapes the use and evolution of the internet" (van Eeten and Mueller 2012, 731). This chapter recognises that the internet in China has both *political* and *economic* dimensions that the Chinese state needs to attend to over the course of

DOI: 10.4324/9781003008309-8

its development: first, to manage the flow of information facilitated by the internet to maintain social stability and the Party's rule and, second, the internet is the pivot through which digital capitalism negotiates its entry and interacts with the institutional context of China. This is evident in the volatile flows of transnational capital in and out of the Chinese internet industry, especially as the domestic companies grow and expand. Therefore, internet governance in China, as broadly conceived, must address both the political and economic aspects. Positioned in a critical political economy theoretical framework, this chapter contextualises China's cyber development as the outgrowth of techno-nationalism, embraced in its national information and communications technology development, and asks, how does the state adjust its role with respect to the rise of the internet in China?

Looking at the policies, official statistics and procedural aspects of how the Chinese state channels and acts as a gatekeeper of foreign capital and mobilises leading domestic corporations to build a strong nationalistic and commercially viable internet, this chapter contributes to an understanding of the reciprocal relationship between structures of power in security, finance and knowledge in the political economy of Chinese internet development (Haggart 2019; Bannerman and Orasch 2019). In particular, it highlights the role of US structural power over global finance and production in shaping current Chinese models of internet development and for the type of internet that the next billion internet users will come to know.

This chapter first overviews the key claims of techno-nationalism and traces its manifestation in Chinese information and communications technology development. It then dissects the roles of foreign capital and domestic corporations in state policy initiatives designed to build "China into a cyber superpower." This chapter concludes by noting the historical continuities and adaptations in the development of the internet in China and its implications in ongoing geopolitics.

China's long-standing techno-nationalism

In April 2018, Chinese President Xi Jinping announced China's Cyber Superpower (网络强国) strategy. This represented an expansion on its previous strategy, announced in 2012, to become a Cyber Power (网络大国). Both strategies regarded the internet as the underlying infrastructure to be harnessed to further strengthen national power and social governance and as a sector that would allow for profit accumulation and economic growth. In turn, these strategies could be seen as an outgrowth of a 2004 goal, set by the Ministry of Information Industry (MII) minister, Wang Xudong, for China to become a Strong Telecommunications Nation (电信大国). This strategy was designed to expand the scale of China's information and communications technology industry (ICT) and to build this core competency into a globally competitive industry.

The struggle for national sovereignty in telecommunications development is a continuous element throughout modern Chinese history (He 1997). The three aforementioned strategy announcements are part of this long-standing tradition, representing national aspirations formalised at the policy level to achieve

superpower status in communications that carry with them a strong and central role for the state, a role that remains central to Chinese policy in the internet age. Efforts to achieve greater control of networked communications infrastructure are driven by the core imperative of ensuring Chinese *national, as opposed to foreign*, control over information network infrastructure and development (Zhao 2010).

The Chinese path of ICT development can be seen as a form of techno-nationalism, that is, the pursuit of technological prowess by nations in the context of international competition (Qiu 2010). Techno-nationalism offers a framework for understanding developing countries attempting to catch up with more technologically advanced states, such as Japan's *gijutsu rikkoku* (nation-building via technology) industrial policy of the post–World War II period (Nakayama 2012), particularly regarding ICT policies, technical standards and the trade dimensions of technology. In China, successive generations of leadership have subscribed to a policy and ideology of techno-nationalism, treating high technology as a source of national power and a central means of defining China's position in the world (Feigenbaum 1999, 2017). Techno-nationalism, as it relates to national security, carries with it an emphasis on the importance of technological autonomy, as well as being a means to support and reinforce the country's overall technological capabilities (Shim and Shin 2016).

As an overarching policy position, techno-nationalism encompasses many policy tools and has come to shape Chinese industrial development in general. Chinese techno-nationalist policy places a razor-sharp focus on enterprise groups, deploying comprehensive, long-term industrial strategies to build internationally competitive domestic firms and to replace foreign technology and products with those designed and made by Chinese companies, first for its home market and then the overseas market (Koleski and Salidjanova 2018). China's policy tools to these ends include state funding, subsidies, tax breaks, government procurement, technological standards, foreign investment restrictions and import guidance, acquisition of foreign technology and foreign talent, and industrial espionage (Koleski and Salidjanova 2018; Naughton 2004). Chinese techno-nationalism treats national interests as paramount, even in situations where techno-nationalist policies may carry short-term costs (Breznitz and Murphree 2013). For example, driven by the need to foster technological capabilities, national security and national pride, China proposed the 3G TD-SCDMA[1] standard, which later was accepted by the International Telecommunications Union in 2000. However, the actual implementation process was lengthy and costly, sparking domestic resistance (Thun and Sturgeon 2019; Hong 2010 cited in Zhao 2010). While China promoted this standard in order to prevent royalties and licensing fees from being paid to foreign manufacturers, its adoption did not much benefit domestic Chinese mobile handset manufacturers, as the production processes still relied heavily on imported components (Thun and Sturgeon 2019).

As this example suggests, technological development is a highly contested global-power battleground (Han 2009), with standards setting being a particularly important issue area. The battle over 5G mobile standards, for example, in which the Chinese company Huawei has figured prominently, has played a key role in

rising economic tensions between China and the United States in the 2010s and early 2020s. The Chinese government's sustained commitment to techno-nationalism, of which the battle over standards is but one part, is often seen as a growing challenge for the United States and the European Union, as well as for foreign firms seeking to enter China's market or compete with its state-supported firms abroad (US-China Economic and Security Review Comission 2016; White House Office of Trade and Manufacturing Policy 2018; Wübbeke et al. 2016).

While techno-nationalism may be the overarching ideology of Chinese leadership, it would be a mistake to cast the Chinese state's role in monolithic terms. China's techno-nationalist policies increasingly engage a host of non-state actors. Qiu (2010) has noted a decisive drift away from the statist mode of command-and-control centred structurally and discursively on a tiny segment of China's ruling elite and towards participation of multinational corporations and domestic commercial media. The rise of an internet-based subculture group known as the "industry party" also indicates the rising public interests in China's techno-nationalist development. This is a group of netizens involved in technology and the sciences who are concerned with the state of the country's industrial and technological developments and have become increasingly vocal in online discussions (Zhao and Wu 2020). In short, the pursuit of national objectives in tech development increasingly needs to accommodate heterogeneous sets of interests from states, market players and the general public (Naughton and Segal 2002).

Beyond the domestic, scholars have refined the concept of techno-nationalism to account for the inherent complexity of China's pursuit of national objectives within an industry ecosystem that is integrated on a global scale. For example, examining China's handset industry, Shim and Shin (2016, 208) argue that China is demonstrating a form of neo-techno-nationalism, where industry development must take into account international norms and cooperation with foreign partners and recognise the need for new forms of public-private accommodation. In this view, as China integrates evermore deeply into the global marketplace, techno-nationalist policies (neo- or otherwise) need to strike a balance between leveraging the opportunities presented by globalisation for national economic and security advantages and mitigating their risks, such as increased dependence (Suttmeier and Yao 2004; Suttmeier 2005), while also noting that the boundaries between economic concerns and national security considerations are increasingly blurred, and economic concerns often can be more important that national security issues, strictly defined (Ahmed and Weber 2018).

China's cyber ambition

For the techno-nationalist Chinese government, the internet plays a key role in several important political and economic policy issues (see Luo and Lv, this volume). From the government's perspective, the internet should be developed so as to safeguard the Party's rule as well as to modernise production processes, stimulate domestic consumption, and – eventually – to help China to reclaim its rightful, dominant position in the world (Shi 2018). Scholars have noted that

internet-related policymaking in China became increasingly neoliberal and technocratic, encouraging individual success stories of entrepreneurs and technocrats salvaging the national economy in the aftermath of the 2008 Global Financial Crisis (Jiang and Fu 2018; Wu and Yun 2018). In 2015, China's annual economic growth rate fell below seven percent for the first time in decades, sparking domestic consternation and social unrest, leading authorities to double down on this narrative. As a result of ongoing (as of July 2020) sluggish economic growth (at least by recent historical standards), the new political and economic realities have made ICT and the internet even more increasingly central to China's overarching project of economic growth, national rejuvenation and integration into transnational capitalism (Schiller 2005).

The 2012 installation of Xi Jinping as President and Li Keqiang as Premier marked a sea change in China's approach to internet development. First introduced in the State Council's 2010 White Paper, the concept of cyberspace sovereignty rises to the fore as the key guiding principle in domestic internet governance, where the Chinese state plays an active role in shaping, guiding, supervising and managing online activities. In 2014, to centralise regulatory authority over the internet and settle various agency turf battles regarding internet regulation,[2] Xi created (and personally chairs) the Central Leading Group for Cybersecurity and Information (CLGCI) (Miao and Lei 2016). Xi followed this move with the introduction of the aforementioned Cyber Power (网络大国) strategy in 2014 at the first meeting of the CLGCI. The Cyber Power strategy signalled a new stage of China's aspirations to become a formidable power in the cyber domain.

The Cyber Power strategy encompasses multiple policy focuses. First, it seeks to address the reality that while China has the world's largest share of people who are online, the country still lags in innovation and depends on the United States in core technologies, such as integrated circuit chips (Zhao and Cao 2014). To facilitate domestic high-tech manufacturers' innovation capacities, China launched the *Made in China 2025* (MIC25) strategy in 2015. The MIC25 was regarded as a threat and received pushback from the United States (Martina, Yao and Chen 2018). Although the Chinese government no longer refers to the MIC25 name at key political venues such as National People's Congress, it constantly updates the strategy and pilot projects are well underway (Zenglein and Holzmann 2019). In addition, the Internet Plus plan, formalised in 2015, positions the internet as a means to address a host of social, political and economic objectives, including using the internet to allocate resources in traditional industries and gauging public opinion to better manage social control (Creemers 2017; Hong 2017a).

Second, the Cyber Power policy further reinforced the idea that as a necessary precondition for its economic development, the *government* will continue to play a central role in safeguarding the security and operation of nation's cyberspace (Zhao and Cao 2014). The Cyber Power strategy is designed to tighten the state's control over online activities. Through the making of laws and regulations, guidance and management of online public opinion, cyberspace is further harnessed as space for propaganda work (Xinhua 2014). As President Xi remarked during the National Propaganda and Ideology Work Conference in 2013: "the internet . . .

directly relates to the national ideology security and the regime security" (People's Daily 2013).

The Cyber Superpower strategy follows the policy contours of the previous call to build China into a cyber power, with key policy focuses on innovation, cybersecurity and the added emphasis on ideological, infrastructural, economic and diplomatic dimensions (People's Daily 2017). The strategy's central idea is to enforce the cybersecurity and informatisation[3] of the Chinese society. It is worth noting that the concept of cybersecurity is an expansive one, in that it includes not only the security of information infrastructure, operators and enterprises, but also the security of the Party's leadership position and ideology (Creemers, Triolo and Webster 2018). By folding ideology into the dimension of national cybersecurity, the Party has consolidated its control over online activities by moving the Central Leading Group for Cybersecurity and Information within the Central Commission for Cybersecurity and Informatisation, which is under the direct supervision of the Party's Central Committee.

Through its Cyber Superpower strategy, China seeks to become the agenda- and standards-setter of global internet governance in order to counter US dominance and hegemony over the internet. For example, China not only launched the annual World Internet Conference in 2014 but has also promoted its vision of cyberspace sovereignty at venues such as the WSIS and the United Nations. In international relations and diplomacy, the Chinese internet industry is featured prominently and occupies a central position in the Belt and Road Initiative (BRI), launched in 2013 to mitigate industrial overcapacity, to facilitate Chinese firms' globalisation and to construct a China-centred transnational internet infrastructure (Liu and Dunford 2016, Shen 2018). Even with an explicit nationalistic overtone, the Chinese government acknowledges that the Cyber Superpower-building process cannot be a closed-door development: It will depend on transnational linkages and global flows of information, human capital and financial capital (信息流、技术流、资金流) (Creemers, Triolo and Webster 2018, Inkster 2016).

Following China's long-standing techno-nationalist tradition, the Cyber Superpower strategy aims to build and project China's national power through the development of the internet both at home and in the global arena. It reckons that the realisation of national aspirations of becoming a cyber power requires the participation of heterogeneous sets of actors, such as the state, private actors and capital. To better grasp the emerging dynamics among these actors, the following section first reviews the role of ICT enterprises and financing model in the state-led telecommunications industry development to contextualise and compare China's cyber power building process.

Techno-nationalism in the digital age

As key indicators of and the embodiment of national techno-power and as a matter of national security, the telecommunications sector in China underwent a prolonged reform beginning in the 1980s. The government broke the Ministry of Post and Telecommunication's monopoly on telecommunications service in 1994 and introduced

market competition through the creation of three state-owned enterprises, China Unicom and Jitong in 1994 and China Netcom in 2000. The sector was restructured, liberalised and marketised on the eve of China's accession to the World Trade Organisation. In a matter of decades, China broke away from dependency on foreign technologies, especially on telephone switch development in the 1980s and 1990s, and became one of the world's largest markets and exporters for telecommunications products. However, the country still faces the challenges of climbing up the value chain, from being a manufacture centre to a technology super-state.

Similar development patterns prevailed in China's internet-related development: After becoming the 77th country to join the global internet in 1994, the Chinese internet took off at a rapid rate. Reaping the economies-of-scale benefits of being a large economy, China surpassed the United States as the world's largest internet population in 2008 and the Chinese internet industry evolved from being primarily a market for emerging Western internet companies in the early 2000s to being the birthplace of several of the world's largest internet companies.

Drawing on such historical parallels, this section analyses how the Chinese state mobilises two key actors to hasten national technology development: domestic enterprises and foreign capital. Focusing on the national champion policy and the China-China-Foreign financing model in telecommunications development, this section shows that there are both continuities and changes when comes to managing internet in China to achieve Cyber Superpower status.

Making national champions for telecommunications development

The national champions policy, formally pursued since 1991 and officially endorsed in 1997 at the 15th Party Conference, seeks to use China's large economies of scale to develop and promote a handful of large-scale, globally competitive Chinese enterprises. As then-President Jiang Zemin remarked in 1992: "We should encourage Chinese enterprises to expand their investments abroad and their transnational operations" (Jiang, cited in Zhang 2003, 69). The national champion policy not only deployed concerted state resources and planning (such as soft-loan financing from state banks) but also strategically leveraged foreign capital (through stock market listing) to cultivate large-scale enterprises (mostly state-owned) in a so-called lifeline industry[4] to secure its home-market advantages as the country reintegrates into global capitalism and opens up itself to foreign capital. At the time, national champions were primarily state-owned enterprises, which further highlights state involvement in the implementation of industrial policy (Eaton 2015; Nolan 2014; Sutherland 2003; Szamosszegi and Kyle 2011). These champions were fostered primarily through government-ordered mergers and takeovers of loss-making enterprises. Through these means, the Chinese state exerted its power over the market to turn domestic enterprises into national champions: "the fullest expression of state capitalism in China – the global face of China Inc." (Lin and Milhaupt 2013).

The ICT sector was a primary focal point of the national champions policy. As part of the initial group of national champions in 1991, and later in 1997,[5]

the State Council handpicked several technology enterprises to receive support and preferential policies: the Great Wall Group, a leading personal computer producer, Changjiang Computer Group, Legend (now Lenovo) and Founder Group[6] (Sutherland 2003; Ning 2009). Three of the nation's telecommunications operators, China Mobile, China Telecom and China Unicom, are also the crown jewels of this national team, ranking among the world's largest telecommunications corporations after raising considerable capital through their listing on foreign stock exchanges. At the time, the number of Chinese telecommunications companies listed in the Fortune 500 was taken to be a key indicator of the country's technopower. By 1999, of the six Chinese enterprises listed in the Global Fortune 500 list, none were ICT-related (Fortune n.d.a). By 2019, China had 129 Fortune 500 companies, surpassing the United States (121 companies) for the first time (Murray and Dunn 2019), among which Huawei ranked 61st, Alibaba 182nd, Lenovo 212nd, Tencent 237th, and Datang 438th (Fortune n.d.b).

Beyond designating and supporting national champions, the Chinese government has poured significant financial support into fostering domestic companies' research and innovation. Huawei, ZTE, Datang and Great Dragon, four domestic telecom manufacturers, have all benefitted from government support in financial subsidies and assistance with their self-developed technologies in large-scale switch equipment (Fan and Gao 2016). The Chinese government also acts in a matchmaker role in linking the domestic market to domestic producers (Fan and Gao 2016). With loans provided by state banks totalling to nearly RMB 40 billion (Thun and Sturgeon 2019), Datang pioneered the successful technological development and implementation of the homegrown 3G TD-SCDMA[7] standard with close cooperation from Siemens in 1999 (Fan 2010).

The national champion policy approach of the state picking winners and fostering innovation started to encounter difficulties in the 2000s, partly due to the stagnation of the economy in Japan and South Korea's *chaebol* crisis, which showed the limitations and weaknesses of such an approach, and partly due to the attractive market-led innovation model in the West (Naughton 2004). In response, the Twelfth Five-Year Plan (2011–2015) improvised the policy of fostering national champions to spearhead the development of the nation's backbone industries such as biotechnology, new energy and next-generation IT (Szamosszegi and Kyle 2011), only this time "national champions" was more expansive in its scope, taking the focus away from state ownership so that any targeted company, as long as it is Chinese, is worthy of state support and nurturance.

Internet companies: adapting the national champion model

Compared to the telecommunications industry, which is led by state-owned and -fostered large-scale enterprises, the Chinese internet grew from a much more market-oriented origin (see discussions in Jiang 2012; Creemers 2018). The Chinese internet industry is spearheaded and represented by few giant home-born companies such as Baidu, Alibaba and Tencent (collectively known as BAT). These privately held companies (that is, held by company founding figures and

other institutional shareholders) are often referred to as "national champions" (Jiang and Fu 2018; Keane and Wu 2018; Leong 2018; Plantin and de Seta 2019), including by these companies' CEOs themselves. Such is a telling indicator of the changing faces and the overall framing of the "Team China." The adaptation of the national champions model, which aimed to foster state-owned enterprises, showcases that the Chinese state is more open in welcoming various market participants, regardless of ownership types, into its techno-power construction, as Naughton and Segal (2002) put it: "what matters now for a national champion is not that it is state, collective, or privately owned, but that it is Chinese" (163).

The Chinese state is thus gradually embracing multiple actors and forces in realising its techno-nationalist objectives. Internet enterprises' CEOs' use of the rhetoric of "national champion" is not only a showcase of the corporate identity but also demonstrates their goodwill in cooperating with the state and in siding with national policy initiatives. For example, when faced with the question of whether Alibaba is owned by the Japanese – Softbank, a Japanese holding group, held 25.9 percent of Alibaba's shares in 2019 and was its largest shareholder in 2019 – former Alibaba CEO Ma (Jack) Yun openly proclaimed that Alibaba is a "national enterprise" (国家企业) and that it should represent "Chinese culture, the Chinese value system, Chinese technologies and Chinese productive forces" (CNR 2014). The success of the China-based digital platform WeChat, an all-in-one mobile app integrating mobile chat, digital payment and other services, offers another example of how the commercial interests of platform companies simultaneously help realise the state's mandate to build national digital infrastructure and protect the domestic market from foreign competitors (Plantin and de Seta 2019).

In the meantime, non-state-owned enterprises are increasingly participating in national projects and diplomatic missions. Alibaba's former CEO, Jack Ma, was the only Asian co-chair elected to the NetMundial Initiative in 2015. In 2017, a number of Chinese companies, led by Alibaba, Tencent and Baidu, injected private capital of US$11.7 billion into the country's telecommunications operator China Unicom to revitalise the state-owned company (Weinland 2017). In 2019, Alibaba also invested in the state-owned mobile communication infrastructure company China Tower Corp (China Daily 2018). This shows the rising financial and political might of these internet companies, as they are allowed to partake in ownership reform of state-owned enterprises. China's cyber diplomacy, which is centred on the concept of cyber sovereignty, also increasingly engages commercial actors (Segal 2017) in aligning the geopolitical ambitions between the quickly globalising Chinese internet companies and the Chinese state.[8] This co-dependence between state and domestic internet giants is demonstrated in the appearance of Chinese internet entrepreneurs, products and services in state-level visits, such as Baidu's launch of its Brazilian search service Busca in Xi's visit to Brazil in 2014.

Chinese internet companies are appointed important roles in the digitisation of social services provision and social governance by providing crucial data and digital infrastructure. Alibaba and Tencent are assisting local police in the state-led smart cities projects by providing surveillance networks and cloud-based data systems to use facial-recognition programs to identify and arrest criminals and to track and

forecast movements of crowds (Lin and Chin 2017). Several city governments, together with Alibaba, implemented the City Brain in Shanghai, Guangzhou and Hangzhou, an AI-driven system designed to provide solutions to traffic congestion, detect accidents and improve traffic efficiency (Alibaba Clouder 2019). In 2017, for China's Next Generation Artificial Intelligence Development Plan, the government handpicked four domestic tech companies to co-develop artificial intelligence open-innovation platforms: Baidu for self-driving cars; Alibaba for the smart city; Tencent for medical imaging; and iFlyTek for voice recognition (People's Daily 2019). The four-company national AI team was later expanded to 15, to further advance development of AI in finance, education, health care and smart homes (People's Daily 2019). Furthermore, the construction of the Social Credit System (SCS), a national project that sets a comprehensive outline for the establishment of data infrastructure for credit and social scoring, has deepened the symbiosis between the state and leading Chinese platform companies (Liang et al. 2018; Jia 2020). The SCS project is the formation of "corporate-state nexus" that not only uses data gathered from commercial platforms and social behaviours to feed the national surveillance infrastructure but also involves the government sharing data with commercial sectors for purpose of credit rating (Liang et al. 2018).

The recognition of domestic private internet companies as national champions demonstrates that techno-nationalism is no longer an exclusively state-led process. The state encourages a handful of domestic internet companies to become globally influential companies to fortify China's cyber power on the global stage. Meanwhile, instead of direct state intervention in resource allocation and management, the Chinese government grooms market actors into cyber power–building teams by integrating domestic tech enterprises into various government initiatives and tech development plans. However, as private internet companies grow, the need for capital access is limited by restrictions on foreign ownership. The Chinese state has taken a pragmatic approach and exercises administrative and strategic flexibility to allow private internet companies to access foreign capital market.

Financing the superpower: from the China Unicom model to the Sina model

China-China-Foreign investment in basic telecommunications services

The lack of financial capital and state investment has been a pervasive problem for China's telecommunications industry, particularly in the early 2000s (Keck 2000; DeWoskin 2001; Lu 2000; Fan 2010; Hong 2017b). China Unicom offers a typical example of how a state-owned telecommunications enterprise devised creative structures and arrangements to raise capital. To introduce competition into the telecommunications service market, China Unicom, a venture co-owned by Ministry of Energy, Ministry of Railroads and Ministry of Electronics Industries, received an operating licence in 1994 as an alternate carrier for voice over both mobile and wireline networks. However, the company was starved of capital

because other than its existing private network infrastructure, which belonged to its parent ministries (of railroads and energy), the government did not provide it with any capital (DeWoskin 2001). Furthermore, unlike the telecommunications equipment manufacturing sector, the telecommunications service sector[9] was prohibited from receiving foreign direct investment (Guan 2003).

Unable to access sufficient capital to compete with the incumbent monopoly, China Telecom, beginning in 1995 China Unicom entered into over 40 government-approved joint ventures with foreign telecommunications enterprises such as Sprint, Deutsche Telekom, France Telecom, Bell Canada, NTT International, Itochu, Korea Telecom and Singapore Telecom (DeWoskin 2001; Wang 1999; Keck 2000). This arrangement, named the China-China-Foreign (CCF) model, was designed to work around formal limitations in the Chinese law. The model works as follows: A subsidiary of China Unicom formed a joint venture with a foreign company, and then the joint venture entered into contract terms (usually 15 years) with China Unicom (Harwit 1998). China Unicom operated the joint-venture entities under the required license, while foreign investors provided the capital investment. Revenue was shared between China Unicom and foreign investors (see Figure 5.1). By the end of 1997, China Unicom had raised US $1.4 billion through this model, representing a full 72 percent of its total funding.

As successful as this policy was for China Unicom, the government was concerned about losing control over these entities to foreign companies. The CCF arrangements were terminated in 1998, with China Unicom paying back all its capital investment and interest depending on the profitability of the specific joint venture (Guan 2003). In response, in 2000, the State Council promulgated the Regulation Concerning Telecommunications of the People's Republic of China that formally limited foreign ownership stakes to 49 percent in basic telecommunications services, such as businesses providing public network infrastructure, public data transmission and basic voice communications services, and placed a 50 percent cap in value-added telecommunications services, such as email, databases and

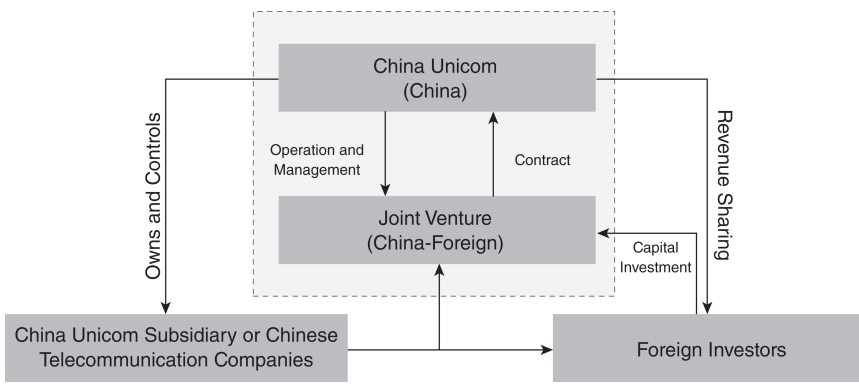


Figure 5.1 The China-China-foreign financing model

Table 5.1 Public listing of state-owned media and telecom enterprises in China

Company	*Listed on*	*Year*	*IPO raised*	*Underwriters*
China Mobile	HKSE	1997	4.2 billion	China International Capital; Goldman Sachs
China Unicom	HKSE	2000	4.92 billion	Morgan Stanley
China Telecom	HKSE	2002	1.4 billion	Morgan Stanley, Merrill Lynch, China International Capital

reselling of telecommunications service, such as internet connection services to third parties.

With the state's ban on CCF arrangements and limitations on foreign investment in the telecommunications sector prior to the country's accession to World Trade Organisation, public listing through stock exchanges becomes the preferred and the more economical way of raising capital. Three state-owned telecommunications companies are listed on the Hong Kong Stock Exchange, with foreign and Chinese investment banks as their underwriters (Table 5.1).

The variable interests entity structure and finance of internet companies in China

Despite their current successes, many Chinese internet companies initially ran into similar problems with raising capital. Accessing global capital markets is made more difficult by China's regulations on value-added telecommunications services (VATS) preventing foreign entities from owning more than a 50 percent equity stake in these companies. This limitation explains why large Chinese internet companies are all registered in offshore jurisdictions through the deployment of a corporate structure known as variable interests entity (VIE) to structure their offshore shell companies and domestic operation arms. First pioneered in 2000 by Sina, one of the most established internet companies in China offering internet content services, in its initial public offering (IPO) (Jiang 2012), the VIE structure has been widely adopted by foreign listed Chinese internet companies.

A VIE structure is usually composed of a wholly foreign-owned enterprise (WFOE), a domestic Chinese holding company that is owned by a shell company registered in an offshore jurisdiction. The WFOE controls operating companies in China through a series of contractual agreements detailing the level of control held by each party and profit distribution (see Figure 5.2). The VIE structure thus kills several birds with one stone: It circumvents the maximum 50 percent foreign ownership restriction on VATS companies, it provides companies with relatively unfettered access to capital markets, and it allows for the distribution of profits and benefits to foreign investors, while leaving effective control firmly in hands of the Chinese company.

VIEs are not without their downsides. Their complex and opaque nature presents regulatory and legal challenges for foreign investors: Shares owned by foreign

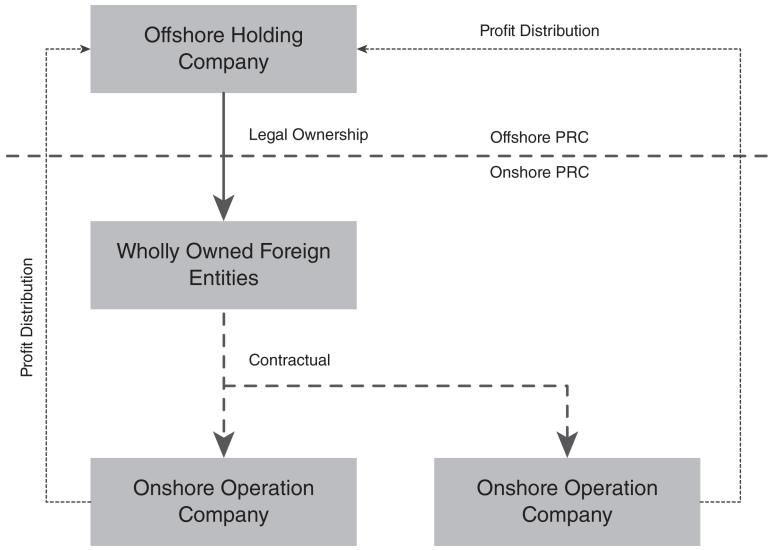


Figure 5.2 An example of a VIE structure

investors are not directly in the operating entities in China but in the WFOE; therefore, the VIEs give investors contractual claims to a company's profits but do not legally grant them ownership of the company (Casey 2014). This case raised serious concerns about the protection of foreign investors' equity right under the VIE arrangement (Shen 2012). In 2014, just before Alibaba's IPO, the US-China Economic and Security Review Commission released a report warning about the risk of the VIE structure, where the contracts linking the WFOE with onshore operating entities are only under protection of the Chinese law (Rosier 2014).

Within China, the legality of VIE structures is an ongoing debate between state and corporate actors. Having benefited from the VIE structure, Baidu's CEO, Yanhong Li, proposed to cancel state-imposed restrictions on the VIE structure during Lianghui[10] (Sina 2013). Different ministries and regulatory agencies, meanwhile, harbour diverging opinions on the legality of the VIE structure. For example, in 2009, the General Administration of Press and Publication clearly prohibited the VIE structure in the online gaming sector (Guo 2014). Similarly, the Ministry of Commerce and the China Securities Regulatory Commission have also discouraged VIEs, especially in the internet sector. However, the Chinese government's attitude towards tighter regulation of VIEs has been purposefully ambiguous. Without inter-bureaucratic consensus, the Chinese government has not launched any significant efforts to systematically regulate the VIE structure.

The regulation (or lack of formal regulation) of VIE structures in China defies the Western perception of a unified, all-controlling Chinese state. The wide deployment of the VIE structure by large publicly traded internet companies

in China demonstrates the contradiction-ridden cyber power–building process: Companies take advantage of legal loopholes in restrictions on foreign ownership to maximise their worldwide hunt for capital, and the state leaves private companies a significant (grey) area in which to maneuver, thereby safeguarding corporate interests. As Yu Hong (2017a, 1500) puts it: "[A]lthough creating friction, state actions collude with corporate interest on making the Internet an omnipresent vehicle of accumulation and enlisting private and transnational capital as stakeholders." The purposefully ambiguous stance taken by the Chinese state shows that techno-nationalism needs to accommodate US structural power in finance to ensure the capital supply needed by private internet companies. This goes to show that securing economic growth is a paramount concern and an objective in internet governance processes. For this reason, as Naughton and Segal (2002) argue, techno-nationalism is justified in China by ensuring the growth of a strong national economy that the Chinese government continues to claim its role as the defender of national interest and pride.

Taking back control

Private Chinese internet companies are deeply interlocked with global networks of finance through fund-raising, share issuance and the underwriting processes (Jia 2018). As geopolitical contestation is increasing between China and the United States, growing pressure is being imposed upon foreign-listed and -financed Chinese internet companies, thereby threatening the economic dimensions of cyber power. China is exploring domestic alternatives to circumvent and reduce reliance on US structural power in the techno-power–building process.

Chinese internet firms have received preferential treatment with respect to access to capital in other ways as well. Since 2000, domestic Chinese internet firms have had to gain approval from the MII before they are allowed to receive foreign capital, cooperate with foreign businesses or list domestic or overseas stocks (CNN Money 2000). While this ruling gives the MII an effective veto over foreign investments, such rules have been applied lightly, resulting an official tolerance for the listing of China-based internet stocks in overseas jurisdictions (Hughes 2004).

As the supply of capital is crucial for the survival and prosperity of internet companies, especially those that are operating according to a platform logic sustained by deep-pocket capital investment to win out as market monopoly.[11] In 2016, the Committee on Foreign Investment in the United States (CIFUS) launched investigations into Chinese tech investment in the United States, forcing Beijing Kunlun Tech to sell back the 60 percent share it bought in US gay dating app Grindr, and also blocked the sale of the money transfer service MoneyGram to Alibaba's Ant Financial for national security reasons (The New York Times 2018). CIFUS also questioned the impact of TikTok, the popular Chinese social media app, on US national security as well as its acquisition of the app Muscial.ly (Roumeliotis et al. 2019; Gewirtz 2019).

The Cyberspace Administration of China, together with the China Securities Regulatory Commission, launched the reform of capital market in 2017 and 2018.[12]

This reform aims at promoting the role of the domestic capital market to encourage the growth of start-up companies and to reap greater economic benefits and "increase party-state influence over domestic tech companies" (Laskai et al. 2018). The capital market reform entails stock market reform to loosen the requirements for tech companies to go public. The China Securities Regulatory Commission (CSRC), People's Bank of China and Shanghai City Government proposed changes to the Technology Innovation Board on the Shanghai Stock Exchange. The goal is to create a looser regulatory environment than many other counterparts, such as Hong Kong Stock Exchange, for the regulators to relinquish responsibilities in assessing the applicants' earnings potential and let the market decide the worth (He and Wei 2019). By lessening the entry requirements on stock markets, the Chinese government aims to bring back foreign-listed internet companies to leverage the capitalisation and privatisation of Chinese internet companies.

In 2019, Alibaba was successfully listed on the Hong Kong Stock Exchange, raising US$11.2 billion from this second listing outside the NASDAQ. This stock listing was a highly politicised event and was portrayed in a nationalistic light. The Hong Kong IPO was dubbed the "homecoming" listing (Xinhua 2019) where Alibaba's Chief Executive Daniel Zhang said, "we return to Hong Kong, return to home" (Woo 2019). Alibaba's Hong Kong listing further signals to other foreign-listed Chinese internet companies the possibility and feasibility of returning from foreign exchanges to domestic ones. More importantly, coming home to the Shanghai or Hong Kong Stock Exchanges helps Chinese internet companies reduce reliance on foreign stock markets and therefore counterbalances the financial power of the US in China's cyber superpower–building process. This anchors China's pragmatic use of securities and capital markets to manage financialisation to achieve specific policy goals (Petry 2019), in this case, to advance the goal of fostering the nation's cyber power.

The geopolitical contestation between United States and China are also expressed in the financial markets: In May 2020, the Senate unanimously passed the Holding Foreign Companies Accountable Act, which requires Chinese companies listed on US exchanges[13] to disclose their state ownership and to comply with audits from the Public Company Accounting Oversight Board (Fanck 2020). Several internet companies, including Baidu and NetEase have considered de-listing from NASDAQ. The reliance on foreign capital markets and financial services, especially on US stock exchanges, is a continuous challenge in China's quest to be a techno-power because such dependency not only introduces instability to foreign-listed Chinese internet companies but also dilutes the Chinese state's ability to oversee their operations. However, to what degree China's ongoing capital market reforms will salvage and provide viable alternatives remains to be seen, as US-China geopolitical contestation is borne out in the realm of finance (Wang 2019).

A strong home market and a sovereign internet

The Chinese state has remained open and flexible in allowing domestic internet companies to access foreign investment through the VIE arrangement, thereby

exhibiting a techno-globalist orientation. However, the emphasis on public opinion work and ideological security, which is mandated as part of Cyber Superpower strategy represents an opposite force of control and tightening of regulation to serve the Party's political interests, a dynamic also explored in Luo and Lv's chapter in this volume. As a result, China's internet governance is characterised by a dual-track approach: strategic flexibility to facilitate economic growth and tight political control.

The concept of cyber sovereignty was first proposed in the State Council's 2010 White Paper "Internet in China" and reaffirmed in the 2013 White Paper on Diplomacy and the Cybersecurity Law and in various multilateral cooperations (Budnitsky and Jia 2018, Arsène 2016). It stipulates that "within Chinese territory, the internet is under the jurisdiction of Chinese sovereignty" and that therefore any foreign internet companies must abide by Chinese laws (People's Daily Online 2010). The Chinese tenet of cyber governance, "cyberspace is not beyond the law" (互联网不是法外之地), reflects the gist of the cyber sovereignty claim. However, as Hong and Goodnight (2020) point out, the Chinese state is not the only governing subject in the cyberspace, and its actions are subject to disagreement and contestation. When it comes to managing and censoring online content, the state delegates this responsibility to private internet companies, which incur large labour and financial costs.

The inclusion of ideology as a key dimension of cybersecurity legitimises the tightening of control in China's Cyber Superpower project. President Xi Jinping stated in the guiding opinions of national cybersecurity:

> We must strengthen online positive propaganda, unequivocally adhere to the correct political direction, and the guidance of public opinion . . . we must strengthen self-discipline in the internet sector, muster the vigor of all netizens, and mobilise forces on all sides to participate in governance.
>
> (Creemers, Triolo and Webster 2018)

In fact, through the promulgation of new regulations and laws, there is an expansion of state-imposed regulations covering different kinds of online and mobile content, and internet companies are under pressure to closely monitor and report suspicious user activities. These efforts are to safeguard one of China's cybersecurity priorities: political security – the protection of one-party state from cyber-based political subversion or other cyber threats originated within and outside China (Austin 2018).

News has historically been the most strictly controlled media content areas in China. Revised for the first time in 2017, China further regulated online news after the Cyberspace Administration of China fined several news portals for sharing independent news stories. The provision of online news is only allowed when websites, apps, public accounts on WeChat, or microblogs have obtained online news licenses, and the change of senior editors must be approved by the authorities. Similar licensing rules apply to the dissemination and distribution of audiovisual content online, the fast-growing, live-streaming industry in China, and domestic

providers of financial information as financial data, news, analysis and trading strategies are subject to the rules that govern mainland-based foreign bureaus.[14] The websites hosting this content are subject to various forms of punishment if they fail to comply, ranging from fines and the withdrawal of licenses to temporary shutdowns. The government has frequently used "campaign-style" regulation[15] to fine, summon, and punish domestic companies (Xu, Tang and Guttman 2019). In 2018, for example, the government cracked down on celebrity gossip blogs and entertainment-related social media accounts (Shepherd, 2017). In the post-2012 period, the state has also regularly clamped down on online content and regulated the circulation of rumours, and online satiric content, and has ordered web companies to suspend comment functions in order to clean up content. In 2017, the government tightened the regulations on virtual private networks (VPNs),[16] outlawing non-government-approved VPNs.

Along with the broadening of the scope of content regulation, the Chinese government also changed how it intervenes and enforces regulation: Control is normalised and routinised, seeping more subtly into the operational structure of the company. Internet companies, both domestic and foreign, are required to establish Party units into their managerial organisation (Martina 2017).[17] According to the State Council Information Office, the purpose of these units is to let party organisations advise company managers on government policies and to help businesses cultivate talent and resolve friction with workers without interfering with the management of foreign companies and joint ventures (Wong and Dou 2017). However, many worry about the Party's increasing influence on business operations and decisions. The Provision on the Interview of Entities Providing Internet News Information Services, formulated in 2015, further provides the regulatory basis for the State Internet Information Office or local Internet Information Office to summon, warn, rectify and correct the wrongdoing of internet news information services. This piece of regulation provides a warning system to avoid the social unrest caused by government shutdowns of popular internet websites or services. For example, Neihan Duanzi, an app owned by ByteDance was shut down for hosting vulgar jokes and videos and failure to respect "core socialist values," and the shutdown caused social unrest for the online subculture communities and led to car drivers honking rhythmically at crowded street intersections (Zhong, Mozur and Zhao 2018).

The Provisions on Internet Security Supervision and Inspection by Public Security Organs put forth by the Ministry of Public Security in 2018 allows central and local public security authorities to enter the premises of all companies providing internet services and to inspect, look up and copy information considered relevant to cybersecurity. The formulation of the Provisions on the Governance of the Online Information Content Ecosystem in 2020 represents an apex in the government's efforts to guide online content production as the regulation explicitly warns against the production and circulation of "negative" content. The negative content is not necessarily illegal content but very vaguely defined to include "sensational headlines, excessive celebrity gossip and sexual innuendo." It further mobilises a range of actors to partake in governing the information content

ecosystem, from government, enterprises, and society to internet users (Bandurski 2020). Private internet companies are important actors to operationalise the censorship and control mechanisms that help maintain the Party's ideological security. Through promulgation of rules and regulations, the Chinese government is enhancing control over online information flows. This shows the highly dynamic and constantly evolving characteristics of Chinese internet governance, as content regulation is responsive to emerging forms of technology and means of distributions.

Conclusion

By analysing the dynamics between the Chinese state and its active shaping of market mechanisms and the deployment of foreign capital into the telecommunications infrastructure in the 1990s, this chapter demonstrates that there are both similarities and changes in how the internet is governed in China. Covering both strategic deployment of foreign capital and state support for domestic enterprises, China's techno-nationalism in the age of the internet nonetheless shows the participation of a wider set of actors. China relaxes control in foreign investment by allowing the VIE structure to secure the economic growth of the internet industry, while it tightens political control through the promulgation of rules and policies to sustain the security of the Party.

The Chinese state is far from being uniform as depicted in the "Chinese model" of internet governance. While China may be pursuing a form of techno-nationalism that enhances and tightens the Party's control, it faces various constraints in its ability to do so – constraints tied primarily to the need for foreign capital to finance its internet industry. Chinese internet governance is much more dynamic and adaptive through both the *active* shaping of policies, regulations and reforms as well as *inactive* actions such as the state leniency towards companies' continued exploitation of legal loopholes and regulatory grey areas in company financing and securitisation, which by definition dilutes state control. As demonstrated by the CCF and the VIE models, when needed, the Chinese government pragmatically allows for the leveraging of foreign capital to foster domestic telecommunications and internet sector growth, while also attempting to maintain tight political control over these sectors, either by regulating the internet content or by scaling back foreign investment in the telecommunications.

Still, the government remains crucial in China's ICT and internet development. However, its role is neither static nor all-controlling. It has taken a very pragmatic approach to leveraging foreign capital to foster the growth of domestic market giants and ensuring post-WTO marketisation and liberalisation of telecommunications industry, while securing and advancing state control through the promulgation of regulations under the banner of cybersecurity. The techno-nationalist strategy of building a cyber superpower provides a powerful policy tool and a discursive framework to justify the dual-track approach and legitimise the state's claim to be a rightful guardian of economic prosperity and the Party's rule – as "national interests."

The ultimate success of China's Cyber Superpower strategy is linked to the very real challenge resulting from China's technological and financial dependence on the United States. Overlooking the transnational linkages or overemphasising the state's totalising role in regulating the internet in China will miss the intricate wrestling of power as China projects its tech power on a global stage. With the ongoing US–China trade disputes that put a spotlight on the high technology and ICT sectors, there remains the question of whether a national and protected internet will generate commercial success and competitiveness globally. The geopolitical confrontations and contestations will only continue to push China to reform its domestic capital market to reduce the fast-growing internet sector's reliance on the financial power of the United States.

Notes

1 The Time Division Synchronous Code Division Multiple Access standard was proposed by the China Wireless Telecommunication Standard Group to the International Telecommunications Union in 1998 as a candidate for a 3G standard. It was approved in May 2000.
2 Often known as the problem of nine dragons run the water (九龙治水), which describes the fragmented internet governance framework developed in China. See the discussion in the chapter by Luo and Lv.
3 Informatisation (信息化) aims to harness ICT in the arena for policymaking and nation-building and is the foundational strategy for China's economic modernisation from a planned economy to a market economy.
4 These include energy supply, electronics, iron and steel, autos, machinery, pharmaceuticals, construction, aviation and aerospace, and chemicals (Sutherland 2003).
5 The initiatives were outlined in two key policy documents: State Council Directive Policy Document Number 71, December 1991: *Request for permission to choose a batch of large enterprise groups to undergo trials*; Policy Document Number 15, April 1997: *Opinions on Deepening the Trial Work on Large Enterprise Groups*.
6 The reason these enterprises are called groups (集团) is that they are neither privately owned nor state-owned. They all have linkages to academic and research institutions. Founder Group is a company spun off from Beijing University and Legend was established by a group of researchers from the Chinese Academy of Sciences.
7 The TD-SCDMA standard is one of the international standards of 3G mobile communications. It was developed by Datang with Chinese government supports in pushing market adaptation. Despite problems, TD-SCDMA is regarded as a successful example of international standard setting.
8 For a more detailed discussion, see Budnitsky and Jia (2018).
9 These two regulations were Interim Arrangements for the Approval and Regulation of the Deregulated Telecommunications Services (1993) and Interim Rules on the Regulation of the Market of Deregulated Telecommunications Services (1995).
10 Lianghui refers to the annual plenary session of the People's Congress and the Chinese People's Political Consultative Conference.
11 See for example: Srnicek (2016); Foster and McChesney (2011); Khan (2017); and for Chinese internet industry Jia and Winseck (2018); Xia (2018); Xia and Fuchs (2016).
12 The key document is *Guiding Opinions on Promoting Capital Markets to Serve the Strategy of Building a Cyber Superpower*.
13 There are, as of 2019, 156 Chinese companies listed on the US exchanges, including both state-owned enterprises and privately owned business. See the full list: www.uscc.gov/sites/default/files/Chinese%20Companies%20on%20U.S.%20Stock%20Exchanges.pdf

14 For a complete list of laws, regulations, legal interpretations and guiding documents, see www.cac.gov.cn/zcfg/A0909index_1.htm
15 The campaign-style regulation speaks to a regulation approach that is focused on the short-term impacts and enforced in a top-down measure.
16 One of the most common VPN uses is to circumvent the Great Firewall, as China blocks Google, Facebook, Twitter, YouTube and many other websites.
17 Many foreign enterprises in China have established Party units, not limited to internet businesses, such as Disney, L'Oréal, Samsung and Nokia (Martina 2017).

References

Ahmed, Shazeda, and Steven Weber. 2018. "China's Long Game in Techno-nationalism." *First Monday* 22 (5).

Alibaba Clouder. 2019. *City Brain Now in 23 Cities in Asia*. 28 October. www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479. Accessed 5 August 2020.

Arsène, Séverine. 2016. "Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order?" *China Perspectives* 2: 25–35. https://doi.org/10.4000/chinaperspectives.6973.

Austin, Greg. 2018. *Cybersecurity in China: the Next Wave*. Cham: Springer.

Bandurski, David. 2020. *Mass Line Internet Control*. Janurary 6. https://chinamediaproject.org/2020/01/06/mass-line-content-control/. Accessed 5 August 2020.

Bannerman, Sara, and Angela Orasch. 2019. "A Strange Approach to Information, Network, Sharing, and Platform Societies." In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 53–89. Cham: Palgrave Macmillan.

Breznitz, Dan, and Michael Murphree. 2013. *The Rise of China in Technology Standards: New Norms in Old Institutions*. Research Report, The U.S.-China Economic and Security Review Commission.

Budnitsky, Stanislav, and Lianrui Jia. 2018. "Branding Internet Sovereignty: Digital Media and the Chinese-Russian Cyberalliance." *European Journal of Cultural Studies* 21 (5): 594–613. https://doi.org/10.1177/1367549417751151.

Casey, Robert. 2014. *Casey to SEC: Protect U.S. Investors in Chinese IPOs; Transactions Could Leave U.S. Investors with Few Safeguards If They Invest in Shell Corporations*. 11 July. www.casey.senate.gov/newsroom/releases/casey-to-sec-protect-us-investors-in-chinese-ipos-transactions-could-leave-us-investors-with-few-safeguards-if-they-invest-in-shell-corporations. Accessed 5 December 2017.

Chen, Wenhong. 2019. "Now I Know My ABCs: U.S.-China Policy on AI, Big Data, and Cloud Computing." *Asia Pacific Issues* 140. www.eastwestcenter.org/publications/now-i-know-my-abcs-us-china-policy-ai-big-data-and-cloud-computing. Accessed 5 August 2020.

China Daily. 2018. "CTC and Alibaba Team Up for Cloud Services." *China Daily*. 1 August. https://europe.chinadaily.com.cn/a/201808/01/WS5b60faa1a31031a351e91540.html. Accessed 5 August 2020.

CNN Money. 2000. "Chinese Web IPOs on Hold." *CNN Money*. 11 May. https://money.cnn.com/2000/05/11/deals/ipo/. Accessed 5 August 2020.

CNR. 2014. "Ma Yun de Xin Jihua: Alibaba Yaozuo Zhongguo de Guojia Qiye." *CNR*. 31 December. http://china.cnr.cn/xwwgf/20141231/t20141231_517280085.shtml. Accessed 5 August 2020.

Creemers, Rogier. 2017. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century." *Journal of Contemporary China* 26 (103): 85–100. https://doi.org/10.1080/10670564.2016.1206281.

Creemers, Rogier. 2018. "Disrupting the Chinese State: New Actors and New Factors." *Asiascape: Digital Asia* 5 (3): 169–197. https://doi.org/10.1163/22142312-12340094.

Creemers, Rogier, Paul Triolo, and Graham Webster. 2018. *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference*. 30 April. www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. Accessed 5 August 2020.

DeWoskin, Kenneth. 2001. "The WTO and the Telecommunications Sector in China." *The China Quarterly* 167: 630–654.

Eaton, Sarah. 2015. *The Advance of the State in Contemporary China*. Cambridge: Cambridge University Press.

Fan, Peilei. 2010. "Catching-up Through Staged Development and Innovation: The Case of Chinese Telecom Companies." *Journal of Science and Technology Policy in China* 1 (1): 64–91. https://doi.org/10.1108/17585521011032559.

Fan, Peilei, and Xudong Gao. 2016. "Catching Up and Developing Innovation Capabilities in China's Telecommunication Equipment Industry." In *China as an Innovation Nation*, edited by Yu Zhou, William Lazonick, and Yifei Sun, 215–239. Oxford: Oxford University Press.

Fanck, Thomas. 2020. *Bill to Delist Chinese Stocks Moving at 'Warp Speed' as a Crackdown Gains Bipartisan Support*. 21 May. www.cnbc.com/2020/05/21/bill-that-could-delist-chinese-stocks-in-the-us-moving-at-warp-speed.html. Accessed 5 August 2020.

Feigenbaum, Evan. 1999. "Who's Behind China's High-Technology 'Revolution'?: How Bomb Makers Remade Beijing's Priorities, Policies, and Institutions." *International Security* 24 (1): 95–126.

Feigenbaum, Evan. 2017. *The Deep Roots and Long Branches of Chinese Technonationalism*. August12.https://macropolo.org/deep-roots-long-branches-chinese-technonationalism/.

Fortune. n.d.a. *Global 500 1999*. https://fortune.com/global500/1999/. Accessed 4 June 2020.

Fortune. n.d.b. *Global 500*. https://fortune.com/global500/. Accessed 4 June 2020.

Foster, John, and Robert McChesney. 2011. "The Internet's Unholy Marriage to Capitalism." *Monthly Review* 1–30.

Gewirtz, Julian. 2019. *Look Out: Some Chinese Thinkers Are Girding for a 'Financial War'*. 17 December. www.politico.com/news/magazine/2019/12/17/look-out-some-chinese-thinkers-are-girding-for-a-financial-war-086610. Accessed 5 August 2020.

Guan, Yunxiang Scott. 2003. *China's Telecommunications Reforms: From Monopoly Towards Competition*. New York: Nova Science Publishers.

Guo, Li. 2014. "Chinese-Style VIEs: Continuing to Sneak Under Smog?" *Cornell International Law Journal* 47 (3): 569–606.

Haggart, Blayne. 2019. "Taking Knowledge Seriously: Towards an International Political Economy Theory of Knowledge Governance." In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 25–51. Cham: Palgrave Macmillan.

Han, Sukhee. 2009. "China's Pursuit of Peaceful Power Transition: A Case of ICT Standard Setting." *International Area Review* 12 (3): 27–42. https://doi.org/10.1177%2F223386590901200302.

Harwit, Eric. 1998. "China's Telecommunications Industry: Development Patterns and Policies." *Pacific Affairs* 71 (2): 175–193. https://doi.org/10.2307/2760975.

He, Laura, and Ren Wei. 2019. *Shanghai's Hotly Anticipated Tech Board Vital to China's Global Financial Ambitions, Says Top Official*. 23 January. www.scmp.com/business/

companies/article/2183223/shanghais-hotly-anticipated-tech-board-vital-chinas-global. Accessed 5 August 2020.

He, Zhou. 1997. "A History of Telecommunications in China: Development and Policy Implications." In *Telecommunications and Development in China*, edited by Paul S.N. Lee, 55–89. Cresskill: Hampton Press.

Hong, Yu. 2010. *China's Networked Recovery in the Aftermath of the 2008 Global Economic Recession*. Paper Presented at the 8th Chinese Internet Research Confnerece, June 29–30, 2010, Peking University, China.

Hong, Yu. 2017a. "Pivot to Internet Plus: Molding China's Digital Economy for Economic Restructuring?" *International Journal of Communication* 11: 1486–1509.

Hong, Yu. 2017b. *Networking China: The Digital Transformation of the Chinese Economy*. Urbana: University of Illinois Press.

Hong, Yu, and Thomas Goodnight. 2020. "How to Think about Cyber Sovereignty: The Case of China." *Chinese Journal of Communication* 13 (1): 8–26. https://doi.org/10.1080/17544750.2019.1687536.

Hughes, Christopher. 2004. "Controlling the Internet Architecture." In *Cyber China: Reshaping National Indetities in the Age of Information*, edited by Fancoise Mengin, 71–90. New York: Palgrave MacMillan.

Inkster, Nigel. 2016. *China's Cyber Power*. Abingdon: Routledge.

Internet Governance Forum. 2018. *IGF 2018 Speech by French President Emmanuel Macron*. www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron. Accessed 5 August 2020.

Jia, Lianrui. 2018. "Going Public and Going Global: Chinese Internet Companies and Global Finance Networks." *Westminster Papers in Communication and Culture* 13 (1): 17–36. http://doi.org/10.16997/wpcc.280.

Jia, Lianrui. 2020. "Unpacking China's Social Credit System: Informatization, Regulatory Framework, and Market Dynamics." *Canadian Journal of Communication* 45 (1): 113–127.

Jia, Lianrui, and Dwayne Winseck. 2018. "The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization." *International Communication Gazette* 80 (1): 30–59. https://doi.org/10.1177%2F1748048517742783.

Jiang, Min. 2012. "Internet Companies in China: Dancing between the Party Line and the Bottom Line." *Asie. Visions* 47.

Jiang, Min, and King-Wa Fu. 2018. "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?" *Policy and Internet* 10 (4): 372–392. https://doi.org/10.1002/poi3.187.

Keane, Michael, and Huan Wu. 2018. "Lofty Ambitions, New Territories, and Turf Battles: China's Platforms 'Go Out'." *Media Industries* 5 (1): 51–68. https://10.3998/mij.15031809.0005.104,

Keck, Christine. 2000. "Telecom in China: Access to a Growing World Power." *Cambridge Review of International Affairs* 13 (2): 152–163. https://doi.org/10.1080/09557570008400306.

Khan, Lina. 2017. "Amazon's Antitrust Paradox." *The Yale Law Journal* 126 (3): 701–805.

Koleski, Katherine, and Nargiza Salidjanova. 2018. *China's Technonationalism Toolbox: A Primer*. Issue Brief, U.S.-China Economic and Security Review Commission.

Laskai, Lorand, Paul Triolo, Xiaomeng Lu, and Samm Sacks. 2018. "Unleashing China's Capital Markets to Build a 'Cyber Superpower'." *New America*. 17 April. www.newamerica.org/cybersecurity-initiative/digichina/blog/unleashing-chinas-capital-markets-build-cyber-superpower/. Accessed 5 August 2020.

Leong, Susan. 2018. "Prophets of Mass Innovation: The Gospel According to BAT." *Media Industries* 5 (1): 69–87. http://dx.doi.org/10.3998/mij.15031809.0005.105.

Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil Hussian. 2018. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure." *Policy & Internet* 10 (4): 415–453. https://doi.org/10.1002/poi3.183.

Lin, Li-Wen, and Curtis Milhaupt. 2013. "We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China." *Stanford Law Review* 65: 697–759.

Lin, Liza, and Josh Chin. 2017. "China's Tech Giants Have a Second Job: Helping Beijing Spy on Its People." *Wall Street Journal*. 30 November. www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284. Accessed 5 August 2020.

Liu, Weidong, and Michael Dunford. 2016. "Inclusive Globalization: Unpacking China's Belt and Road Initiative." *Area Development and Policy* 1 (3): 323–340. https://doi.org/10.1080/23792949.2016.1232598.

Lu, Ding. 2000. "China's Telecommunications Infrastructure Buildup: On Its Own Way." In *Deregulation and Interdependence in the Asia-Pacific Region*, Vol. 8, 371–413. University of Chicago Press.

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Martina, Michael. 2017. "In China, the Party's Push for Influence Inside Foreign Firms Stirs Fears." *Reuters*. 24 August. www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU. Accessed 5 August 2020.

Martina, Michael, Kevin Yao, and Yawen Chen. 2018. "Beijing Softens 'Made in China 2025' Message in Face of Looming U.S. Trade War." *The Globe and Mail*. 25 June. www.theglobeandmail.com/business/international-business/asia-pacific-business/article-beijing-softens-made-in-china-2025-message-in-face-looming-us/. Accessed 5 August 2020.

Miao, Weishan, and Wei Lei. 2016. "Policy Review: The Cyberspace Administration of China." *Global Media and Communication* 12 (3): 337–340. https://doi.org/10.1177%2F1742766516680879.

Murray, Alan, and Katherine Dunn. 2019. "China Takes Lead in Fortune Global 500: CEO Daily." *Fortune*. 22 July. https://fortune.com/2019/07/22/china-takes-lead-in-fortune-global-500-ceo-daily/. Accessed 5 August 2020.

Nakayama, Shigeru. 2012. "Techno-Nationalism Versus Techno-Globalism." *East Asian Science, Technology and Society: an International Journal* 6 (1): 9–15. https://doi.org/10.1016/S0166-4972(00)00061-4.

Naughton, Barry. 2004. "The Information Technology Industry and Economic Interactions Between China and Taiwan." In *Reshaping National Identities in the Age of Information*, edited by Françoise Mengin, 155–184. New York: Palgrave Macmillan.

Naughton, Barry, and Adam Segal. 2002. "Technology Development in the New Millennium: China in Search of a Workable Model." In *Crisis and Innovation: Asian Technology After the Millennium*, edited by Keller William and Richard Samuels, 160–186. New York: Cambridge University Press.

Negro, Gianluigi. 2019. "A History of Chinese Global Internet Governance and Its Relations with ITU and ICANN." *Chinese Journal of Communication*. https://doi.org/10.1080/17544750.2019.1650789.

The New York Times. 2018. "Cifus, Powerful and Unseen, Is a Gatekeeper on Major Deals." *The New York Times*. 5 March. www.nytimes.com/2018/03/05/business/what-is-cfius.html. Accessed 5 August 2020.

Ning, Lutao. 2009. *China's Rise in the World ICT Industry: Industrial Strategies and the Catch-up Development Model*. London and New York: Routledge.

Nolan, Peter. 2014. *Chinese Firms, Global Firms: Industrial Policy in the Age of Globalization*. Abingdon: Routledge.

People's Daily. 2013. "习近平:胸怀大局把握大势着眼大事 努力把宣传思想工作做得更好" ["Xi Jinping: Advancing Propoganda and Ideological Work"]. *People's Daily*. 21 August. http://cpc.people.com.cn/n/2013/0821/c64094-22636876.html. Accessed 5 August 2020.

People's Daily. 2017. 从网络大国到网络强国，中国在路上. *[From Cyber Power to Cyber Superpower, China is on the Way]. People's Daily*. 7 December. http://it.people.com.cn/n1/2017/1207/c1009-29691084.html. Accessed 5 August 2020.

People's Daily. 2019. "人工智能创新平台再添生力军" ["AI Open Innovation Platform Added New Members"]. *People's Daily*. 15 October. www.xinhuanet.com/info/2019-10/15/c_138472595.htm. Accessed 5 August 2020.

People's Daily Online. 2010. "White Paper Explains 'Internet Sovereignty'." *People's Daily Online*. 9 June. http://en.people.cn/90001/90776/90785/7018630.html. Accessed 5 August 2020.

Petry, Johannes. 2019. "Financialization with Chinese characteristics? Exchanges, Control & Capital Markets in Authoritarian Capitalism." *Economy and Society* 49 (2): 213–238. https://doi.org/10.1080/03085147.2020.1718913.

Plantin, Jean-Christophe, and Gabriele de Seta. 2019. "WeChat as Infrastructure: the Techno-Nationalist Shaping of Chinese Digital Platforms." *Chinese Journal of Communication*. https://doi.org/10.1080/17544750.2019.1572633.

Qiu, Jack Linchuan. 2010. "Chinese Techno-Nationalism and Global Wifi Policy." In *Reorienting Global Communication: Indian and Chinese Media Beyond Borders*, edited by Michael Curtin and Hemant Shah, 284–304. Urbana: University of Illinois Press.

Rosier, Kevin. 2014. "The Risks of China's Internet Companies on U.S. Stock Exchanges." *Staff Report, U.S.-China Economic and Security Review Commission*. www.uscc.gov/research/risks-chinas-internet-companies-us-stock-exchanges-addendum-added-september-12-2014. Accessed 5 August 2020.

Roumeliotis, Greg, Yingzhi Yang, Echo Wang, and Alexandra Alper. 2019. "Exclusive: U.S. Opens National Security Investigation into TikTok." *Reuters*. 1 November. www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL. Accessed 5 August 2020.

Ruan, Lotus, Jeffrey Knockel, Jason Ng, and Masashi Crete-Nishihata. 2016. *One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally*. Citizen Lab Research Brief No. 84.

Schiller, Dan. 2005. "Poles of Market Growth?: Open Questions about China, Information and the World Economy." *Global Media and Communication* 1 (1): 79–103. https://doi.org/10.1177%2F1742766505050174.

Segal, Adam. 2017. *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Aegis Paper Series No.1703, Hoover Institution.

Shen, Hong. 2016. "China and Global Internet Governance: Toward an Alteranative Analytical Framework." *Chinese Journal of Communication* 9 (3): 304–324. https://doi.org/10.1080/17544750.2016.1206028.

Shen, Hong. 2018. "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative." *International Journal of Communication* 2683–2701.

Shen, Wei. 2012. "Deconstructing the Myth of Alipay Drama- Repoliticizing Foriegn Investment in the Telecommunications Sector in China." *Telecommunications Policy* 36: 929–942. https://doi.org/10.1016/j.telpol.2012.08.008.

Shepherd, Christian. 2017. "China Closes 60 Celebrity Gossip Social Media Accounts." *Reuters*. 8 June. www.reuters.com/article/us-china-internet-censorship-idUSKBN18Z0J3. Accessed 5 August 2020.

Shi, Anbin. 2018. "China's Role in Remapping Global Communication." In *China's Media Go Global*, edited by Daya Kishan Thussu, Hugo de Burgh, and Anbin Shi, 34–51. Abingdon: Routledge.

Shim, Yongwoon, and Dong-Hee Shin. 2016. "Neo-Techno Nationalism: The Case of China's Handset Industry." *Telecommunications Policy* 40: 197–209. https://doi.org/10.1016/j.telpol.2015.09.006.

Sina. 2013. "李彦宏：建议取消VIE政策限制. Yanhong Li: Proposed to Cancel VIE Policy Resrtiction." *Sina Finance*. 4 March. http://finance.sina.com.cn/world/20130304/035314704085.shtml. Accessed 8 August 2020.

Srnicek, Nick. 2016. *Platform Capitalism*. Cambridge: Polity.

Sutherland, Dylan. 2003. *China's Large Enterprises and the Challenge of Late Industrialisation*. London: RoutledgeCurzon.

Suttmeier, Richard P. 2005. "A New Technonationalism? China and the Development of Technical Standards." *Communications of the ACM* 48 (4): 35–37. https://doi.org/10.1145/1053291.1053313.

Suttmeier, Richard, and Xiangkui Yao. 2004. *China's Post-WTO Technology Policy: Standards, Software, and the Changing Nature of Techno-Nationalism*. NBR Special Report, Seattle: The National Bureau of Asian Research.

Szamosszegi, Andrew, and Cole Kyle. 2011. *An Analysis of State-Owned Enterprises and State Capitalism in China*. Washington, DC: U.S.-China Economic and Security Review Commission.

Thun, Eric, and Timothy Sturgeon. 2019. "When Global Technology Meets Local Standards." In *Policy, Regulation and Innovation in China's Electricity and Telecom Industries*, edited by Loren Brandt and Thomas Rawski, 177–220. Cambridge: Cambridge University Press.

U.S.-China Economic and Security Review Comission. 2016. *2016 Report to Congress of the U.S.-China Economic and Security Review Commission*. Washington, DC: U.S. Government Publishing Office.

van Eeten, Michel, and Milton Mueller. 2012. "Where is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–736. https://doi.org/10.1177%2F1461444812462850.

Vila Seoane, Maximiliano Facundo. 2019. "Alibaba's Discourse for the Digital Silk Road: The Electronic World Trade Platform and 'Inclusive Globalization'." *Chinese Journal of Communication*. https://doi.org/10.1080/17544750.2019.1606838.

Wang, Orange. 2019. "China-US Rivalry on Brink of Becoming a 'Financial War', Former Minister Says." *South China Morning Post*. 9 November. www.scmp.com/economy/china-economy/article/3037039/china-us-rivalry-brink-becoming-financial-war-former-minister. Accessed 5 August 2020.

Wang, Xiangwei. 1999. China Unicom Gives CCF Investors August Quit Deadline." *South China Morning Post*. 26 July. www.scmp.com/article/289010/china-unicom-gives-ccf-investors-august-quit-deadline. Accessed 5 August 2020.

Weinland, Don. 2017. "Alibaba and Tencent Join State-Owned Groups in $11.7bn China Unicom Investment." *Financial Times*. 16 August. www.ft.com/content/7b1e59bc-c1fa-393a-bee4-0851a0a1df30. Accessed 5 August 2020.

White House Office of Trade and Manufacturing Policy. 2018. *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*. Washington, DC: The White House.

Wong, Chun Han, and Eva Dou. 2017. "Foreign Companies in China Get a New Partner: The Communist Party." *Wall Street Journal*. 29 October. www.wsj.com/articles/foreign-companies-in-china-get-a-new-partner-the-communist-party-1509297523. Accessed 5 August 2020.

Woo, Stu. 2019. "Alibaba Shares Enjoy a Strong Start in Hong Kong." *Wall Street Journal*. 26 Novemeber. www.wsj.com/articles/a-strong-open-sesame-for-alibaba-in-hong-kong-11574746859. Accessed 5 August 2020.

Wu, Jing, and Guoqiang Yun. 2018. "From Modernization to Neoliberalism? How IT Opinion Leaders Imagine the Information Society." *The International Communication Gazette* 80 (1): 7–29. https://doi.org/10.1177%2F1748048517742773.

Wübbeke, Jost, Mirjam Meissner, Max Zenglein, Jaqueline Ives, and Björn Conrad. 2016. *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries*. Berlin: Mercator Institute for China Studies.

Xia, Bingqing. 2018. "Capital Accumulation and Work in China's Internet Content Industry: Struggling in the Bubble." *The Economic and Labor Relations Review* 29 (4): 501–520. https://doi.org/10.1177%2F1035304618810987.

Xia, Bingqing, and Christian Fuchs. 2016. *The Financialisation of Digital Capitalism in China*. London, UK: Westminster Institute for Advanced Studies.

Xinhua. 2014. 习近平主持召开中央网络安全和信息化领导小组第一次会议 *Xi Jinping Chairs First Meeting of Central Leading Group On Cybersecurity and Informatization*. 27 Feburary. http://cpc.people.com.cn/n/2014/0227/c64094-24486402.html. Accessed 5 August 2020.

Xinhua. 2019. *Alibaba Makes Robust 'Homecoming' Listing in Hong Kong*. 27 November. www.china.org.cn/business/2019-11/27/content_75450775.htm. Accessed 5 August 2020.

Xu, Duoqi, Shiya Tang, and Dan Guttman. 2019. "China's Campaign-Style Internet Finance Governance: Causes, Effects, and Lessons Learned for New Information-Based Approaches to Governance." *Computer Law & Security Review* 35: 3–14.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'." *Politics & Policy* 45 (3): 432–464. https://doi.org/10.1111/polp.12202.

Zenglein, Max, and Anna Holzmann. 2019. "Evolving Made in China 2025: China's Industrial Policy in the Quest for Global Tech Leadership." *MERICS Papers on China, Mercator Institute for China Studies*. https://merics.org/en/report/evolving-made-china-2025. Accessed 5 August 2020.

Zhang, Yongjin. 2003. *China's Emerging Global Businesses: Political Economy and Institutional Investigations*. Basingstoke and New York: Palgrave Macmillan.

Zhao, Lei, and Yin Cao. 2014. "President Xi Vows to Boost Cybersecurity." *China Daily*. 28 Feburary. www.chinadaily.com.cn/china/2014-02/28/content_17311483.htm. Accessed 5 August 2020.

Zhao, Yuezhi. 2010. "China's Pursuits of Indigenous Innovations in Information Technology Developments: Hopes, Follies and Uncertainties." *Chinese Journal of Communication* 3 (3): 266–289. https://doi.org/10.1080/17544750.2010.499628.

Zhao, Yuezhi, and Jing Wu. 2020. "Understanding China's Developmental Path: Towards Socialist Rejuvenation?" *Javnost- The Public* 27 (2): 97–111. https://doi.org/10.1080/13183222.2020.1727274.

Zhong, Raymond, Paul Mozur, and Iris Zhao. 2018. "*Horns Honk, and Censors in China Get a Headache.*" *The New York Times*. 12 April. www.nytimes.com/2018/04/12/business/china-bytedance-duanzi-censor.html. Accessed 5 August 2020.

6 "Nine dragons run the water"

Fragmented internet governance in China

Ting Luo and Aofei Lv

Introduction

At the Internet Governance Forum in November 2018, French President Emmanuel Macron summarised the Chinese form of internet governance as one controlled by a dominant authoritarian state (Macron 2018). While this summary is overly simplistic and lacks the nuance necessary to understand Chinese internet governance, it does reflect the predominant view of the Chinese model by Western scholars and observers (for example, see King, Pan and Roberts 2013; 2017). Standing in contrast to the cyber-utopian vision, which considers the internet as a liberating technology that mobilises political movement and strengthens democracy (Castells 2015), this perspective perceives China's internet model as one in which the all-powerful authoritarian government is able to utilise the internet as technologies of surveillance and control and to sustain its authoritarian regime. In this telling, the authoritarian control over the internet in China started with the building of the Great Firewall of China in the 1990s, which separates the Chinese domestic network from the global net (see, for example, Qiu 2000). Within the Chinese domestic network, China has used the internet as a tool for surveillance and control, which includes blocking websites and censoring information (Chase and Mulvenon 2002; MacKinnon 2009), suppression of dissident use (Chase and Mulvenon 2002; Qiu 2000), and employment of web commentators to shape and alter public debate (Bandurski 2008; Han 2015; Miller 2016; Gallagher and Miller 2017; King, Pan and Roberts 2017).

These studies focus on the use of the internet in sensitive areas – those vital to the legitimacy and survival of the regime. Issues that directly threaten the regime's stability are deemed sensitive, such as criticising top political leaders or organising collective actions (Birney 2014; King, Pan and Roberts 2013; Shirk 2007). It is important to note that the definition of "sensitive" is dynamic and changes over time (Stern and Hassid 2012; Stockmann, Luo and Shen 2020). Non-sensitive issues can become sensitive over time. Take the Covid-19 pandemic, underway as we write this, as an example. When the discussion in early-2020 in China on Covid-19 focuses on doctors fighting the virus, it is not considered to be sensitive; however, as soon as the discussion shifts towards the whistleblower doctors and their heroic acts of warning others about the emergence and seriousness of

DOI: 10.4324/9781003008309-9

Covid-19 before any official announcements by the government, it becomes sensitive because it is considered to be a challenge to government authority and reputation and likely to destabilise the regime. Among the aforementioned studies on China's internet model, for example, Chase and Mulvenon (2002) analysed the use of the internet by the Chinese government to silence dissidents. King, Pan and Roberts (2013, 2017) focused on two aspects of the online censorship programme adopted by the Chinese government: silencing collective expression and employment of web commentators to distract public debate over controversial issues. These are the uses of the internet in sensitive areas which the Chinese government deems to have the potential to destabilise the regime.

In contrast, little attention has been paid to Chinese internet governance in non-sensitive areas, such as promoting technology-driven economic development, the use of the internet in providing better social services and public goods, and the protection of user privacy. In this chapter, we use the concept of "fragmented authoritarianism" to argue that in contrast to the Chinese government's efforts to centralise the internet in overtly sensitive areas – those perceived as being vital to the stability and survival of the regime, fragmentation persists in other non-sensitive areas, such as health, the focus of case study in this chapter.

We make two important contributions to fragmented authoritarianism theory. We are among the first to adapt fragmented authoritarianism – a framework to explain the political system and policy process in China (Lieberthal and Oksenberg 1988) – to the field of internet governance. We argue that in the governance of the internet in non-sensitive areas, a fragmentation that can be characterised as "Nine dragons run the water" (*jiulong zhishui*) is the dominant form of governance.[1]

"Nine dragons run the water" is a Chinese proverb that vividly depicts how internet governance actually occurs in China. In Chinese mythology, dragons are authorities responsible for controlling and managing water and weather. When the nine dragons each has its own opinion on how to run the water, either no dragon takes the initiative to manage the water or all compete for the management of the water. The results are natural disaster, whereby there is either too much water (floods) or too little water (drought). This proverb has been used by scholars in China to describe the multiple-principal problem in food regulation, public administration, and internet governance (Ding and Sun 2014; Fang 2016; Shi and Sun 2008). In China, different authorities at the central level are assigned different responsibilities (and pursue diverging agendas) related to the internet in non-sensitive areas, leading to confusion as well as tensions between authorities and resulting in obstacles and barriers to effective internet governance.

Second, we enrich the fragmented authoritarianism theory. Previous scholarship in fragmented authoritarianism demonstrated that political fragmentation provides fissures whereby information – one of the most important aspects of power – is jealously guarded by competing authorities, leading to intense bargaining and competition in the policymaking process and allowing policy entrepreneurs to enter the process (Lv 2015; Mertha 2009; Zhu 2008). Yet, another scenario that has not been studied is when fissures provide a regulatory vacuum whereby it is in no authority's interest and responsibility to act and regulate.

In this chapter, relying on interviews with government officials and product managers of internet companies, we select two online health scandals as our case studies. We find that the centralised authoritarian nature of internet governance in China only applies to sensitive areas – those vital to the political stability and survival of the regime – while in other non-sensitive areas fragmentation persists, such as online health content, as the two cases have suggested, creating a regulatory vacuum and resulting in the situation of "Nine dragons run the water". In the case of online health content, the regulatory vacuum gives rise to exaggerated claims of medical treatment or even fake medical information online, seriously affecting patients' life choices.

This chapter proceeds as follows. We begin by elaborating our theoretical framework, fragmented authoritarianism. In the section that follows, we apply the framework to internet governance in China and argue that the Chinese government's internet governance in non-sensitive areas – those not vital to Party survival – are characterised by the Chinese metaphor "Nine dragons run the water". We then use two health scandals caused by fragmentation in the regulation of online health content as a case study. Finally, we conclude the chapter by considering the political implications of our findings beyond China. The challenge of dealing with the regulation of online user-generated content is shared by Chinese and Western governments, while the criteria, which are used to judge type of content to regulate and to decide the allocation of staffing resources, who are considered to be the relevant authorities and their responsibilities as well as sources of legitimacy, are specific to the nature of the regime (that is, democratic or authoritarian).

Fragmented authoritarianism

Fragmented authoritarianism is a theoretical framework developed and used by scholars to study the political system and policy process in China. The concept was first introduced by Lieberthal and Oksenberg (1988) to explain environmental policymaking in China and was further developed by Mertha (2009) to explain environmental politics and international trade politics in China. This concept highlights two key characteristics of the Chinese political system. First is its authoritarian nature, characterised by the one-party rule of the Chinese Communist Party. As depicted in Figure 6.1, the Chinese political system has a hierarchical pyramidal structure consisting of five levels, from the highest central level to the lowest township level (Luo 2014). Within this structure, policymaking power is monopolised by a small number of top officials and party leaders at the central level.

Second, the authoritarian state is not unified, but rather is fragmented and disjointed: Responsibilities and authority are delegated not only vertically from the central government to various local-level governments but also horizontally across different government ministries or bureaus. As a result, although the central government remains at the top of the power hierarchy, this delegation provides opportunities for competition and bargaining between governments at different levels

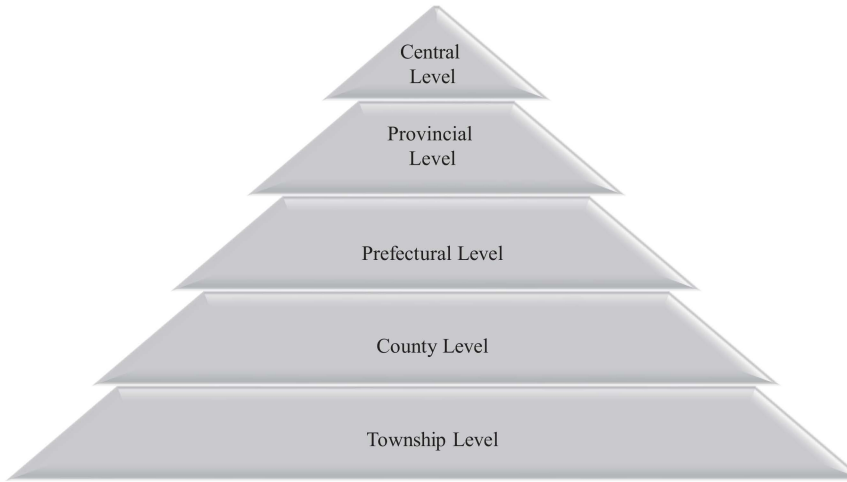


Figure 6.1 The administrative hierarchy of the Chinese political system

and between different government ministries or bureaus (Zhang et al. 2012). In other words, there are fissures within vertical and horizontal political systems whereby problems and opportunities are equally likely to occur.

We borrow this framework of fragmented authoritarianism to explain internet governance in China. On internet governance, authoritarianism is practiced in sensitive areas that are seen to directly threaten the regime's stability, such as criticising top leaders and government performance, organising protests and engaging in any collective action organised outside of the governmental control (King, Pan and Roberts 2013). With respect to these issues, the government's internet governance efforts focus on centralising political control over and utilising the internet for surveillance and censorship. This approach is reflected by the institutional changes adopted by Xi Jinping's administration in 2014 creating a centralised and integrated institutional framework for propaganda and political censorship on China's cyberspace (Creemers 2017).

However, in internet governance areas that are not perceived as being sensitive, such as health[2] or e-commerce, fragmentation dominates, providing actors with opportunities as well as obstacles to implement policies. Opportunities emerge as the system leaves space for policy outsiders to enter the policy process and bring in opinions and voices from outside the government in areas such as health, environment, and urban migrant policy (Lv 2015; Mertha 2009; Zhu 2008). Obstacles arise when different and conflicting interests either compete for resources or do not want to take responsibility.

A comparative study of the drafting of China's Internet Security Law (ISL) drafted between mid-2014 to June 2015 and the E-Commerce Law (ECL) drafted between

late 2013 to March 2016 illustrates how fragmented authoritarianism framework can be extended to internet governance (Deng and Liu 2017). The study examines the lawmaking process for two laws characterised as having different degrees of political sensitivity for the Chinese government. The first, China's ISL, directly touched on issues of national security and party leadership; the central leadership remained in control over its drafting, which was subject to only limited and formalistic consultation, especially from policy entrepreneurs. This degree of state dominance was not observed, however, in the drafting of the ECL. Being a law that emphasised economic interests that were not directly related to national security and party control, the drafting of this legislation reflected the opportunities and obstacles that one would expect from a system characterised by political fragmentation, in an area not seen as being directly relevant to party survival. The process included both meaningful consultation and participation, thus providing actors with opportunities to influence the process. At the same time, however, the process also created obstacles, in that tensions between different ministries and bureaus resulted in the drafting of "unreasonably polarised" law (Deng and Liu 2017, 692).

Based on this comparative study of the drafting of two laws related to internet issues with different levels of sensitivity to the regime, it is reasonable to believe that fragmented authoritarianism also characterises internet governance in China. Therefore, we propose to understand China's internet model from the perspective of fragmented authoritarianism. More importantly, while some scholars overemphasise the authoritarian nature of the China model (for example, Chase and Mulvenon 2002; King, Pan and Roberts 2013; Qiu, 2000), we suggest that we should start looking at the fragmentation aspect and derive a more accurate understanding of China's internet governance. In this spirit, the following section starts by applying fragmented authoritarianism to internet governance in China.

Fragmented internet governance in China: nine dragons run the water

Fragmented authoritarianism has two key characteristics: centralised authoritarian control and political fragmentation. Internet governance in China shares these two characteristics. Because policymaking power is monopolised by top officials and party leaders at the central level, our analysis focuses on the authorities at the central level.

On the governance of information and communications technology, which includes the internet, the Chinese government faces a dilemma (Zheng 2007). On the one hand, the government deems information and communications technology to be an important engine for economic growth; therefore, decentralisation and autonomy are needed in order to promote technological innovation and development. On the other, information and communications technology is also of political significance and has the potential to affect the regime's stability and survival, therefore requiring centralisation and political control to rein in the negative political impact of technology as it relates to national security and the Chinese Communist Party's continued rule.

However, these two tasks – promoting technological development and innovation and exercising political control and censorship on the internet – do not always align with each other (Lee and Lio 2016). As a result, on the governance of information and communications technology the leadership oscillates between a desire for decentralisation to promote technological innovation and development and a desire for centralisation in order to rein in the liberating potential of information and communications technology, a tendency we also witness over time in the change of the governance structure of information and communications technology (Zheng 2007).

To complicate this dilemma further, these two objectives are assigned to authorities from two different systems. Within China's political institutions, the de facto top decision-making body is the Politburo Standing Committee, headed by the general secretary, which since 2012 has been Xi Jinping. There are two separate systems underneath the Politburo Standing Committee, the Chinese Communist Party system and the State Council system, each of which has relatively clear divisions of labour and responsibility. The Party system is in charge of maintaining and promoting the ideology of the Chinese Communist Party and its principles,[3] disciplining government officials (in cases, for example, of corruption), ensuring the Chinese state's territorial integrity (a mandate that covers issues such as those related to the status of Taiwan, Hong Kong, Macao and the South China Sea), and commanding the military. The State Council system, meanwhile, is responsible for practical and administrative issues, such as economic development and the provision of social services (such as health care provision and welfare support). The State Council is also known as the chief administrative authority or the central people's government and is led by the premier.

On internet governance, the Party system is responsible for undertaking political surveillance and censorship and maintaining stability, while the State Council system is responsible for promoting the internet-driven economy (Lv and Luo 2018; Zheng 2007). Because of the leadership position of the Chinese Communist Party, promoting the internet-driven economy is subordinate to and has to serve the principal political goal of undertaking political surveillance and censorship and maintaining stability. This arrangement defines the centralised authoritarian nature of internet governance in China.

The development of internet governance in China can be divided into two periods with the creation of the Central Leading Group for Internet Security and Informatisation (CLGISI) chaired by President Xi in 2014 serving as the dividing line (Xinhua News 2014). The main change between the two periods involved the centralisation of the mandates regarding content regulation, which were taken away from various ministries, bureaus, and departments from both systems and placed in the hands of the CLGISI and its functional office, the Cyberspace Administration of China (CAC). Figure 6.2 shows the institutional structure of ministries and bureaus with mandates on internet governance within the State Council system, which remains unchanged since 2014. Figure 6.3 shows the institutional structure of ministries, bureaus, departments and offices with clear mandates on

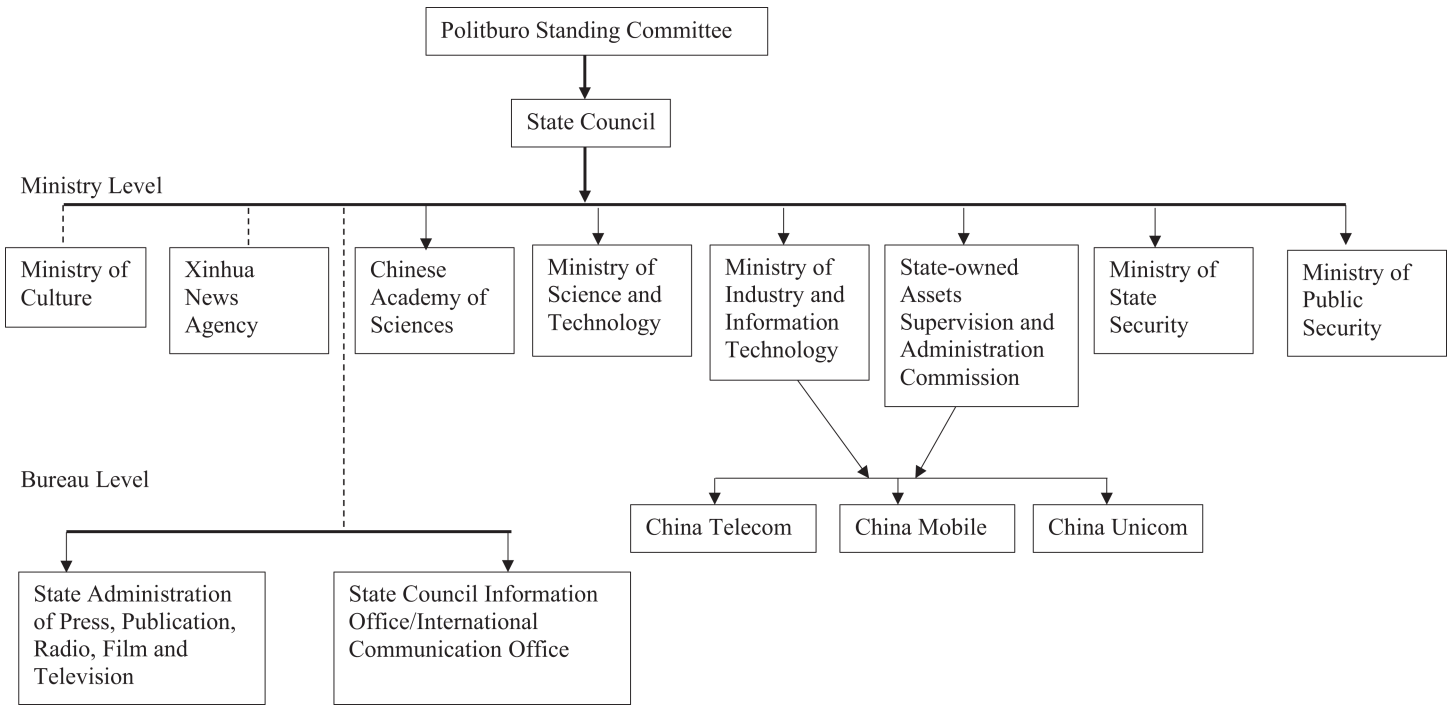


Figure 6.2 Institutional structure of internet governance in China within the State Council system

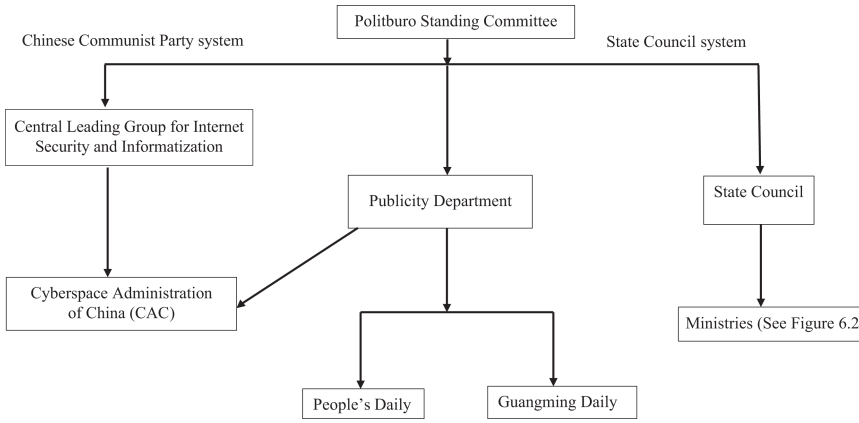


Figure 6.3 Institutional structure of internet governance in China after 2014

internet governance within both systems after 2014, the primary institutional change being the creation of the CLGISI and its subordinate authority – the CAC.

Recentralisation of internet censorship in sensitive areas

The key change in the mandates regarding content regulation had to do with sensitive areas of internet governance – those likely to threaten stability and regime survival. The primary objective of the newly established authorities, the CLGISI and its subordinate, the CAC, was in control of areas deemed to be related to national security and the party's rule inherited from the political nature of the regime.

Before 2014, the internet was treated by the Chinese government as just another media channel similar to traditional mass media, with online content regulation assigned to authorities, within the two systems, that were already tasked with producing, managing, regulating and censoring content in traditional media. Within the State Council System, the key agencies were the Ministry of Culture[4] and Xinhua News agency at the ministry level; at the bureau level these were the State Administration of Press, Publication, Radio, Film and Television and the State Council Information Office/International Communication Office.

Within the Chinese Communist Party system, the relevant agency was the Publicity Department, which fell under Politburo Standing Committee in charge of ideology control on any media and in any format, such as print publications, radio, film and television as well as media including, for instance, traditional media, such as party newspapers (such as *The People's Daily* and *Guangming Daily*). A very important aspect of ideology control is content surveillance and censorship. Ministries and bureaus whose responsibilities involve content production,

management, surveillance and censorship – the Ministry of Culture, Xinhua News Agency at the ministry level, and the State Administration of Press, Publication, Radio, Film and Television at the bureau level and State Council Information Office/International Communication Office at the bureau level – are in practice answerable to the Publicity Department, even though institutionally they are placed under the State Council in the State Council system.

Given its pre-2014 treatment of the internet as an alternative media channel similar to traditional media, the Chinese government found that both its strategy and its institutional structure posed challenges when it came to controlling effectively online content and public opinion and implementing effective regulation in sensitive areas, especially in times of crises. The distinctive feature of the internet is its technological property of decentralisation, which makes it unlike traditional media (Lei 2011). The internet, especially social media, breaks the monopoly of information dissemination by organisations, such as traditional media outlets, or state or party institutions, by allowing individuals to be not only the audience but also the source of information (Newhagen 1998; Stockmann and Luo 2017). For example, in the aftermath of the collision of two high-speed trains in Wenzhou in Southeast China on 23 July 2011, stories and video about the crash were published online by internet users, sparking heated discussions and criticism about the government's performance in constructing the high-speed railways the trains had used and on the government's initial cover-up of the number of deaths and injuries caused by the collision. The government had a hard time controlling online discussions on the accident and silencing criticism (Murphy 2011).

In 2014, the CLGISI and its functional office the CAC were created by President Xi to centralise administration and regulation on cyberspace (State Council 2014). As part of the process of centralising cyberspace administration and regulation, the CAC has taken over mandates related to cyber administration from various departments, bureaus and ministries within both systems. It took over online content control from the Publicity Department of the Party system and from Ministry of Culture, Xinhua News Agency, State Administration of Press, Publication, Radio, Film and Television, and the State Council Information Office/International Communication Office. It also took over regulation and technical control on cyberspace from the Ministry of Industry and Information Technology, the Ministry of Science and Technology, and the Chinese Academy of Sciences and law enforcement related to cyberspace administration from the Ministry of Public Security. As a result, the CAC has centralised regulation and control over online content with its clear mandate, authority, and technical control on content regulation and law enforcement power. Its decisive authority in the area of content control and regulation is also underscored by a comment from an official from the Ministry of Industry and Information Technology in an interview:

> The CAC holds the decisive power [in cyberspace administration and regulation], although it should be us [Ministry of Industry and Information Technology]. . . . Since the foundation of the CAC, it took lots of power from us. How can we say no? The head of the CAC directly reports to the Party

> Secretary [Xi Jinping], but we have to report to the Minister, who reports to the Prime Minister and then reports to the Party Secretary; by then they [the CAC] already got what they want. When they circulate a policy document for our suggestions, we have to respond as soon as possible; however, when we ask for their opinions, we can't decide the policy without their confirmation and they usually delay it![5]

While the CAC formally has responsibility for cyber administration (including internet governance), its routine work prioritises the regulation of sensitive online content over non-sensitive online content, such as online medical content. This is underscored in the speech by President Xi in the first meeting of CLGISI: "Without cyber security, there will be no national security" (Xinhua News 2014). Cybersecurity is the upmost goal of the new leading group and its functional office. It is important to note that the notion of sensitivity or the concept of cybersecurity, as mentioned earlier, is dynamic and changing. What issues that might threaten the regime are based on judgement calls and perceptions of the party and the CAC. A pandemic, like the Covid-19 pandemic, can change from a non-sensitive issue concerned only the symptoms of the affected to a sensitive one concerned the legitimacy of the party's ruling in China.

Persistent fragmentation in non-sensitive areas

Despite this centralisation of certain aspects of internet governance, fragmentation has persisted in non-sensitive areas throughout the pre-2014 and the post-2014 periods, characterised by the existence of different relevant authorities at the central level of the Party and State Council systems, all with mandates touching upon different aspects of internet governance. The key difference lies in whether they have mandates on regulating content. As mentioned earlier, content regulation was scattered around several authorities within the Party and State Council systems before 2014 and was centralised in the hands of the CAC in 2014.

None of the remaining ministries and bureaus within the State Council – the ones not placed under the CAC – are involved in content regulation. Instead, they focus on non-content-related areas of internet governance. More specifically, the Ministry of Science and Technology is responsible for planning science and technology development which information and communications technology is a part of and coordinating science and technology activities. The Ministry of Industry and Information Technology is responsible for the regulation and development of the internet, wireless, broadcasting, communications, production of electronic and information goods, the software industry, and so on. Internet infrastructure is provided by three state-owned enterprises, China Telecom, China Mobile, and China Unicom. They provide technical infrastructural services essential for the connection to the internet, such as broadband, cables, signals, base stations, and sim cards. These three state-owned enterprises are answerable to the State-owned Assets Supervision and Administration Commission, the responsibility of which, as its name suggests, is to preserve and increase state-owned

assets, while the regulatory standard for internet infrastructure is set up by the Ministry of Industry and Information Technology. The Chinese Academy of Sciences, functioning as the national scientific think tank and academic governing body, is responsible for providing advisory and appraisal services on issues related to science and technological progress.

None of these aforementioned ministries and bureaus have law enforcement power. They can only execute administrative sanctions, such as issuing warnings, warrants, and penalties. In contrast, the Ministry of Public Security (the police) and the Ministry of State Security (intelligence agency) have law enforcement power and can arrest and charge companies as well as individuals with violations of regulations and laws related to areas of internet governance.

In keeping with a finding that this part of internet governance – the part focused on non-sensitive issues – is characterised by fragmentation, we observe two things. First, as the earlier description of ministries and bureaus with mandates on non-content-related internet governance suggests, mandates and law enforcement power are assigned to different authorities, creating a governance situation resembling nine dragons running the water. Second, the diverging agendas pursued by the two systems – one seeking technological innovation and development and the other stability and national security – and the centralisation of cyberspace administration authority, especially online content regulation, within the CAC has further exacerbated the fragmentation of Chinese internet governance, as areas not vital to the political stability and the Party's ability to rule have been left effectively decentralised. The result has been a regulatory vacuum with respect to non-sensitive areas of internet governance, such as the economic development aspects of Chinese internet governance.

Case study: Baidu's health scandals

Online health content – with the exceptions noted earlier – falls into non-sensitive areas and, therefore, in the following section, we turn to two case studies of online health scandals and demonstrate the characteristic of "Nine dragons run the water" in China's internet governance in areas not vital to regime stability. As previously discussed, while the creation of the CAC resulted in centralised internet censorship and surveillance of online content in sensitive areas, in non-sensitive areas Chinese internet governance remains characterised by fragmentation, with different authorities at the central level assigned different, sometimes conflicting responsibilities and having diverging agendas related to the internet. This fragmentation provides fissures and leads to a scenario in which no authority has a direct interest in and responsibility for regulating online content in non-sensitive areas or access to the information needed to act and regulate. Two health scandals vividly demonstrate the scenario whereby fragmentation provides a regulatory vacuum in the regulation on online health content.

We choose to focus on the following two health scandals for the following reasons. First of all, as the chapter in this volume by Rone notes, online content is an important aspect of internet governance. Second, because online health content is not

seen as vital to the legitimacy and survival of the regime, it is a non-sensitive area of the type in which we would expect fragmentation to persist. The major exception to this rule, of course, is the global novel coronavirus pandemic that began in late 2019. As we write this in mid-2020, the virus has created an existential crisis to the regime. Measures to contain the virus have serious implications to individual life, which have given rise to public outcry questioning the legitimacy and ruling of the Party. There is evidence that public outcry occurred online since the outbreak of the pandemic towards government's handling of the virus, including but not limited to the lack of humanitarian care due to draconian lockdown measures, the government's initial cover-up of the emergence of the pandemic, the reprimand of the whistleblower doctors, and the massive censorship and surveillance online (Ruan, Knockel and Crete-Nishihata 2020). The legitimacy of the regime is contingent on the delicate handling of the pandemic by the government. Therefore, there were centralised efforts to contain online content related to Covid-19 and content on Covid-19 became sensitive. That said, online health content not related to a pandemic like Covid-19 tends not to be considered as sensitive.

The regulatory vacuum regarding online health content

The number of internet users in China more than doubled between 2009 and 2018, rising from 338 million to 829 million (CNNIC 2009, 2018). One distinctive feature of the internet, particularly as it relates to social media, is the prevalence of user-generated content. Such content tends to be published on online platforms owned and managed by private companies. The sheer amount of online content produced every day and the decentralised nature of online content production poses a great challenge for those agencies and countries wishing to regulate and manage online content, one not unique to China (see, for example, Mintzes 2016). For its part, because of its potential to have real effects on people's health and wellbeing, online health information is a special area of online content that requires professional knowledge in order to be useful (and not harmful).

As was previously noted, China's initial approach to regulating the internet involved treating it as just another form of mass media. However, these institutional structures and the fragmentation that characterised internet governance proved unable to deal with the peculiarities related to the massive decentralised production of online health content, and in particular the fake online medical content that culminated in 2016 with two major health scandals, in which the management and moderation rights of some medical sub-forums were sold to commercial companies. Subsequently a student died after receiving experimental treatments proven to have failed clinical trials in the United States that he learned of from a promoted result on Baidu search.

In the run-up to the 2016 health scandals, fragmentation had created a regulatory vacuum as it related to online medical content. While the CAC has a clear mandate and priority on online content in sensitive areas, no one was directly responsible for regulating medical content which is not sensitive in this fragmented system.

Effective regulation of online medical content in China would involve engaging the knowledge and expertise of many different authorities. First, because online medical content is related to health care and medical services and requires professional medical knowledge, it always falls under the purview of the Ministry of Health, which is the policymaker and regulator of medical services and health care in China.[6]

Second, medical content is published on online platforms owned and managed by commercial companies and thus touches upon the commercial activities of technology companies. What's more, because online medical content can affect consumer choices regarding medical services, it brings consumer interests and rights into play. As a consequence of both of these aspects of online medical information, the State Administration for Industry and Commerce at the bureau level, responsible for regulating business activities and consumer protection, would also have the authority and expertise to regulate this content.[7]

Third, because producing online medical content is a commercial activity of internet companies, it also falls under the purview of the Ministry of Industry and Information Technology, responsible for monitoring the daily operation of the internet industry. All three aforementioned departments are within the State Council system. Last but not least, content-regulating authorities could also be seen to have a responsibility for managing and regulating online health content. As a reminder, the CAC within the Party system has been responsible for regulating content since 2014 although, as has been noted, its focus is on content deemed sensitive.[8] Investigating and regulating fake online medical content, therefore, requires the coordination of all these authorities that have the mandate, resources, and expertise.

As a consequence of this fragmentation, no single government agency is responsible for regulating online medical content, making it difficult for any single authority to initiate a coordination of authorities and resources, particularly given the lack of overlap (and somewhat conflictual/contradictory objectives) between the Party system's prioritisation of political stability and the State Council's prioritisation of economic development. As mentioned earlier, although the CAC formally has responsibility for cyberspace administration and regulation, it prioritises the regulation of sensitive online content over non-sensitive online content, such as online medical content. For their part, authorities within the State Council system have only expressed a limited interest in regulating online medical content, concentrating instead on economic-development issues. The State Council's 2015 "Internet Plus" national development plan positioned information and communications technology development as a new engine for sustainable economic growth (State Council 2015). In order to realise this potential, the State Council and its ministries and bureaus followed policies to give internet companies a relatively free environment in which to experiment and develop digital technologies, including data-driven algorithms (Lv and Luo 2018).

Moreover, as an internet giant and a key contributor to China's internet-driven economy, Baidu, the focus of the following case studies, heavily relies on online health advertising as its source of revenue (Huang 2016). Policy and pragmatism

therefore resulted in a situation in which it was neither in the CAC's nor in the State Council's interest to regulate and control online health-related advertising.

Conflicting agendas and interests in regulating online health content led to a regulatory vacuum and culminated in two health scandals on platforms owned by Baidu, one of the three biggest Chinese internet giants. We focus on two platforms owned by Baidu – Baidu Tieba and Baidu Search – because they are the main sources of health content and information in China. Baidu was founded as an internet search engine in 2000 and soon grew to become China's main search engine. As of January 2016, Baidu accounted for 75 percent of search engine market share by all platforms in China, including desktop, tablet, and mobile.[9] In China, there are few options for patients to seek information about treatment for diseases, especially rare and complex ones, such as cancer, HIV/AIDS, and hemophilia. As the main search engine in China, people mainly look for health information on Baidu Search. As an integrated part of Baidu Search, Baidu Tieba is a bulletin-board system, an online forum whereby users build their own interest groups and exchange information. The only way to look for and get into specific sub-forums is to search the keywords on Baidu Search.[10] People searching for detailed health information on a specific type of disease can usually find relevant information in those sub-forums on Baidu Tieba, as it aims to provide a communication channel for people with niche interests or hobbies as well as those looking for specific knowledge.[11]

The hemophilia forum scandal

As of January 2016, Baidu Tieba has more than a billion registered users and 20 million sub-forums covering an enormous range of topics, from entertainment and lifestyle, such as music, sports, video games, and food, to more specialised knowledge, such as medical information (Feng 2016; Meng 2016). Users are free to set up their own sub-forums, and each sub-forum has its own coordinators, referred to as forum hosts and vice-hosts, who are considered as the owner and head administrator of their particular sub-forum. Their responsibilities include coordinating and regulating activities and posts, attracting new members, and establishing relationships and organising online or offline activities with other sub-forums. According to a Baidu Tieba senior product manager, anyone can be a sub-forum coordinator: "Baidu Tieba provides the platform, while all content on the platform are generated and organised completely and voluntarily by the users. We do not intervene; instead, we give them freedom and autonomy to organise their own interest groups."[12] In other words, the responsibility to moderate and manage content in sub-forums is left to the users instead of the commercial companies that run the platform. Sub-forum users judge and check whether content on the sub-forums is legitimate and trustworthy or not, regardless of expertise or background.

Since 2015, as part of a business plan to generate revenue from Baidu Tieba, Baidu sold the moderation and management rights of some health-related sub-forums to pharmaceutical companies and hospitals (Securities Daily 2016). The issue was brought into the spotlight by a whistleblower, a member of the

management team of the sub-forum on hemophilia, a genetic blood disease that affects the blood's ability to clot. This sub-forum is claimed to be the most popular source of information on hemophilia in China (NetEase 2016). On 10 January 2016, the whistleblower published a post on a question-and-answer website Zhihu (much like the American Quora site), in which she claimed that she had been stripped of her rights and responsibilities as a host of the sub-forum and that her account had been suspended.[13] She revealed that Baidu had sold the management and moderation rights of the sub-forum to a third party – an unlicensed private, for-profit hospital that specialises in hemophilia treatments – and that the former management team of the sub-forum had been not notified of the change (Fan 2016).

The sub-forum was created and managed by users from the very beginning. Before this scandal, as noted earlier in the interview with a Baidu Tieba senior product manager, Baidu exercised oversight responsibility without directly intervening in the selection of the management team and the daily management of the sub-forum and only stepped in if there were user complaints. Baidu Tieba has a set of formal rules if they were to remove forum moderators from their role, such as receiving user complaints, initiating confidence votes, announcing the voting results, and informing the moderators.[14] In this scandal, the former management team has been removed from their role without following any set rules, and their accounts were also suspended. Baidu has in effect violated its principle of "giving users freedom and autonomy to organise their own interest groups"[15] and changed the nature of Baidu Tieba from user-managed and not-for-profit forums to commercial and profit-driven ones.

The sale of these moderation and sub-forum management rights was consequential. The for-profit hospital bought the rights in order to bring in new customers and thus to make more money. After the sale, the hospital allegedly flooded the sub-forum with medical advertisements, including ones containing misleading information and exaggerated claims regarding the effects of treatments carried out by the hospital (Bai 2016). What's more, the moderation rights allow the owner to edit content on the sub-forum. In this case, it allowed the hospital to moderate or even delete negative content that may harm its reputation or business practices. This is not an abstract concern: Forum users and the media report that the founder and president of the hospital allegedly sold unproven medicines and posted misleading advertisements back in 2014 (Meng 2016).

However, after the sub-forum was sold to the hospital, any negative information about the hospital or its treatments was deleted. In other words, the sale changed these medical sub-forums from a channel whereby users can exchange and discuss medical information to a commercial platform containing only information about and advertisements for the hospital that owns the sub-forum's management rights.

The whistleblower's post on the Zhihu website brought Baidu's business practice – selling medical sub-forums to commercial companies – into the spotlight. As the key source of information for patients, these medical sub-forums have a real effect on people's health. The key public interest concern is the selling of these professional sub-forums to commercial companies without any vetting of

the qualifications of these organisations or any monitoring of their behaviours on Tieba. These commercial actors, driven by their for-profit goals, have a tendency to flood exaggerated or even fake medical information and advertisement into these sub-forums. Therefore, many users of Baidu Tieba accused Baidu of putting profits before the wellbeing of its users, especially of patients, by selling these sub-forums' management and moderation rights.[16]

On this issue, the government response was lenient. Following an online outcry by the public and criticism, the CAC made an announcement criticising misleading and fake information/advertainments on Baidu and summoned Baidu Tieba's responsible managers for a meeting (Xinhua News 2016). Following the meeting, Baidu promised that it would take actions to reform Tieba. On 13 January 2016, Baidu announced that it would stop selling the management and moderation rights of medical forums to commercial parties and that it would transfer control of the hemophilia sub-forum to a non-profit organisation, the Hemophilia Home of China (Ifeng News 2016).

Despite these formal announcements by the government and Baidu, measures taken by the government were one-off and targeted a specific issue. There were no legal steps by the government to avoid the occurrence of similar problems in the future on social media platforms, tragically foreshadowing another health scandal with tragic consequences only one year later.

The Wei Zexi scandal

Although Baidu stopped selling management and moderation rights of forums to commercial companies, fake information and misleading advertisements are still evident on Baidu Search. Given the Baidu search engine's predominant market share in China, it is therefore very likely that users will be affected by fake information and misleading advertisements.

Wei Zexi, a 21-year-old Chinese college student, died in April 2016 after receiving an experimental treatment for a rare form of cancer, synovial sarcoma, at a state military hospital in Beijing. He had learned of the experimental treatment and the hospital from a promoted result on the Baidu search engine. Before his death, he posted an answer to a question, "What do you think is the greatest evil of human nature?" on Zhihu, detailing his experience seeking treatment for his condition.[17] In the post, he accused Baidu of ripping off patients' families and destroying their hope by taking money from hospitals to promote false medical information on its search results. As claimed in his writing, he later found out that the experimental treatment failed clinical trials in the United States and US hospitals had long stopped using this treatment, while Baidu Search allowed the hospital to advertise the failed experimental treatment and exaggerate its treatment effect.

Although the promotion of advertisements paid by commercial companies is a common practice in digital marketing – Google, for example, uses a similar strategy – search results on Baidu were determined almost exclusively by financial considerations rather than by some measures related to accuracy or user interest

in the topic. Baidu sells its listings and rankings to the highest bidder without vetting claims or products (Lv and Luo 2018). A former employee of Baidu revealed: "Our main task is to earn profit for Baidu. We don't have authority or expertise to judge whether the ads are real or not."[18] Similarly, a product manager of Baidu defended Baidu's business practice with words that echo the fragmented nature of online governance in this part of the Chinese internet:

> There are millions of advertisements on Baidu every day, how can we check and verify whether they are genuine or not? We don't even have any rights or power to do so, isn't it? It should be the government's responsibility to do so.[19]

Furthermore, at the time of the Wei Zexi scandal, Baidu did not clearly label sponsored ads or distinguish them from organic, unpaid results.

The government responded to this scandal by initiating a joint investigation led by the CAC, joined by the Ministry of Health and by China's online-advertising regulator, the State Administration for Industry and Commerce.[20] The investigation's report, published in May 2016, concluded that Baidu's pay-for-placement strategy had influenced Wei Zexi's decision to choose the failed experimental treatment. Specifically, the report stated that the pay-for-placement strategy emphasises money over accuracy and there was no clear distinction between promoted results and organic results, affecting the fairness and objectivity of search results and misleading users. The report ordered Baidu to attach "eye-catching markers" and disclaimers to promoted ads, limit the number of promoted ads to no more than 30 percent of each search page, consider quality and reputation in the algorithm of ranking Baidu search results, and establish institutional channels for users to report and log complaints about fake and misleading online content (CAC 2016).

A few months later, in September 2016, a new regulation – The Internet Ad Interim Measures – announced by the State Administration for Industry and Commerce went into effect (State Administration for Industry and Commerce 2016).[21] The regulation clearly stipulated that online ads should be clearly labelled as such and promoted results should be clearly labelled and distinguished from the organic results. There are also stricter rules on health-related ads. Medical products and services need to be vetted by relevant government authorities in charge of advertising before they can be advertised online. The platforms, such as Baidu, are now required to verify the documents proving the authenticity of the products being advertised before they place the ads on the platforms. In other words, online platforms have been given the responsibility for verifying ad content.

In summary, these two health scandals on Baidu vividly demonstrate that in regulating online medical content which falls into non-sensitive areas, conflicting agendas and interests lead to a regulatory vacuum and give rise to exaggerated claims of medical treatments or even fake medical information online, seriously affecting patients' life choices. The responses from the government were lenient. On the one hand, the responsibility of regulating online content – for example, vetting authenticity of the content and qualifications of the advertisers – was

delegated to internet companies. Given that online advertisement accounts for a large share of their profit, it is not in their for-profit nature to enforce this responsibility. On the other hand, the system remains fragmented with conflicting and diverging agendas and interests in the regulation on non-sensitive content, leaving the regulatory vacuum effectively unchanged. Future incidents similar to the two health scandals are likely to recur.

Conclusion

Existing studies of China's internet emphasise the authoritarian nature of the China model and focus on the regime's ability to utilise the internet as a tool of political surveillance and censorship (such as Chase and Mulvenon 2002; King, Pan and Roberts 2013, 2017; Qiu 2000) for political stability and the Party's rule. Our study, however, finds that the centralised authoritarian nature of internet governance in China only applies to sensitive areas – those vital to the political stability and survival of the regime – while in other non-sensitive areas fragmentation persists, such as online health content and online advertising, as the two cases have suggested, resulting in the situation of "Nine dragons run the water".

Furthermore, complementing the existing fragmented authoritarianism framework, which focuses on the scenario whereby fragmentation results in intense bargaining and competition, in our case study we demonstrated that fragmentation can also lead to a regulatory vacuum whereby it is in no authority's mandate and responsibility to act and regulate. In contrast to the regulation of sensitive areas of internet governance of which mandate, expertise, resources, and priority are centralised in the hands of the CAC, the regulation of non-sensitive areas involve the conflict between the Party system's prioritisation of political stability and the State Council's prioritisation of internet-driven development. And there are diverging agendas and conflicting interests among relevant authorities within the two systems. This applies not only to online fake information and misleading ads but also to other non-sensitive areas that fall in between the priorities and mandates of the (potentially) relevant authorities. Such issues include protection of user privacy and the selling of counterfeit products on online e-commerce platforms.

In a comparative perspective, regardless of the nature of the political regime – democratic or authoritarian – China does not differ from Western liberal democratic countries, such as the US or the UK, in their struggle to regulate and manage user-generated content online, especially online advertising (Tusikov 2017). Given the sheer amount of online advertising nowadays and the comparatively limited staffing in governments (see, for example, Mintzes 2016), we believe that governments around the world share similar difficulties in reviewing and verifying all promotional information. The delay between first posting and regulatory action exposes people to this misleading and inaccurate information. This adverse effect of misleading or fake information is particularly serious in the health area as it affects people's health.

Moreover, increasingly, platforms have also become a regulator of online content. Across most popular social media sites, the burden of content moderation

and management is also offloaded by the platforms to their users through the mechanism of user-driven complaints and flagging (Crawford and Gillespie 2014; Gillespie 2010, 2018). In other words, in response to the decentralised nature of content production, content regulation authority is also decentralised to involve not just governments but also platforms and users. Similarly, in the two health scandals in China, government response involves placing the regulatory burden (such as verifying qualifications, vetting content) onto the platform – namely, Baidu in the case study – and the inclusion of user-driven complaints and feedback mechanisms on the platform. Given the financial reliance of many internet companies on revenues from online advertisements, it is not in their for-profit nature to enforce such a regulatory burden, while the system on regulating non-sensitive areas of internet governance remains fragmented, leaving the regulatory vacuum effectively unchanged. There are already signs of similar incidents to the two health scandals recurring in the near future. In 2018, media reports revealed that fake medical advertisements reappeared in Baidu search results but that new techniques were being used to disguise these fake advertisements (Xinhua News 2018). For example, a Baidu search for a specific hospital might show up the name of the hospital but with a link to a different hospital that has paid Baidu for listing. There is not yet any action or response from the government and Baidu on the reappearance of fake advertisements. Despite the importance of content regulation, we have not had any effective form of governance that can curb fake information online.

Finally, as mentioned earlier, the definition of sensitivity is fluid and dynamic and changes over time (Stern and Hassid 2012; Stockmann, Luo and Shen 2020). And the notion of sensitivity is based on judgement calls and perceptions of the Party and the CAC. Health is considered to be a non-sensitive area as long as it does not directly threaten the regime's stability and the Party's rule. The moment that the focus shifts towards government performance involving criticism of the government and strong negative sentiments likely to arouse protests, it becomes sensitive. The Covid-19 pandemic offers a typical example of this dynamic. When discussion on the pandemic can create panic and negative sentiments against the government among the public and is likely to incite protests, it becomes sensitive and there is centralised effort to contain the spread of such messages. For example, the death of a whistleblower Chinese doctor who was detained by police for trying to raise the alarm about Covid-19 in late December led to large-scale censorship of posts mourning his death (Yu 2020).

That said, while issue areas can shift from being non-sensitive to sensitive, political efforts in China nonetheless focus on sensitive areas whereas leaving the governance of non-sensitive areas fragmented. Furthermore, the Chinese government is able to centralise authority, responsibility, and resources and take effective measures on sensitive issues that were once deemed non-sensitive. This reality does suggest that when it comes to understanding internet governance in China, the primary issue is less the capability to regulate and more about the level of importance accorded to a regulatory area by the regime. Certainly, given the shortage of staffing resources vis-à-vis the volume of user-generated content online,

governments have to spend resources in areas they deem important, which in China – as in the West – involves setting priorities, with the criteria determining what is important influenced by the nature of the regime.

Acknowledgements

This research was supported by the project "Authoritarianism in a Global Age" at the University of Amsterdam (www.authoritarianism-global.uva.nl/) and received funding from the European Research Council (Grant No. 323899).

Notes

1 In Chinese, the pronunciation of number nine is similar to the Chinese words "long lasting"; therefore, it is considered as a lucky and special number and is also historically associated with the emperors of China. Dragon is also the symbol of emperor in Chinese culture; hence, nine dragons run the water.
2 The definition of "sensitive" is dynamic and fluid, as noted earlier. Most health issues are not sensitive, as long as the discussion does not focus on challenging government authority and reputation, as the example of the Covid-19 pandemic has demonstrated.
3 Under different leadership, there are different principles – socioeconomic and cultural vision – promoted in the society by the Party. For example, under the Hu Jintao administration from 2002 to 2012, it was the Harmonious Society, and under the current Xi Jinping administration since the end of 2012 it is the Core Socialist Values. Hu's Harmonious Society vision emphasises values bridging gaps in a divided society, while Xi's Core Socialist Values focuses on imposing the state's prescribed values as basis for any consensus.
4 The Ministry of Culture was reformed to create the Ministry of Culture and Tourism in March 2018.
5 Interview with an official of the Ministry of Industry and Information Technology, October 2015, Beijing.
6 In 2013, it was reformed to create a new ministry, the National Health and Family Planning Commission. Since March 2018, it has been renamed the National Health Commission. On what the commission does, please refer to http://en.nhc.gov.cn/about.html, retrieved 3 January 2020.
7 On what the bureau does, refer to www.gov.cn/fuwu/2014-02/22/content_2618761.htm, retrieved 3 January 2020. In 2018, as part of an ongoing institutional reform, the functions of State Administration for Industry and Commerce have been assumed by the State Administration for Market Regulation.
8 Before 2014, those content-regulating authorities which would have a mandate on regulating online medical content included, within the party system, the Publicity Department and, within the State Council system, the Ministry of Culture at the ministry level and the State Council Information Office/International Communication Office at the bureau level.
9 StatCounter GlobalStats, https://gs.statcounter.com/search-engine-market-share/all/china/2016, retrieved 23 September 2019. Here, we focus on the figures in 2016, because the two health scandals happened in 2016 which had dramatic impacts on Baidu's business strategy and practices after 2016.
10 Interview with a Baidu Tieba senior product manager, April 2015.
11 Interview with a Baidu Tieba senior product manager, April 2015.
12 Interview with a Baidu Tieba senior product manager, April 2015.
13 The original post can be found on: www.zhihu.com/question/39322261/answer/80899690, retrieved 4 January 2020.

14 More information on how to become or remove a sub-forum moderator can be found here: eba.baidu.com/helpcenter/index#/questions/forum-manager/manager/qa6, retrieved 17 June 2020.
15 Interview with a Baidu Tieba senior product manager, April 2015.
16 On Zhihu, there was a heated discussion on Baidu's sale of Tieba management rights. Please refer to www.zhihu.com/question/39322261/answer/80899690, retrieved 4 January 2020.
17 The original post by Wei Zexi can be found on: www.zhihu.com/question/26792975/answer/88170767, retrieved 4 January 2020.
18 Interview with a former employee of Baidu, June 2017.
19 Interview with a product manager of Baidu, May 2017.
20 A separate investigation on the military hospital was conducted by Ministry of Health and relevant authorities from the military, as the case also concerns the privatisation of military hospitals, which is beyond the scope of this chapter.
21 The Chinese version of the regulation can be assessed at www.cac.gov.cn/2016-07/08/c_1119187555.htm, and the English version can be assessed at http://en.pkulaw.cn/display.aspx?cgid=b5634342d689e699bdfb&lib=law, retrieved 5 January 2020.

Legislation

Standing Committee of the National People's Congress. 2016. *Zhonghua renmin gongheguo wangluo anquanfa [Cybersecurity Law of the People's Republic of China]*. 11 July, Beijing.
Standing Committee of the National People's Congress. 2018. *Zhonghua renmin gongheguo dianzi shangwufa [E-Commerce Law of the People's Republic of China]*. 31 August. Beijing.

References

Bai, Ge. 2016. "Baidu Behind Baidu's Selling Haemophilia Forum: Disease Forums Are Controlled by For-Profit Institutions." *NetEase*. 13 January. http://money.163.com/16/0113/15/BD7H6F2600253B0H.html. Accessed 5 August 2020.
Bandurski, David. 2008. "China's Guerilla War for the Web." *Far Eastern Economic Review* 171 (6): 41–44.
Birney, Mayling. 2014. "Decentralization and Veiled Corruption under China's 'Rule of Mandates.'" *World Development* 53: 55–67.
CAC. 2016. "Guojia wangxinban lianhe diaochazu gongbu jinzhu baidu diaocha jieguo [The Joint Investigation Team of the CAC Announced the Results of the Investigation into Baidu]". *Cyberspace Administration of China*. 9 May. www.cac.gov.cn/2016-05/09/c_1118833529.htm. Accessed 5 August 2020.
Castells, Manuel. 2015. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge: John Wiley & Sons.
Chase, Michael S., and James C. Mulvenon. 2002. *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*. Santa Monica, CA: Rand Corporation.
CNNIC. 2009. "Zhongguo Hulianwang Fazhan Zhuangkuang Tongji Baogao [The 23rd Statistic Report on the Development of China's Internet]." *China Internet Network Information Center*. Beijing.
CNNIC. 2018. "Zhongguo Hulianwang Fazhan Zhuangkuang Tongji Baogao [The 42nd Statistic Report on the Development of China's Internet]." *China Internet Network Information Center*. Beijing.
Crawford, Kate, and Tarleton Gillespie. 2014. "What Is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint." *New Media & Society* 18 (3): 410–428. https://doi.org/10.1177/1461444814543163.

Creemers, Rogier. 2017. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century." *Journal of Contemporary China* 26 (103): 85–100. https://doi.org/10.1080/10670564.2016.1206281.

Deng, Jinting, and Pinxin Liu. 2017. "Consultative Authoritarianism: The Drafting of China's Internet." *Journal of Contemporary China* 26 (107): 679–695.

Ding, Huang, and Wen Sun. 2014. "Cong Xinzheng Jianguan dao Shehui Gongzhi: Shiping Anquan Jianguan de Tizhi Tupo – Jiyu Wangluo Fenxi de Shijiao [From Administrative Regulation to Joint Social Governance: Institutional Breakthrough in Food Safety Regulation – Based on Network Analysis]." *Jiangsu Xinzheng Xueyuan Xuebao* [*The Journal of Jiangsu Administration Institute*] 1: 109–115.

Fan, Yiying. 2016. "Baidu Tieba Hemophilia Scandal Drags on in Libel Case." *Sixth Tone*. 11 August. www.sixthtone.com/news/1179/baidu-tieba-hemophilia-scandal-drags-libel-court-case. Accessed 5 August 2020.

Fang, Xingdong. 2016. "Zhongguo Hulianwang Zhili Moshi de Yanjin yu Chuangxin – Jianlun 'Jiulong Zhishui' Moshi Zuowei Hulianwang Zhili Zhidu de Zhongyao Yiyi [On the Evolution and Innovation of the Chinese Internet Governance Model]." *Renmin Luntan Xueshu Qianyan* [*Frontiers*] 6: 56–75.

Feng, Jiayun. 2016. "Baidu Gives Up on Commercializing Tieba Forums." *Sixth Tone*. 28 July. www.sixthtone.com/news/1124/baidu-gives-up-on-commercializing-tieba-forums/. Accessed 5 August 2020.

Gallagher, Mary, and Blake Miller. 2017. "Can the Chinese Government Really Control the Internet? We Found Cracks in the Great Firewall." *Monkey Cage – The Washington Post (blog)*. 21 February. www.washingtonpost.com/news/monkey-cage/wp/2017/02/21/can-the-chinese-government-really-control-the-internet-we-found-cracks-in-the-great-firewall/. Accessed 5 August 2020.

Gillespie, Tarleton. 2010. "The Politics of 'Platforms'." *New Media and Society* 12 (3): 347–364. https://doi.org/10.1177/1461444809342738.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press.

Han, Rongbin. 2015. "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army'." *Journal of Current Chinese Affairs* 44 (2): 105–134.

Huang, Zheping. 2016. "Baidu, China's Version of Google, is 'Evil', a Growing Number of Users Say." *Quartz*. 2 May. https://qz.com/674030/baidu-chinas-version-of-google-is-evil-a-growing-number-of-users-say/. Accessed 5 August 2020.

Ifeng News. 2016. "Baidu huiying chumai xueyoubing ba [Baidu's Response on Selling Haemophilia Forum]." *Chinanews*. 12 January. http://news.ifeng.com/a/20160112/47037078_0.shtml. Accessed 5 August 2020.

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." In *American Political Science Review*. Cambridge University Press, 107 (2): 326–343. https://doi.org/10.1017/S0003055413000014.

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111 (3): 484–501. https://doi.org/10.1017/S0003055417000144.

Lee, Ming-Hsuan, and Mon-Chi Lio. 2016. "The Impact of Information and Communication Technology on Public Governance and Corruption in China". *Information Development* 32 (2): 127–141. https://doi.org/10.1177%2F0266666914529293.

Lei, Ya-wen. 2011. "The Political Consequences of the Rise of the Internet : Political Beliefs and Practices of Chinese Netizens." *Political Communication* 28 (3): 291–322. https://doi.org/10.1080/10584609.2011.572449.

Lieberthal, Kenneth, and Michel Oksenberg. 1988. *Policy Making in China: Leaders, Structures, and Processes*. Princeton, NJ: Princeton University Press.

Luo, Ting. 2014. *Village Economic Autonomy and Authoritarian Control over Village Elections in China: Evidence from Rural Guangdong Province*. PhD Thesis. The London School of Economics and Political Science (LSE).

Lv, Aofei. 2015. *Explaining Health Policy Change in China between 2003 and 2009: Actors, Contexts and Institutionalisation*. PhD Thesis. University of Glasgow.

Lv, Aofei, and Ting Luo. 2018. "Asymmetrical Power Between Internet Giants and Users in China." *International Journal of Communication* 12: 3877–3895.

MacKinnon, Rebecca. 2009. "China's Censorship 2.0: How Companies Censor Bloggers." *First Monday* 14 (2). https://firstmonday.org/ojs/index.php/fm/article/download/2378/2089. Accessed 7 August 2020.

Macron, Emmanuel. 2018. "IGF 2018 Speech by French President Emmanuel Macron." *Internet Governance Forum*. November. www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron. Accessed 27 September 2019.

Meng, Qian. 2016. "Baidu xueyoubing ba beimai Shijian shimo [Baidu Hemophilia Forum Was Sold]." *Tencent Technews*. 12 January. https://tech.qq.com/a/20160112/052408.htm. Accessed 5 August 2020.

Mertha, Andrew. 2009. "Fragmented Authoritarianism 2.0: Political Pluralization in the Chinese Policy Process." *The China Quarterly* 200: 995–1012.

Miller, Blake. 2016. *Automated Detection of Chinese Government Astroturfers Using Network and Social Metadata*. https://dx.doi.org/10.2139/ssrn.2738325.

Mintzes, Barbara. 2016. "The Tip of the Iceberg of Misleading Online Advertising Comment on 'Trouble Spots in Online Direct-to-Consumer Prescription Drug Promotion: A Content Analysis of FDA Warning Letters'." *International Journal of Health Policy and Management* 5 (5): 329–331. https://doi.org/10.15171/ijhpm.2016.19.

Murphy, Zoe. 2011. "China Struggles to Censor Train Crash Coverage." *BBC News*. 28 July. www.bbc.co.uk/news/world-asia-pacific-14321787. Accessed 10 January 2020.

NetEase. 2016. "Baidu huiying xueyoubing ba shijian: yi zhuoshou diaocha [Baidu Is Investigating Selling Hemophilia Forum]." *NetEase*. 11 January. http://tech.163.com/16/0111/13/BD27EV5K000915BF.html. Accessed 5 August 2020.

Newhagen, John E. 1998. "Hitting the Agenda Reset Button: Matching Internet Research with Development." *Convergence* 4 (4): 112–119. https://doi.org/10.1177%2F135485659800400410.

Qiu, Jack Linchuan. 2000. "Virtual Censorship in China: Keeping the Gate Between the Cybersapces." *International Journal of Communications Law and Policy* 4: 1–25.

Ruan, Lotus, Jeffrey Knockel, and Masashi Crete-Nishihata. 2020. "Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media." *Citizen Lab Research Report No. 125*. March. https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/. Accessed 5 August 2020.

Securities Daily. 2016. "Baidu tieba yeman shangyehua, yunyingquan sanwanyuan qishou [Baidu Tieba's Barbaric Commercial Operation]." *Tencentnews*. 13 January. https://tech.qq.com/a/20160113/024230.htm. Accessed 24 September 2019.

Shirk, Susan L. 2007. *China: Fragile Superpower*. Oxford: Oxford University Press.

Shi Xuehua, and Fafeng Sun. 2008. "Zhengfu 'Dabuzhi' Mianmianguan [On Preventing Negative Effects of 'Super Ministry']." *Zhongguo Xinzheng Guanli [Chinese Public Administration]* 3: 29–32.

State Administration for Industry and Commerce. 2016. "Hulianwang guanggao zanxing guanli banfa [Interim Measures for the Administration of Internet Advertising]." 4 July. www.cac.gov.cn/2016-07/08/c_1119187555.htm. Accessed 5 August 2020.

State Council. 2014. "Guowuyuan guanyu shouquan wangxinban neirong guanli gongzuode tongzhi [Notice on Authorizing the Cyberspace Administration of China to Be in Charge of Content Regulation on Cyberspace]." www.gov.cn/zhengce/content/2014-08/28/content_9056.htm. Accessed 5 August 2020.

State Council. 2015. Guowuyuan guanyu jiji tuijin 'hualianwang+' xingdongde zhidao yijian [Guiding Opinions of the State Council on Actively Promoting the 'Internet +' Action].

Stern, Richard E., and Jonathan Hassid. 2012. "Amplifying Silence: Uncertainty and Control Parables in Contemporary China." *Comparative Political Studies* 45 (10): 1230–1254. https://doi.org/10.1177/0010414011434295.

Stockmann, Daniela, and Ting Luo. 2017. "Which Social Media Facilitate Online Public Opinion in China?" *Problems of Post-Communism* 64 (3–4): 1–14.

Stockmann, Daniela, Ting Luo, and Mingming Shen. 2020. "Designing Authoritarian Deliberation: How Social Media Platforms Influence Political Talk in China." *Democratization* 27 (2): 243–264. https://doi.org/10.1080/13510347.2019.1679771.

Tusikov, Natasha. 2017. *Chokepoints: Global Private Regulation on the Internet*. Berkeley, CA: University of California Press.

Xinhua News. 2014. "Zhongyang wangluo anquan he xinxihua lingdao xiaozu chengli [Central Leading Group for Cybersecurity and Informatization Was Established]." *Chinanews*. 27 February. www.chinanews.com/gn/2014/02-27/5892579.shtml. Accessed 5 August 2020.

Xinhua News. 2016. "Guojia wangxinban yuetan Baidu gongsi fuzeren, Baidu jiu xueyoubingba shijian zaici shengming [The CAC Summoned Baidu Representatives, Baidu Once Again Declared on the 'Haemophilia' Incident]." *Xinhua News*. 16 January. www.gov.cn/xinwen/2016-01/16/content_5033431.htm. Accessed 5 August 2020.

Xinhua News. 2018. "Yiliao jingjia guanggao juantu chonglai [The Return of Medical Bidding Ads]." *Tencentnews*. 10 May. https://finance.qq.com/a/20180510/006547.htm.

Yu, Verna. 2020. "'Hero Who Told the Truth': Chinese Rage over Coronavirus Death of Whistleblower Doctor." *The Guardian*. 7 Febuary. www.theguardian.com/global-development/2020/feb/07/coronavirus-chinese-rage-death-whistleblower-doctor-liwenliang. Accessed 5 August 2020.

Zhang, Lei, Eric Pul Fung Chow, Jun Zhang, Jun Jing, and David P. Wilson. 2012. "Describing the Chinese HIV Surveillance System and the Influences of Political Structures and Social Stigma." *The Open AIDS Journal* 6: 163–168. https://doi.org/10.2174/1874613601206010163.

Zheng, Yongnian. 2007. *Technological Empowerment: The Internet, State, and Society in China*. Redwood City, CA: Stanford University Press.

Zhu, Xufeng. 2008. "Strategy of Chinese Policy Entrepreneurs in the Third Sector: Challenges of 'Technical Infeasibility'." *Policy Sciences* 41 (4): 315–334. https://doi.org/10.1007/s11077-008-9070-2.

7 Russia

An independent and sovereign internet?

Ilona Stadnik

That the internet might fracture along state lines has become a significant topic of academic and political concern (Hill 2012; Fehlinger 2014; Mueller 2017). This concern stems from a number of reasons, including worries about the fragmentation of information space, away from the promise of a universal information commons, and the disintegration of the global internet into fragmented corporate or national networks. Politically, we see a trend of greater state involvement in internet governance issues, such as cybersecurity, content regulation, and data governance. Phrases such as "cyber sovereignty," "information sovereignty," "digital sovereignty," and "nationalisation of internet governance" are associated with a proposed and, in some places, ongoing process of internet fragmentation.

While these trends are usually associated with authoritarian countries, many non-authoritarian states also seek greater control of the internet and look for ways to apply sovereignty to digital space (Macron 2018; Merkel 2019). From this perspective, the catchy term "sovereignisation" refers to various practices of state authorities in internet governance, independent of whether that state is authoritarian or democratic. These practices can include expansive filtering and blocking of unwanted websites and services, localisation of data, and even the insulation of a domestic network's physical infrastructure from the global internet.

Nevertheless, when it comes to exerting sovereign authority over the internet, non-democratic states tend to be leading the way, and Russia is one of the most prominent examples. As such, the Russian case can reveal much about the possibilities, limitations, and consequences of increased sovereignisation. Russia stands out due to its rapid implementation of stricter internet regulation. The Russian case is also particularly interesting because the government has gone beyond an interest in regulating data and content and expressed ambitions to make its national segment of the internet independent of the global internet, while also preserving connectivity to the world network. A study of Russian policy may thus shed light on possible future directions of internet governance more generally, particularly in relation to greater state involvement. This chapter also contributes to the currently very limited English-language literature on Russian governance of the internet at a time when greater transcultural understanding is sorely needed.

This chapter examines how the Russian government is gradually (and often with difficulty) implementing various initiatives to assert sovereignty over the

DOI: 10.4324/9781003008309-10

"Runet" (a name applied, somewhat loosely, to the internet in Russia). The aim of the government is twofold: to make Runet more centralised and more detached from the global network and to compel foreign technology companies to follow Russian regulations regarding the internet. The chapter discusses the details of these initiatives, their feasibility, and the consequences that may follow. We categorise the various Russian measures according to the three facets of cyberspace alignment theory: the national securitisation of cyberspace; the territorialisation of information flows; and efforts to structure control of critical internet resources in line with national borders (Mueller 2017).

Overall, this chapter argues that Russia's actions with respect to internet governance are best understood as what Mueller calls the alignment of cyberspace to national borders, albeit with important limitations. Many complications hinder the creation of an independent and sovereign Runet, for example, the high external connectivity of Russian networks, the lack of nationally produced equipment, and inconsistent regulation of network operators. In addition, there are contradictory goals of trying to centralise the management of Runet while making it more stable and resilient. Although the Russian government declares the aim to create its own resolver in the domain name system (DNS) for its national domains (i.e., .ru, .рф, .su), in practice the authorities focus more on controlling content rather than controlling the routing of traffic. Then there are problems with compelling foreign information technology giants to comply with Russian laws. Russian businesses and ordinary users continue to use many foreign platforms and services. Realising the possible catastrophic consequences of cutting Russia off of the global internet, the government is constrained to hold back from its declared aspiration to gain full sovereignty over Runet.

The body of this chapter is organised into six parts. The first part discusses key terms in Russian discourse about internet governance, including cyber sovereignty, information sovereignty, digital sovereignty, and internet fragmentation. The second, third, and fourth sections review policy measures of Russian internet governance under the headings of securitisation, territorialisation, and control of critical internet resources. The fifth part summarises the main outcomes of Russian policies to date and considers their implications for wider global internet governance. The sixth, concluding, part offers some final observations about the tensions between political ambitions and technical practicalities in Russian state regulation of the internet.

Making sense of "internet sovereignty"

Before proceeding to describe and assess the range of Russian regulatory measures regarding the internet, it is important to clarify certain concepts that figure prominently in the discourse. Notions of "internet sovereignty" and "information sovereignty" (also widely circulating in China) are particularly significant signposts in Russian internet policy. After discussing these concepts, this section lays out a threefold framework to guide the review of Russian efforts to achieve "sovereignty" over the internet. Adapted from Mueller (2017), this framework highlights trends

of securitisation, territorialisation of information flows, and national regulation of internet names and numbers.

Understanding Russia's approach to internet governance as it relates to sovereignty must begin on the confusing terrain of language itself. Literature addressing the influence on state sovereignty of both global communications technology in general and the internet in particular dates from the 1990s (Barlow 1996; Giacomello 2005; Giacomello and Mendez 2001; Johnson and Post 1996). However, as the following paragraphs elaborate, the field truly expanded after 2013, mostly due to Edward Snowden's revelations of the US National Security Agency's capabilities to conduct surveillance on an unprecedented scale (Greenwald 2014).

The term internet sovereignty is usually associated in the first place with China (Information Office 2010; Jinping 2015). However, although the term is widely used, especially regarding Chinese and Russian approaches to internet governance (Giles and Hagstead 2013), internet sovereignty lacks a clear definition. The problem lies partly with language, particularly the absence of close Chinese analogues to English words. A consensus definition is also complicated by the lack of common definitions for "cyberspace" and "information space" as being loosely interchangeable with the internet. As a result, different terms are often used to describe similar ideas: "internet sovereignty," "information sovereignty," and "network frontiers" (Zeng, Stevens and Chen 2017).

In China, according to Yang (2012), information sovereignty refers to a state's right to control transboundary flows of information, to adjudicate over disputes arising in this context, and to share information based on intergovernmental agreements. Du and Nan (2014) extend the notion of internet sovereignty to include control over platforms that produce, transmit, and share digital information. Finally, Chinese media have described "cyber sovereignty" as a way that China may improve global internet governance and be a responsible "cyber power" (BJNews 2019), in line with a more general Chinese policy to behave like a responsible superpower in international politics. According to Chinese scholars, cyber sovereignty does not imply the fragmentation of the internet into isolated sovereign jurisdictions. Rather, it implies that independent states should coordinate their policies and establish an international legal regime to maintain order in cyberspace and to enshrine the sovereign right of each state to define internet policy inside the country. From this perspective, it is natural for a state to extend sovereignty to the digital domain, justifying such a move on grounds of national security.

Turning to Russia, a growing body of theoretical works addresses the concept of information sovereignty. Polikarpov, Polikarpova, and Polikarpova (2014) define information sovereignty through the analysis of threats coming from information and communication technologies (ICTs) and ways to address them to maintain the sovereignty of a state in the information space. Vinnik (2014) considers information sovereignty in relation to political and legal regimes of internet traffic filtration. Efremov (2017) argues that, given the globalisation of the information space, the priority area for affirming state sovereignty is the formation of an international legal regime based on the principle of sovereign equality of all states.

Kucheryavyiy (2015) proposes a more extensive theory, arguing that information sovereignty involves the supremacy and independence of state authority in the formation and implementation of information policies in the national segment as well as the global information space. Information sovereignty for Kucheryaviy includes three components. The first, "digital-technical" sovereignty, covers national technological production cycles of software and hardware platforms, search and navigation systems, network and information protection equipment, the national segment of internet and social networks, and national payment systems. The second component, "mental-psychological" sovereignty, includes a high level of "information culture of society": with consumption of "appropriate" content and avoidance of "fake" content. The third component, "information-power" sovereignty, covers pro-government elites and mass media as well as the state's information policy.

To summarise, both Chinese and Russian discussions of sovereignty as it relates to the internet emphasise state supremacy in information policy, state regulation of information flows and digital platforms, as well as a priority to establish an international legal regime based on the principle of states' equality in cyberspace. In contrast to Chinese views, however, Russian conceptions of information sovereignty highlight the possible malevolent nature of information, such as extremist content and fake news about state policies.

Chinese and Russian narratives contrast interestingly with Western discourse about sovereignty and the internet. For example, one popular Western view sees cyberspace as a new military domain and applies the notion of territorial sovereignty to cyber operations below the threshold of armed conflict (Schmitt 2013, 2017). Another Western point of view holds that, without sovereign authority, there is no law and order in cyberspace either domestically or internationally (Demchak and Dombrowsky 2011; Franzese 2009). Thus, these Western understandings tend to link internet sovereignty to questions about international conflict and the necessity to establish and follow the rules of the game, which is the responsibility of states.

Mueller (2019), meanwhile, argues that non-democratic countries are concerned about "interdependence sovereignty" – the ability to control the flow of ideas, people, and goods across borders – in cyberspace. Mueller borrows this term from the four types of sovereignty defined by Krasner (1999).[1] It means that cross-border flows of ideas, people, and goods degrade state sovereignty. Appeals to cyberspace sovereignty seek to shield states from interference in internal affairs or political and social disruption caused by information from external adversaries entering the country through cyberspace.

Mueller (2017) argues that, instead of technical fragmentation of the internet, sovereignty relates to attempts to align the control of cyberspace with national borders while preserving the economic and infrastructural benefits of using the global network. He suggests a threefold framework to achieve such an alignment. Adapting Mueller's framework to this chapter, we will highlight what Russia is doing towards enacting greater state control over the internet and other ICT-related issues within its borders.

The first element is national securitisation of cyberspace. Mueller explains securitisation in cyberspace as a process of reframing cybersecurity as a national

security issue, together with the recognition of cyberspace as a military domain. Securitisation means that "societal dependencies on information technologies and networks create vulnerabilities that could pose an existential threat to the state itself" (Mueller 2017, 37). Securitisation also includes the militarisation of cyberspace through the creation of dedicated cyber troops, nationalisation of cyber threat intelligence, reliance on national internet standards and information technologies, and legal authority for kill switches to shut down the internet.[2]

The second element of national alignment of the internet involves territorialisation of information flows. All states regulate flows of information within their borders through the control of telecoms and internet infrastructure (autonomous system numbers and internet exchange points) (Winseck 2019). However, with information sovereignty states seek to control not only the infrastructure but also the content that flows through it, with measures such as filtering, data localisation, and geo-blocking.

The third element of national alignment is the most intriguing in terms of technical feasibility, namely, efforts to structure control of critical internet resources along national lines. Mueller explains it as a partition of the global domain name and Internet Protocol (IP) address spaces along national lines in order to provide nation-states with greater leverage over the governance of the internet in their territory. On these lines, the Chinese state has proposed to break up the existing global DNS into national jurisdictions controlling top-level domains.

Mueller's framework of cyberspace alignment helps to clarify what is happening with internet governance in Russia. Next, we discuss in turn the three elements of securitisation, territorialisation, and national IP/DNS control, looking in each case at the Russian government's policies, the feasibility of their implementation, and potential consequences of those initiatives.

Securitisation of the internet in Russia

The term "cybersecurity" is not common in Russian policymaking and legislation; instead, the phrase "information security" is normally used. This difference highlights the lens through which the Russian state tends to see issues of internet governance and sovereignty.

Securitisation of the digital sphere in Russia began with the 2000 Doctrine on Information Security, which fixed the information sovereignty discourse and defined the main vectors of Russian domestic and foreign policy in this field. Securitisation of the internet in Russia intensified further with the 2016 update of the Doctrine on Information Security. The New Doctrine of 2016 is a strategic planning document in the field of national security of Russia and develops in more detail the general provisions of the National Security Strategy of Russia published in 2015.

According to the 2016 Doctrine, the concept of information security refers to the:

> station of security of *an individual*, *the society* and *the state* from internal and external information threats at which are provided: implementation of the

> constitutional rights and freedoms of an individual and the citizen; good quality of living for citizens; sovereignty, territorial integrity and sustainable social and economic development of the Russian Federation; defense and security of the state.
>
> (Doctrine on Information Security of Russia 2016, Part I, art. 2, emphasis added)

As this passage indicates, information security in Russia is based on a triad of individual, society, and state. Russian national interests in the information field relate to ensuring "objectively significant needs of *the individual, the society and the state* in ensuring their security and sustainable development in the area of information" (Doctrine on Information Security of Russia 2016, Part I, art. 2, emphasis added). More specifically, national interests include a number of responsibilities of the state and other actors, divided into five areas of content security, cybersecurity of information infrastructure, the advancement of technological potential, international information security based on the principle of state sovereignty, and "reliable" presentation of Russian Federation policies to domestic and international audiences (Doctrine on Information Security of Russia 2016, Part II, art. 8). Thus, we see the triad is linked to different issues, and it figures as well in the section of the Doctrine about threats to information security. These threats are identified to include unlawful cross-border content flows; exposure of national critical infrastructure to attacks; use of ICT to influence the psychology of the population and to destabilise the political system; dependency on foreign ICT hardware and software; and improper distribution and control over critical internet resources. Hence, we see that the Doctrine regards IT and networks as major potential threats to the state and its sovereignty.

Militarisation

The creation of military "Cyber Commands" is also a part of national securitisation of the internet, because it is how states develop capabilities to engage in cyber conflict and defend themselves. The militarisation of cyberspace is also happening in Russia, although it was not officially acknowledged until 2017, when the current Minister of Defense mentioned information troops as a separate division in the Army. Details about this new division are classified, but the media signals that its purpose is to repel cyberattacks on the Russian military networks and to "expose foreign sabotage in electronic, paper and television media" (Interfax 2017).

Interestingly, the militarisation of cyberspace runs against the Russian government position at the international level. In the United Nations General Assembly, the UN Group of Governmental Experts (GGE), and the Open-Ended Working Group (OEWG) of the UN Office for Disarmament Affairs, Russia has opposed cyberconflict and promoted the idea of peaceful use of ICT and responsible state behaviour. In 2011, before the first mentions in the press of "scientific troops" with ICT specialists in the Army (RIA 2012), the Russian Ministry of Defense issued a

framework document entitled "Conceptual Views on the Activity of the Russian Armed Forces in the Information Space" (Ministry of Defense 2011). It stated that the armed forces should adhere to "deterrence and prevention of conflicts in the information environment, conduct conflict resolution if it occurred through negotiations, reconciliation, appeal to the UN Security Council or to regional bodies or agreements, or other peaceful means."

However, the document also asserts that, in the case of escalation of a conflict in the information space and its transition to the crisis phase, the armed forces would "use the right to individual or collective self-defense using any chosen methods and means that do not contradict the universally recognised norms and principles of international law." Thus, despite the government's clear opposition to militarisation of cyberspace on the international level and critique of other states who openly declare their offensive cyber capacities, Russia prefers to develop its own capacities in this area covertly.

Nationalisation and centralisation of threat intelligence

Another aspect of internet securitisation is nationalisation and centralisation of threat intelligence reporting and sharing capabilities, together with the development of national computer emergency response teams (CERTs). In January 2013, President Putin signed a directive to create GOSSOPKA (State System of Detection, Prevention and Elimination of Consequences of Computer Attacks on Information Resources) under the supervision of the Federal Security Service (known as FSB) (Decree No. 31 2013). The purpose was to create a system of information sharing between the most significant organisations and entities in the country regarding ongoing cyberattacks and thus to develop preventive capabilities. It is a good example of the centralisation of threat intelligence reporting. In 2017, the FSB initiated a law on critical information infrastructure, 187-FZ, that defines significant infrastructure objects and requirements to ensure their cybersecurity. This law also integrates GOSSOPKA more tightly into the state, making it a centre of official competences (Federal Law 187-FZ 2017).

The centralisation of threat intelligence in Russia was completed in July 2018 with the creation by the FSB of the National Coordination Centre for Computer Incidents (NCCCI). This new body absorbed the functions of GOV-CERT. A special order regulates the way that Russian agencies concerned with critical information infrastructure can exchange information about computer incidents between each other and with foreign CERTs (Order No. 52107 2018). The powers of the NCCCI are significant. All international incident response interactions must go only through this body (except where special cooperation agreements exist, though even then the NCCCI must be notified). Moreover, the NCCCI can refuse to share information about incidents with foreign counterparts if such information is deemed to threaten the national security of Russia.

Thus, the introduction of laws and orders between 2013 and 2018 added major institutional arrangements to ensure information security in Russia. Now the government has developed more unified and centralised control of cyber threat

intelligence for critical national infrastructure as well as international cooperation around these matters. That said, Law 187-FZ is not yet fully implemented, since there are still some omissions regarding, for example, the categorisation of critical infrastructure objects. Finally, private CERTs continue to exist for certain sectors like the CERT of Group-IB (CERT-GIB), the Kaspersky Industrial Control Systems CERT, smaller SOCs (Security Operations Centers), and FinCERT at the Bank of Russia. These CERTs currently remain more active than the NCCCI, which is just beginning to gain power (Stadnik 2019b).

Nationally Produced Technologies

Another area of greater Russian state involvement in internet governance is reliance on nationally produced technologies to substitute for the importation of foreign software and applications. Import substitution has been a buzzword for the Russian government since 2014, after events in Ukraine and Crimea triggered a cascade of economic sanctions against Russia (Moniz Bandeira 2019). This situation spurred debates about Russia's high dependence on foreign software and hardware, especially for government needs. Another prompting for import substitution in the IT sector was the Snowden revelations in 2013, which showed the US National Security Agency's ability to use vulnerabilities and back doors in software and devices for surveillance purposes. The problem of technological dependence is also reflected in the 2016 Doctrine on Information Security.

After a long discussion with the internet industry, the Russian government in 2015 issued Decree No. 1236, "On the Establishment of a Ban on the Admission of Software Originating from Foreign Countries for the Purposes of Procurement for State and Municipal Needs." The decree established a registry of Russian-made software that now comprises more than 5000 items, covering operating systems, cloud storage, office software, and database toolkits.[3] The government assumed that import substitution in IT should cover not only the public sector but also ordinary users.

However, in practice state agencies still have licenses for foreign software, and domestic analogues are very inconvenient to use. Another limitation is that "Russian" software in many cases is not completely Russian: The registry has an owner category, "Russian commercial organisation with foreign persons in the chain of ownership." This provision shows how difficult it is to develop software from scratch without international collaboration. Importantly, no one in Russia is talking about the development of national standards for internet protocols, because it would be inexpedient to withdraw from the benefits of using the global network.

In 2019, a new trend appeared in the legislative domain: a veiled attempt to nationalise publicly significant Russian internet services through a reduction of foreign ownership. Russia has domestic equivalents of Google, Facebook, Amazon, and other platforms, although these substitutes generally have less popularity among Russian users. However, the Russian government has started to think of limiting to 20 percent the foreign ownership of information resources that are important for the domestic information infrastructure (Forbes 2019). While

industry players argue that such a policy would kill foreign investments in domestic companies, the state is concerned about the issue of future control over companies and services that are important to Russian citizens. Still, the feasibility of this initiative is questionable, since there is no common understanding of what these socially significant information resources are and how they should be selected.

Network kill switches

A final point regarding securitisation concerns legal authority for network kill switches. The Russian government is concerned with external threats to internet operations in Russia, including shutdowns of the Runet by hostile states. The Russian government admits that the creation of a national kill switch for the internet in the country is a radical measure that, if used, would harm the national economy and disrupt daily operations in various sectors. Nevertheless, there are documented cases of local shutdowns of mobile internet during political protests, for example, in the Republic of Ingushetia in 2018 and in Moscow in 2019.

Ambitions to create a "Sovereign Runet" date back many years. During the period 2013 to 2016, the Russian government actively criticised the Internet Corporation for Assigned Names and Numbers (ICANN) for its global governance of the DNS and the allocation of IP addresses. The Kremlin called for internationalisation and transfer of ICANN functions to the intergovernmental International Telecommunication Union (ITU), opposing the then-ongoing transition of oversight for the Internet Assigned Numbers Authority (IANA) to ICANN (Cavalli and Scholte, this volume; Becker 2019). However, Russia was in the minority position, as most other states backed the handover to ICANN.

Meanwhile in 2014, the Russian Ministry of Communications (MoC), at the request of the president, conducted special cyber drills. The officially declared aim was to "assess the security and stability of the national segment of the network, the degree of its connection with the global Internet infrastructure." The drills were supposed to "assess potential vulnerabilities, determine the level of readiness for joint work of industry, operators and situational centres of the federal executive authorities in case of negative targeted impact" (Ministry of Communications 2014). Apparently, the MoC tested the probability of a complete internet shutdown orchestrated from outside the country. As a result of these drills, the government decided that it needed to create its own backup DNS servers and IP address databases. Then, in case any problems should arise for Russia in reaching the DNS root zone and the databases of RIPE NCC (the European regional Internet registry), internet service providers (ISPs) in Russia would have alternative sources to continue Runet operations.

In 2016, the MoC introduced a first bill that aimed to protect Runet from an externally generated shutdown. The bill stalled, especially because it overlapped with some provisions of the Law 187-FZ described earlier. Two years later, the Russian government initiated another law to protect Runet from the intervention of foreign states (referring to the latest cybersecurity strategy of the United States). However, combating the "external threats" would involve the same kill switch

technologies as the Russian government would use in local shutdowns: namely, interference into traffic routing and attempts to impose a centralised control point for networks' management and monitoring. So, the issue of protection from foreign interference into Runet was not really addressed until further measures in May 2019, as discussed later.

Territorialisation of the internet in Russia

Russia has a comprehensive mix of content filtering, data localisation, and geoblocking. However, the regime is not as extensive as the Golden Shield that operates in China (Walton 2001). To the contrary, the Russian government has pursued a gradual process of territorialising data and information, as well as creating laws to regulate the blocking of websites with unlawful content and the filtering of search engine results. Interestingly, as elaborated later, new regulations appeared in 2019 that switch strategy towards large foreign internet companies such as Facebook, Twitter, and Google. Instead of blocking these services, the Russian government now fines them for noncompliance with its laws.

Content filtering

Content filtering started in Russia in 2012 after the adoption of Federal Law 139-FZ, which established a special registry (the Blacklist) of websites containing information prohibited by federal laws. Content banned under 139-FZ includes child pornography, as well as the promotion of suicide and illicit drug use. In 2013, Federal Law 398-FZ expanded the prohibited content to cover calls for mass riots, extremist activities, and participation in certain mass public events. Finally, Federal Law 187-FZ of 2013, called the Anti-Piracy Act, allows government authorities to block sites that contain copyrighted content at the request of the rights owner.

The Blacklist is run by Roskomnadzor, a federal supervisory body in the field of telecommunications, information technology, and mass media. Web resources are added to the registry after a court decision or when other federal executive agencies request Roskomnadzor to block web resources, also without a court decision. In 2015, Roskomnadzor started to elaborate a hardware-software complex called "Revizor" that checks whether ISPs are complying with directives to block banned content (RBC 2017). Violations can lead to a fine. By 2017 the system covered 95 percent of all ISPs in Russia.

In 2018, Russian lawmakers passed Federal Law 155-FZ, which imposes fines on search engine operators who refuse to connect to the federal state information system that automatically filters search results. Roskomnadzor sent the requirement to connect to the system to Google, Yandex, Sputnik, and Mail.ru. Only Google did not connect and was fined 500,000 rubles (around US$8,000) for noncompliance (RBC 2018). The company paid the fine a month later, but Roskomnadzor has said it considers expanding the sanctions with a possible ultimate step to ban the search engine. Apparently, Google began manually removing sites on the

Roskomnadzor Blacklist from its search results, although the company has not officially acknowledged this practice (Boletskaya 2019). Silence from Google on this matter allows Roskomnadzor to claim that it successfully made the search engine giant comply with the Russian law, while at the same time Google avoids reputational risks for officially participating in internet censorship (Deutsche Welle 2019). In fact, Roskomnadzor admits it cannot do serious harm to Google while its search engine is serving millions of Russian citizens, unless the situation were to become threatening to national, corporate, and private security (RBC 2019). To this extent, some large foreign internet companies may enjoy a certain immunity from Russian laws, potentially giving them unfair advantages over Russian internet businesses.

In December 2019, a further law, 405-FZ, introduced fines of 1.5 to 5 million rubles if a search engine refuses for a second time to connect to the register of prohibited information (under 155-FZ) or refuses to filter prohibited content. Since Russian search engines – Yandex, Sputnik, Mail.ru, and Rambler – already complied with the earlier laws, the new legislation is mostly aimed at Google. At the time of writing (July 2020) the outcome of this struggle between the state and the global corporate giant remains to be seen.

Localisation and geo-blocking

The Russian Federal Law FZ-242 on localisation of personal data storage and processing came into force in 2016. The law requires all companies that store and process personal data of residents of Russia, including foreign citizens, to locate those databases on the territory of the Russian Federation. If a foreign entity already stores such a database abroad, it should transfer it to Russia. Roskomnadzor can geo-block violators of this law.

The first target was Microsoft's LinkedIn, which has been blocked in Russia since November 2016 due to its refusal to transfer servers containing personal data of residents of Russia to the territory of the Russian Federation (Lenta.ru 2016). Other major giants like Microsoft, Samsung, Lenovo, Aliexpress, eBay, PayPal, Uber, and Booking.com, instead of physically locating their databases to Russia, started to use special cloud services to process personal data and waive the legal responsibility for complying with 242-FZ. Roskomnadzor has not pursued legal proceedings against these companies, who have therefore in practice had little to fear from localisation requirements.

Leading social media networks like Facebook and Twitter initially sought to negotiate compliance with the data localisation law. Roskomnadzor asked the two companies to provide information about their compliance with 242-FZ. However, neither of them provided a consistent report of how they comply or plan to comply with the law. As a result, Roskomnadzor started civil proceedings against Facebook and Twitter in January 2019 (Browne 2019). However, it did not change the companies' policy to localise the data in Russia. Twitter paid a small fine – 3,000 rubles (around US$45) and then challenged the order in court. Facebook ignored the same fine (Roskomsvoboda 2019).

In June 2019, the Russian government introduced a new draft law to tighten penalties for violations in the field of data processing and dissemination of information (Bill No. 729516–7 2019). The bill specifies the size of sanctions for offenses, taking into account the international practice (mainly the European Union's General Data Protection Regulation) and furthermore introduces fines for violation of requirements for localisation of databases with personal data of people resident in Russia. In December 2019, the aforementioned law 405-FZ provides fines for legal entities of about 1 to 6 million rubles for the first violation and up to 18 million rubles (about US$280,000) for the second violation.

The new law signals a shift in tactics from geo-blocking to fines. In the words of the head of Roskomnadzor: "If we said a few years ago that violators should be blocked, now, it seems to me, there is a more civilised and effective method when they are punished economically – in this way we ensure that they comply with the local legislation" (TASS 2019). In February 2020, Roskomnadzor obtained court rulings to impose fines amounting to 4 million rubles (US$63,000) each on Twitter and Facebook, although at the time of writing (July 2020) they have not yet paid. Moreover, there is no way to enforce these payments, since no mechanism of recognition and enforcement of judicial acts vis-à-vis foreign entities exists. This would require special agreements with courts in the US, which is not feasible due to legal complexity of the issue (Roskomsvoboda 2020).

In sum, since 2012 the Russian government has pursued a policy of progressively tougher territorialisation in its internet regulation, with content filtering, data localisation, and (more occasionally) geo-blocking of websites and services. Tools to execute filtering and to check compliance with content laws are multiplying and becoming more centralised and automated. That said, Roskomnadzor still lacks real power to compel foreign internet services to execute full content filtering, except by issuing fines and threatening exclusion from Russian territory. Given the popularity of foreign social networks among the Russian population, the authorities cannot in practice undertake radical restrictions and instead call for a direct dialog with the foreign internet companies.

National control of critical internet resources in Russia

Already in 2006 and 2007, officials in the Security Council and Administration of the President were preoccupied with the possibility of external shutdown of the internet in Russia. They took seriously the possibility that the United States could unilaterally delete. ru and. su domains from the DNS, making the Russian websites inaccessible (Current Time 2019). Hence the Russian government has consistently pushed to transfer ICANN's functions to the ITU and even now, after the IANA transition, continues to criticise ICANN for being a US-based corporation.

Another concern for the Russian government relates to the circulation of Russian internet traffic. Some high-ranking officials believe that many internet communications within Russia loop through international networks (Current Time 2019). Such cross-border flows did actually happen in the early 2000s, during the emergence of the Russian telecom market, because of the low cost of such routes

and competition among ISPs. Inspired by several ideologues from Roskomnadzor, officials from the presidential administration exploited this story later after 2013, saying that loop traffic is unacceptable because foreign intelligence can then spy on Russian internet traffic or snatch and modify it. Some Russian parliamentarians continue to repeat such claims to this day (State Duma Readings 2019).

Following the cyber drills of 2014, mentioned earlier, the Security Council of Russia requested that the MoC should address the challenges for an independent Runet. In 2016, public discussion spread about the necessity to duplicate the DNS, IP number databases, and root servers in case of an external shutdown of the internet in Russia (Bill "On modification" 2016). This bill described the creation of a state information system that would contain data similar to that currently provided by RIPE NCC about routing policies and other databases. The bill proposed that, in case of emergency, all ISPs and telecom operators in Russia would employ this Russia-based system. However, the bill never reached the agenda of the State Duma for formal consideration and approval.

Instead, the government introduced a brand new bill in late 2018 (Bill No. 608767–7 2018; Stadnik 2018). Despite negative reactions of industry and technical experts, this bill rapidly passed the necessary readings in the State Duma and Federation Council. On 1 May 2019, the president signed it as Federal Law 90-FZ, popularly known as the law on "sovereign Runet." It provides that Roskomnadzor keeps registries for traffic exchange points, communication lines that cross Russia's borders, and autonomous system numbers (ASNs). In addition, the law requires telecom operators to ensure the installation in their networks of technical means (so-called black boxes) for countering threats to the stability, security, and integrity of internet operations on the territory of Russia (Stadnik 2019a). These black boxes also serve the purpose of traffic filtering and blocking access to prohibited internet resources. The law further creates a centre for monitoring and control of public communication networks under the supervision of Roskomnadzor. This centre will take over traffic routing in case of threats to the stability and security of the Runet and could be used as a kill switch if wished. Finally, the law also creates a National Domain Name System.

Before 90-FZ came into force in November 2019, Roskomnadzor, the MoC, and the government should have prepared around 40 regulatory acts to give force to its provisions. Among other things they should have presented a list of threats to the Runet and the principles of centralised traffic management; technical parameters and rules for managing the "black boxes"; principles for the registry of traffic exchange points; rules by which operators and owners of ASNs fill in various information systems; technical details for the creation and operation of the national DNS; and the framework for a centre to monitor and control the public communications network (Georgia Tech and Internet Governance Project n.d.). However, by the date of enactment only a third of these regulatory acts were ready, and many of them were technically inadequate.

The Russian internet industry raised three main concerns in relation to the new law. First, the "black boxes" – the technical means to counter threats – can dramatically affect the quality and speed of communication. The law implicitly

accepts this fact by exempting operators from responsibility for future network crashes. Second, legislators mixed up infrastructure-related threats and content-based threats, which come respectively from transport and applications levels of the internet. It is impossible to solve both problems with just one "black box." Third, the issue of duplication of critical elements of the internet infrastructure and domain names has already been agreed with the industry during the discussion of the previous bill introduced by the MoC in 2016. It was not clear why legislators did not push the adoption of the previous bill while there was a consensus with industry and instead invented a new document and added an ambitious aim to filter all Runet traffic.

Why was the bill passed in spite of these objections? Based on the statements of deputies and senators during the various readings of the 2019 bill, the motivation for its adoption can be summarised in several points. The main reason is that 90-FZ responds to the latest US cybersecurity strategy. Russian lawmakers saw several US cybersecurity strategy statements in 2018 – in particular, to use offensive capabilities to protect US networks and interests in cyberspace – as a direct threat to the Russian networks. Russian legislators justified the speed of the law's adoption in terms of its critical importance for implementation of the national programme "Digital Economy." Another argument to adopt the law 90-FZ was the analogy with sanctions by international payment systems in Crimea in 2014, when Russia had to elaborate its own national payment system, "МИР," to avoid a suspension of financial transactions.

Analysis of implementation and consequences

Mueller's framework of cyberspace alignment to national borders has helped to frame the various internet policies of the Russian government. However, the provisions of Russian statutes do not tell everything about the actual situation of internet governance in Russia. As already intimated earlier, implementation often falls well short of the legislated ambition.

In terms of securitisation and especially the internet kill switch, the Russian experience differs from Mueller's interpretation. Although the government has several times attempted to legalise a kill switch for the internet in Russia since 2014, it has never formulated the aim in these terms. Instead, the authorities have talked about improving resilience and making a national version of critical internet infrastructure. Industry and human rights activists have pointed to the covert aim of creating a kill switch, but the authorities have claimed that laws on Runet are needed to protect Russia from internet shutdowns by hostile states. Yet lawmakers in Russia often fail to realise that the centralisation of internet governance actually creates a more vulnerable situation technically, where there is only one command and control centre for the whole Runet. The legislative effort was pushed to its logical end in 2019 with the adoption of Law 90-FZ on a "sovereign Runet." Analysis of the law leaves the impression that it was written by people who see the internet as being similar to telephone communications. Moreover, the drafters appear to believe blindly in the omnipotence of "black boxes" that

will both filter traffic and protect infrastructure. At the time of writing, it seems that the government has realised that the technical separation of Runet from the internet was too ambitious and that it was rather naïve to create a legal instrument that would simultaneously handle content filtering and traffic routing.

Thus 90-FZ likely has the effect of more extensive filtering and censorship under the cover of national security. So, in practice "sovereign Runet" means more surveillance and control of information flows, rather than real traffic routing. Indeed, extensive traffic filtering is the priority for the Russian government. However, technically and economically it is a highly challenging task, given that there are thousands of ISPs, many of them with transborder internet traffic.

In this respect, the situation in Russia differs considerably from China, which has many fewer ISPs and many fewer transborder connections to the global internet. Moreover, China has a self-sufficient internal digital market that can be developed in isolation from the wider world. In contrast, total digital isolation for the much smaller market in Russia would be detrimental economically (lack of competition) and technically (degradation of service).

As for traffic filtering, the Russian authorities are here focused on keeping down significant political opposition, as well as demonstrating power to block services that refuse to comply with the multiplying laws and regulations. The problem for the government is that some web resources cannot be blocked by URL, IP address, or domain names. Instead it requires measures on the transport layer of internet protocols. As Efremov (2017, 203) wrote,

> the adoption of federal laws reveals opportunism and situationality associated with the desire to "combat threats" and "protect sovereignty" without a clear conceptual basis for the essence and content of information sovereignty as a political and legal feature of the state in the modern digital era.

Roskomnadzor's failure in 2018 to block the messenger app Telegram illustrates these shortcomings.

With regard to reliance on national standards and technologies, Russia started to reduce its dependence on imported software and hardware only after foreign sanctions went into effect. Before, there was not such a need for these measures. As things currently stand, it will be a long time before Russian hardware and software developers become competitive with foreign products. The government believes it is possible and will serve as a silver bullet to security and sanction problems, but in practice they are far behind China in terms of reaching technical autonomy.

Finally, regarding domain names and IP addresses, Russia has quite a strong distrust in the current global technical internet governance system, with ICANN in a central role. One of the co-authors of 90-FZ claimed that, under this regime, Russia can technically be disconnected from the internet root servers (Kod Durova 2019). However, he did not consider that the governance of critical internet infrastructure requires trust and cooperation among all involved stakeholders. To say that American companies (namely ICANN and Verisign) can immediately "cut out" records of the Russian domains by the order from the US government is a

major misconception. If ICANN were to set such a precedent, the organisation would forever lose its credibility, and it would threaten the resilience of the global internet as a whole if it lacked an authoritative centre for the coordination of the DNS. The situation would roll back to the late twentieth century when various large regional networks coexisted. This is the last thing the US government wants, because it directly contradicts its policy of globalisation and the spread of the internet around the world.

Still, 90-FZ contains a provision for a National Domain Name System in Russia. In reality, however, the measure amounts to little more than listing nationally significant domains created in accordance with ICANN rules. This is not the same as Chinese ideas about a nationalised DNS. The Russian idea is to keep "national" domains accessible through the local DNS resolvers without needing to reach root servers, but this technology remains challenging and expensive. So, in the end the Russian government is looking for ways to keep open the "window" to the global internet and services while at the same time implementing tough regulation of domestic networks and services. 90-FZ allows for centralised traffic routing in case emergency, but no one can even approximately predict how such a measure would operate and how it would affect the global internet as a whole. Thus, Russia probably will not execute centralised routing, and in any case the technical means to do so are not yet available.

Conclusion

As seen throughout this chapter, the Russian government strongly wishes to align the internet with its national borders. It has pursued this aim in a variety of ways in relation to content, data, and infrastructure. However, achieving this goal takes a lot of time. Some parts have been completed, but the most important and technical measures have not advanced from proposal to practice.

Power and authority relations among state, commercial, and civil society actors in internet governance in Russia are asymmetric. The government emphasises national security at any price and imposes more regulations and control, neglecting the opinions and operational principles of technical and private stakeholders. It is obvious that the Russian government will not drop out of multistakeholder governance processes for the internet, but it needs to pursue more meaningful interaction with all stakeholders. The state should listen and develop policies in accordance with technological realities and not force stakeholders to implement and comply with laws that are often impossible and/or harmful.

In terms of internet policy in general, the Russian case may offer insights for other states that seek more governmental regulation, instead of the rule of global corporate giants when it comes to filtering undesired content or data governance. In terms of French President Emmanuel Macron's classification of internet governance models – Californian-libertarian, new multilateralism, and Chinese-authoritarian (Macron 2018) – Russia lies towards the middle of this spectrum, but closer to the Chinese end due to Russia's adherence to the concept of internet sovereignty.

Notes

1 The other three are international legal sovereignty (legal recognition), Westphalian sovereignty (the right to exclusive control over a state's territory), and domestic sovereignty (the ability to control a state's territory).
2 An internet kill switch is a single point of control (i.e., a switch) for a single authority to control networks' management and monitoring or shut down the Internet in order to protect it or its users. The instrument has become widely used during protests and insurgency in several countries.
3 See the Unified register of Russian software for electronic computing machines and databases, https://reestr.minsvyaz.ru/reestr/.

Cited legislation and government documents

Bill "On Modification of the Federal Law "On Communication" and the Federal Law "On Information, Information Technologies for Information Protection." 2016. https://regulation.gov.ru/projects#departments=31&okveds=33&StartDate=null&search=Интернет&npa=71277.

Bill No. 608767–7. 2018. "On Amendments to Some Legal Acts of the Russian Federation." *The State Duma*. http://sozd.duma.gov.ru/bill/608767-7.

Bill No. 729516–7. 2019. *On Modification of the Code of Administrative Offenses of the Russian Federation*. https://sozd.duma.gov.ru/bill/729516-7.

Decree No 31. of the President of the Russian Federation 15 January 2013. https://rg.ru/2013/01/18/komp-ataki-site-dok.html.

Decree No. 1236 "On the Establishment of a Ban on the Admission of Software Originating from Foreign Countries for the Purposes Of Procurement for State and Municipal Needs." 16 November 2015. http://reestr-minsvyaz.ru/postanovlenie-1236/.

"Doctrine on information security of Russia." 2016. https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

Federal Law No. 90-FZ. "O Sovereign Runet." 1 May 2019. www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=45357485408957758943434615&cacheid=8EE6A7ABEDBC5F60D5E9C98216EA37EA&mode=splus&base=LAW&n=323815&rnd=61079B911638398DD215020D7FD220F9#7rf6rp0x13o.

Federal Law No. 139-FZ. "On Blacklist." 28 July 2012. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=169766&fld=134&dst=1000000001,0&rnd=0.5871394981634195#07263450173105755.

Federal Law No. 155-FZ. "On Fines for Search Engines." 27 June 2018. http://publication.pravo.gov.ru/Document/View/0001201806270048?index=0&rangeSize=1

Federal Law No. 155-FZ. "On Responsibility of Search Engines." 27 July 2018. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=301055&fld=134&dst=1000000001,0&rnd=0.2572145288251887#0806152871819813.

Federal Law No. 187-FZ."Anti-Piracy Law." 2 July 2013. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=160239&fld=134&dst=100008,0&rnd=0.37434718475777107#07569470061777615.

Federal Law No. 187-FZ. "On Critical Information Infrastructure." 26 July 2017. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.24774062659808 37#07294351284912781.

Federal Law No. 242-FZ. "On Personal Data Localization." 21 July 2014. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=173429&fld=134&dst=1000000001,0&rnd=0.9212646286337768#07486283833929902.

Federal Law No. 398-FZ. "On Extremist Content." 28 December 2013. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=156518&fld=134&dst=1000000001,0&rnd=0.1665790389102384#0669269846064224.

Federal Law No. 405-FZ. "On Higher Fines for Failed Data Localization and Filtering of Search Results." 2 December 2019. www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=339082&fld=134&dst=100008,0&rnd=0.716377251051844#02378352942540246.

Order of the Federal Security Service No. 52107. 6 September 2018. http://publication.pravo.gov.ru/Document/View/0001201809100003?index=0.

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 (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed 4 August 2020.

State Duma Readings on the Bill No. 608767–7. 2019. Official Transcript. http://transcript.duma.gov.ru/api_search/?search_mode=number&sessid=5081&dt_start=&dt_end=&deputy=&type=any&number=608767-7&keyWords=.

References

Barlow, J. 1996. *A Declaration of the Independence of Cyberspace*. www.eff.org/cyberspace-independence. Accessed 4 August 2020.

Becker, M. 2019. "When Public Principals Give Up Control over Private Agents: The New Independence of ICANN in Internet Governance." *Regulation and Governance* 13 (4): 561–576. https://doi-org/10.1111/rego.12250.

BJNews. 2019. 网络主权：理论与实践 [*Cyber Sovereignty: Theory and Practice*]. China Institute of Contemporary International Relations, Shanghai Academy of Social Sciences, Wuhan University. 22 October. www.bjnews.com.cn/feature/2019/10/22/639825.html?fbclid=IwAR2PNNRy6OEiyYTJezTLwsSoeYSnBs5kd9BkpR52Np9ebaRkxvQ2FJYxLx0. Accessed 4 August 2020.

Boletskaya, Ksenia. 2019. "Google начал удалять из результатов поиска ссылки на сайты, запрещенные в России [Google Began to Remove Links to Sites Prohibited in Russia from the Search Results]." *Vedomosti*. 6 February. www.vedomosti.ru/technology/articles/2019/02/06/793499-google. Accessed 4 February 2020.

Browne, Ryan. 2019. "Russia Opens Civil Proceedings Against Facebook and Twitter." *CNBC.com*. 21 January. www.cnbc.com/2019/01/21/russia-reportedly-opens-civil-proceedings-against-facebook-twitter.html. Accessed 4 August 2020.

Current Time. 2019. "Кто и как придумал 'суверенный Рунет'. Рассказы инсайдеров [Who and how invented the 'sovereign Runet'. Insider Stories]." 22 April. www.currenttime.tv/a/ex-officials-about-runet-roscomnadzor/29895845.html. Accessed 4 August 2020.

Demchak, Chris C., and Peter J. Dombrowsky. 2011. "Rise of a Cyberred Westphalian Age." *Strategic Studies Quarterly* 5 (1): 31–62.

Deutsche Welle. 2019. "Комментарий: Google начал цензурировать поисковую выдачу в России? [Commentary: Has Google Started Censoring Search Results in Russia?]." 8 February. www.dw.com/ru/комментарий-google-начал-цензурировать-поисковую-выдачу-в-россии/a-47427466. Accessed 4 August 2020.

Du, Zhicao, and Yuxia Nan. 2014. "Analysis of the Relationship between Internet Sovereignty and National Sovereignty." *Journal of Southwest Petroleum University* 16 (6): 79–84 (in Chinese).

Efremov, A.A. 2017. "Formation of the Concept of Information Sovereignty of the State." *Pravo. Zhurnal Vysshey shkoly ekonomiki* 1: 201–215 (in Russian).

Fehlinger, Paul. 2014. Cyberspace Fragmentation: An Internet Governance Debate beyond Infrastructure. *Internet Policy Review*. www.internetjurisdiction.net/uploads/pdfs/Articles/PDF-Internet-Jurisdiction-Cyberspace-Fragmentation-2014_170125_152501.pdf. Accessed 4 August 2020.

Forbes. 2019. "IT без иностранцев: как депутат Горелкин напугал 'Яндекс', Mail.ru и 'Мегафон' [IT Without Foreigners: How the Deputy Gorelkin Frightened 'Yandex', Mail.ru and 'Megaphone']." *Forbes.ru*. 27 July. www.forbes.ru/tehnologii/380813-it-bez-inostrancev-kak-deputat-gorelkin-napugal-yandeks-mailru-i-megafon. Accessed 4 August 2020.

Franzese Patrick, W. 2009. "Sovereignty in Cyberspace: Can It Exist?" *Air Force Law Review* 64: 1–42.

Georgia Tech and Internet Governance Project. n.d. *Federal Law Dated 01.05.2019 No 90-FZ 'On Amendments to the Federal Law 'On Communications and the Federal law 'On Information, Information Technologies and Information Protection'*. www.internetgovernance.org/wp-content/uploads/Federal-law-FZ-90-Summary.pdf. Accessed 4 August 2020.

Giacomello, Giampiero. 2005. *National Governments and Control of the Internet: A Digital Challenge*. London: Routledge.

Giacomello, Giampiero, and Fernando Mendez. 2001. "*Cuius Regio, Eius Religio, Omnium Spatium*? State Sovereignty in the Age of the Internet." *Information and Security* 7: 15–27. http://dx.doi.org/10.11610/isij.0701.

Giles, Keir, and Hagstead II, William. 2013. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." *5th International conference on Cyber Conflict (CYCON 2013)*. https://ieeexplore.ieee.org/abstract/document/6568390/.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York: Metropolitan Books.

Hill, Jonah Force. 2012. "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers." *Belfer Center for Science and International Affairs*. www.belfercenter.org/sites/default/files/files/publication/internet_fragmentation_jonah_hill.pdf. Accessed 4 August 2020.

Information Office of the State Council of the People's Republic of China. 2010. *White Paper on the Internet in China*. www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Internet%20in%20China.pdf. Accessed 4 August 2020.

Interfax. 2017. "В Минобороны РФ создали войска информационных операций. [The Ministry of Defense Created the Troops of Information Operations]." 22 February. www.interfax.ru/russia/551054. Accessed 4 August 2020.

Jinping, Xi. 2015. *Remarks at the Opening Ceremony of the Second World Internet Conference, Wuzhen*. 16 December. www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml. Accessed 4 August 2020.

Johnson, David R., and David Post. 1996. "Law and Borders – The Rise of Law in Cyberspace." *Stanford Law Review* 48 (5): 1367–1402. https://doi.org/10.2307/1229390.

Kod Durova. 2019. "Андрей Клишас: Закон о суверенном Рунете не об ограничениях, а о защите Рунета [Andrey Klishas: The Law on the Sovereign Runet Is Not about Restrictions, But about the Protection of the Runet]." *Kod.ru*. 5 August. https://kod.ru/klishas-o-suverennom-runete-aug-2019/. Accessed 4 August 2020.

Krasner, Stephen. 1999. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press.

Kucheryavyiy, M.M. 2015. "К осознанию информационного суверенитета в тенденциях глобального информационного пространства. [Realizing Information Sovereignty in the Trends of Global Information Space]." *Nauka, novyie tehnologii i innovatsii Kyrgyizstana* 12.

Lenta.ru. 2016. "В России заблокировали LinkedIn [Russia blocked LinkedIn]." *Lenta.ru*. 17 November. https://lenta.ru/news/2016/11/17/linkedin_block/. Accessed 4 August 2020.

Macron Emmanuel. 2018. *Speech at Internet Governance Forum, Paris*. 12 November. www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron. Accessed 4 August 2020.

Merkel Angela. 2019. *Speech at Internet Governance Forum, Berlin*. 26 November. www.un.org/sg/en/content/sg/statement/2019-11-26/secretary-generals-remarks-the-internet-governance-forum-delivered. Accessed 4 August 2020.

Ministry of Communications, Russia. 2014. "Press Release: Ministry of Communications, FSB, and Ministry of Defense Conducted Cyber Drills on Protection of the Russian Segment of the Internet." 28 July. https://digital.gov.ru/ru/events/31441/. Accessed 4 August 2020.

Ministry of Defense, Russia. 2011. *Conceptual Views on the Activity of the Russian Armed Forces in the Information Space*. http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle. Accessed 4 August 2020.

Moniz Bandeira, Luiz Alberto. 2019. "Crimea Back to Russia and Economic Sanctions Against Russia." In *The World Disorder*. Cham: Springer. https://doi.org/10.1007/978-3-030-03204-3_18.

Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. London: Polity.

Mueller, Milton. 2019. "Against Sovereignty in Cyberspace." *International Studies Review* viz044. https://doi.org/10.1093/isr/viz044.

Polikarpov, V.S., E.V. Polikarpova, and V.A. Polikarpova. 2014. "Информационный суверенитет России, сенсорная революция, социальные сети: Интернет и кибервойна.т [Russia's Information Sovereignty, Sensor Revolution, Social Nets, Internet and Cyber War]." *Informatsionnoe protivodeystvie ugrozam terrorizma* 23: 272–278.

RBC. 2017. "Сетевой 'Ревизор': как работает система контроля за запрещенным контентом. [Network 'Revizor': How Works the System of Control over the Prohibited Content]." *Rbc.ru*. 7 September. www.rbc.ru/technology_and_media/07/09/2017/59b00e269a79475c24ccf090. Accessed 4 August 2020.

RBC. 2018. "Роскомнадзор оштрафовал Google и пообещал проверить Twitter и Facebook [Roskomnadzor Fined Google and Promised to Check Twitter and Facebook]." *Rbc.ru*. 11 December. www.rbc.ru/rbcfreenews/5c0f839d9a79478947d36454?from=materials_on_subject. Accessed 4 August 2020.

RBC. 2019. "Александр Жаров – РБК: 'Настало время перейти к надзору за услугами' [Alexander Zharov – RBC: 'It Is Time to Move to the Supervision of Services']." *Rbc.ru*. 10 June. www.rbc.ru/interview/technology_and_media/10/06/2019/5cf9238f9a794756a61a8306.

RIA Novosti. 2012. "В российской армии может появиться киберкомандование, заявил Рогозин [In the Russian Army May Appear Cyber Command, Said Rogozin]." 21 March. *Ria.ru*. https://ria.ru/20120321/601798789.html. Accessed 4 August 2020.

Roskomsvoboda. 2019. "Суд оштрафовал Twitter на три тысячи рублей [The Court Fined Twitter for 3000 Rubbles]." 6 April. https://roskomsvoboda.org/46303/. Accessed 4 August 2020.

Roskomsvoboda. 2020. "Для взыскания штрафов с Facebook и Twitter Роскомнадзор обратился к приставам [Roskomnadzor Turned to Bailiffs to Collect Fines from Facebook and Twitter]." 28 May. https://roskomsvoboda.org/59138/. Accessed 4 August 2020.

Schmitt, Michael. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139169288.

Schmitt, Michael. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2. arg. Cambridge: Cambridge University Press. doi:10.1017/9781316822524.

Stadnik, Ilona. 2018. "Russia Tries to Double Down on a 'National' Internet." *Internet Governance Project (blog)*. 23 December. www.internetgovernance.org/2018/12/23/russia-tries-to-double-down-on-a-national-internet/. Accessed 4 August 2020.

Stadnik, Ilona. 2019a. "Sovereign RUnet: What Does it Mean?" *Internet Governance Project*. Georgia Institute of Technology. 12 February. www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/. Accessed 4 August 2020.

Stadnik, Ilona. 2019b. "DPI System to Filter Traffic is Uncovered." *Internet Governance Project* (blog). 3 April. www.internetgovernance.org/2019/04/03/sovereign-runet-all-the-way-down/. Accessed 4 August 2020.

TASS. 2019. "Жаров заявил, что Россия перейдет от мер блокировки к штрафованию нарушителей в интернете. [Zharov said that Russia Will Move from Blocking Measures to Fining Violators on the Internet]." *Tass.ru*. 21 October. https://tass.ru/obschestvo/7024257. Accessed 4 August 2020.

Vinnik, D.V. 2014. "Цифровой суверенитет: политические и правовые режимы фильтрации данных. [Digital Sovereignty: Political and Legal Regimes in Refining Data]." *Filosofiya Nauki* 2: 95–113.

Walton, Greg. 2001. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Montreal: International Center for Human Rights and Democratic Development, Canada.

Winseck, Dwayne. 2019. "Internet Infrastructure and the Persistent Myth of U.S. Hegemony." *In Information, Technology and Control in a Changing World*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 93–120. New York: Palgrave Macmillan.

Yang, Zewei. 2012. 国际法析论 [*Analysis of International Law*]. Beijing: Renmin University Press.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of Internet Sovereignty." *Politics & Policy* 45 (3): 432–464.


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Part 3

Internet governance and democratic states


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

8 The return of the state? Power and legitimacy challenges to the EU's regulation of online disinformation

Julia Rone

Introduction

In November 2018, at the Internet Governance Forum (IGF) Opening Ceremony, French President Emmanuel Macron shared a new vision of the state's role in internet regulation. Macron argued that states could and should regulate the internet and were the actors in the best position to do so (Macron 2018). According to the French leader, the choice between a *laissez faire* internet, driven by corporate rule (what he referred to as a "Californian internet"), and a compartmentalised internet, "entirely monitored by strong and authoritarian states" (a "Chinese internet"), is a false choice. Democratic states, he argued, should step in to regulate the internet, while preserving respect for human rights and freedom of information. Macron's speech seemed to suggest that there is a third, European, model of regulating the internet.

Several months later, in March 2019, Mark Zuckerberg, the CEO of Facebook, the social networking company with more than 2.45 billion users, published an op-ed in *The Washington Post* claiming that the internet "needs new rules" (Zuckerberg 2019). Considering that Facebook had argued against regulation for years (Kayali 2019), it seemed that finally the company acknowledged the necessity of government regulation.

In a sense, these two interventions, one by the leader of a G7 country and one by the CEO of the world's seventh most valuable private company, both point to a "return of the state" in the field of internet governance, presupposing public control over what was once generally considered the domain of private companies in the West. What is more, it suggests a particular "return of the democratic state", different from existing authoritarian attempts at controlling the internet, and has met as such serious challenges along the way.

This chapter narrows down the general question of the nature of the "return of the state" in internet regulation to focus in particular on the regulation of online disinformation. It focuses explicitly on the case of the European Union, where the topic of disinformation has gained widespread prominence in the aftermath of the Brexit referendum and amid fears of Russian intervention in the 2019 European elections (Apuzzo and Satariano 2019; Cadwalladr 2017; Tucker et al. 2018). We pose several key questions: Who is carrying out the regulation of disinformation

DOI: 10.4324/9781003008309-12

in the EU and what power does this require and give them? What legitimacy challenges arise in the process and how are they addressed? Has the EU managed to offer a third model of internet regulation, going beyond both the Californian model of private-sector-led regulation with minimal government regulation and the Chinese model of centralised control?

While disinformation has been a global problem for internet regulation, much of the literature so far has focused on the US experience and debates (Mourão and Robertson 2019; Nyhan 2019; Tucker et al. 2018). This chapter argues that focusing on the EU could provide a novel and important perspective to the global problem of regulation. The EU has been the most active democratic jurisdiction when it comes to state involvement in internet regulation in general. The implementation of the General Data Protection Regulation in May 2018 has been a crucial step in legislating data protection not only in the EU but also worldwide. In this sense, if democratic states' attempts to regulate disinformation would be successful anywhere, the EU would be a most likely case. Second, the EU has aimed to be a soft-power exporter of regulation to other parts of the world. Consequently, any developments in the field of regulating disinformation in the EU are likely to influence other countries to varying extents. In this sense, it is important to study the EU as a potential trendsetter in global internet regulation. Third, the multilevel governance structure of the EU poses specific challenges and provides a great test case to trace the importance of state power and ambitions in attempting to address internet regulation – a field currently dominated by private players such as Facebook. EU states with big markets such as France and Germany have been much more ambitious in trying to pressure Facebook and Twitter to accept regulation than smaller EU member states. In principle, all sovereign countries are equal when it comes to regulating internet corporations, yet in practice some are more equal than others. We are likely to observe similar power dynamics between states and corporations also in non-EU countries.

To be sure, regulating disinformation – defined as intentionally deceptive falsehood (Tandoc, Lim and Ling 2020, 3) – has been only one field of regulation in a wider EU effort to deal with hate speech, terrorist speech, as well as other platform-related issues such as competition and taxes in the digital environment. Unlike hate speech or terrorist speech, however, disinformation is not illegal in most EU countries and this reality has posed serious problems when it comes to legitimating stricter forms of regulation of internet companies, including legislation. If the EU and its member states are to put forward a model of internet regulation based on democracy and human rights, the question of legitimacy is fundamental. Beyond the issue of political power and clout – that is, whether states can actually make giant US companies comply with their regulations – this need for democratic legitimacy creates an additional limitation to what EU states and institutions can do and leads them to adopt strategies of decentred governance in which public and private actors cooperate – and conflict – in defining the problem of disinformation and addressing it. The chapter's analysis of the regulation of disinformation uses the lens of decentred regulation (see, e.g., Black 2001) that places important decision-making power in the hands of private actors and appears far from a unilateral return of the state as advocated by President Macron.

Focusing on the dynamics among public and private actors and, in particular, the agency of private actors within decentred regulation in the context of internet governance, this chapter introduces two concepts: preemptive cooperation and conflictual cooperation. Preemptive cooperation refers to private actors' readiness to participate in the early stages of drafting state regulation in order to influence it in their preferred direction, usually to weaken it. Cooperation thus acts as a preemptive measure that helps companies avoid unfavourable regulation. Conflictual cooperation, on the other hand, refers to the ways in which private actors enter into conflict with public actors or with each other in the process of cooperation. In short, cooperation does not put an end to regulatory conflicts but allows them to simmer contained within an established network of relations. Together, these concepts provide us with a more nuanced means to understand how decentred regulation may operate within the realm of internet governance.

The chapter proceeds as follows. To begin, it discusses decentred regulation and digital sovereignty generally and the EU's approach to digital sovereignty and how it differs from approaches taken by China or Russia in particular. It then analyses the importance of power and democratic legitimacy to understand the challenges the EU has faced in its recent attempts to regulate disinformation. Next, it focuses on the issue of disinformation and problematises the dangerous trend towards political and legislative bundling together of different types of harmful content such as disinformation, hate speech, and defamation. Importantly, it questions definitions of disinformation that place an excessive focus on foreign actors intent on disrupting elections while relatively neglecting the role of domestic, especially far-right players. The third section of the chapter discusses the concrete actions taken by the EU and its member states in order to regulate disinformation. It highlights initiatives by individual member states, most notably France and the UK (before Brexit), and by EU institutions. We then move on to analyse the complex instances of preemptive and conflictual cooperation between private global platforms and public actors in the EU. The final section of the chapter offers an overview of some of the blind spots of regulatory efforts so far on the basis of interviews with experts. We also offer a suggestion for the broader field of internet regulation based on some of the challenges in regulating disinformation in the EU, namely a possible way out of the legitimacy dilemmas of both state sovereign regulation and decentred regulation through an engagement with parliamentary and popular sovereignty. Parliamentary discussions, as well as public consultations and more deliberative forms of public debates both within nation states and across the EU, are among the important ways to provide much needed democratic legitimacy to the tough decisions involved in internet regulation.

Challenges of power and legitimacy in decentred regulation versus digital sovereignty

President Macron's call for more state sovereignty and for democratic states to move beyond the "Californian model of the internet" is essentially a call to seek an alternative to the decentred regulation that has been at the centre of research

and governance practice for more than 20 years now (see ten Oever, this volume). Indeed, when we talk about a "return of the state" in internet regulation, and especially in the regulation of content, we need to emphasise that this is not a return in the sense of going back to a situation from the past but rather a return of a player that has been relatively marginalised (see Cavalli and Scholte, Santaniello, and ten Oever, all this volume). Since the 1990s, the dominant model of internet regulation in democratic states has been decentred, or networked, regulation, which involves "a shift in the locus of the activity of 'regulating' from the state to other, multiple, locations, and the adoption on the part of the state of particular strategies of regulation" (Black 2001, 112). Accompanying this recognition of non-state actors' role is the understanding that regulatory strategies include non-state-centred forms of governance like industry self-regulation. Forms of decentred regulation have become increasingly common in a wide range of policy fields, from the production and distribution of agricultural commodities (McNaughton and Lockie 2017) to global finance (Andenas and H-Y-Chiu 2014; Scholte 2013) and, of course, the governance of new and emerging digital technologies (Leiser and Murray 2017).

While both the concept of decentred regulation and the related concept of self-regulation have their origins in theories of autopoietic systems, that is, those systems capable of reproducing themselves from within themselves, related concepts such as "networked" or "nodal governance" have been traced rather to the work of Foucault on power perceived as relational and circulating through networks. Drawing on a wide range of authors, Farrand and Carrapico (2013, 359) emphasise that in networked regulation "political decision-making is not restricted to formal governmental institutions, but is the result of the creation, construction, and establishment of policy networks." The concepts of decentred and networked regulation both highlight the multiplicity of actors involved in regulation and the blurring of the distinction between public and private actors. As such, these concepts are starkly opposed to newly emerging doctrines of digital sovereignty that have become increasingly relevant in the past few years.

The use of the term "digital sovereignty" in the ProQuest collection of databases has increased from six mentions in the period before 2011 to 239 mentions in the period from 2015 to 2018 (Couture and Toupin 2019). This term, as well as the related terms "information sovereignty" and "data sovereignty", have been used in a broad range of ways that go beyond narrow conceptions of authoritarian control. Analysts and activists have invoked various and sometimes diametrically opposed discourses such as "indigenous digital sovereignty" (Kukutai and Taylor 2016) – related to indigenous populations' control of technologies and digital infrastructures – and state digital sovereignty – related to the state's capacity to control crucial technical infrastructure and the flow of information within and across its borders (Kukutai and Taylor 2016).

This chapter focuses above all on digital sovereignty, understood as state digital sovereignty, a concept that often comes with a strong geopolitical flavour. While states have traditionally controlled the flows of goods and people over their borders, the idea that the flows of data and content over the internet, or the internet's

infrastructure itself, can (or should) be controlled was put forward explicitly as a state doctrine by China only in 2010 (Powers and Jablonski 2015, 169). In 2015, meanwhile, China and Russia signed a cyber-defence agreement whose purpose was to limit the use of information technologies designed to "interfere in the internal affairs of states; undermine sovereignty, political, economic and social stability; [and] disturb public order" (Margolin 2016). With this move, China and Russia effectively posed a challenge to the dominant American internationalist approach to norms of digital governance. It is this particular understanding of digital sovereignty that Macron referred to when talking about the "Chinese model" of the internet.

Yet, just as sovereignty is the property not only of authoritarian states but of all states in the international state system, the advocacy and pursuit of digital sovereignty is not only the purview of authoritarian states. The doctrine of digital sovereignty started gaining traction in Western democratic countries after the revelations by Edward Snowden that the US National Security Agency, together with its global partners, had engaged in mass surveillance of both foreign nationals and US citizens. The leaks showed that even the phone of German Chancellor Angela Merkel had been hacked (Bauman et al. 2014). In response to these revelations, countries such as Germany and Brazil started contemplating data localisation initiatives (Hill 2014). By 2019, discourses on digital sovereignty made their way into European Union policy with the EU announcing the launch of a new project called Gaia-X that aims to achieve "cloud independence" and allow local providers to compete with dominant US cloud providers (Meyer 2019).

Another crucial watershed in Western political opinion, this time with respect to content regulation, came with Brexit and the election of Donald Trump in the United States in 2016. Major newspapers quickly explained away these complex political developments as the result of fake news and foreign disinformation, leading to increased attention to the topic (Cadwalladr 2017; Viner 2016). In the aftermath, an almost Cold War degree of rhetoric raising concerns about foreign interference flourished. Since then, both the US and the EU have expressed the desire to establish some version of digital sovereignty over flows of information within and across country borders. While China and Russia have a long history of censoring and regulating content online, there was little appetite for such initiatives in the West. Child pornography and terrorist speech, for example, have been the object of regulatory battles since the 1990s (Wagner 2013), but monitoring political speech online was generally considered a no-go zone. Following Brexit and Trump's election, the 1990s-era cyber-libertarian belief that the internet represents the frontier of ultimate freedom from the state ceded ground even more to a generalised acceptance that greater state regulation of the internet is necessary. All this shows that digital sovereignty is not necessarily an autocratic concept and encompasses more than what a narrow invocation of the "Chinese model" of the internet would suggest.

What Macron's speech offered as an alternative to the "Chinese model" seems to be a different, "European", version of digital sovereignty, applicable in democratic states, that respects human rights and democratic process. The problem,

however, is that achieving this is easier said than done. To begin, getting big US corporations to comply with rules that might be costly to them and technically challenging to implement requires considerable state power and capacity, including technical expertise. Second, as already mentioned, while disinformation may not be socially desirable, it remains legal, at least in the EU. Furthermore, there is far from a public consensus on how it should be regulated, with far-right actors calling the EU Commission "Ministry of Truth" because of its attempts to regulate disinformation (Mooney 2019). Due to these problems of both power and legitimacy, the EU and its member states have found it difficult to regulate the digital sphere. In fact, it is impossible to understand the challenges the EU has faced in regulating disinformation, without paying attention to the concepts of power and legitimacy and the ways they relate to each other.

For the purposes of this chapter, we define power as the ability of the state or any other agent "to get others to act in ways that they desire even when the subject does not want to do what the agent wants him to do" (Christiano 2012). When it comes to regulating disinformation, particular actors, such as states, would have power if they manage to get other actors, such as private companies, to do what they want them to do. States' regulatory power in this context comes to a large extent from the size of their markets, as larger states can employ the threat of market access to compel compliance from corporate actors. Following this logic, countries such as Germany and France, with bigger markets, would be more persuasive than smaller countries such as Slovenia and Bulgaria, for example. But state regulatory capacity is not only about country size. It also has elements of expertise. Similar to other highly technical areas of regulation, such as stock markets, in order to be able to tell internet companies what they should do, states need to know better how these companies operate, including what algorithms they use. Yet, internet giants have been opaque about their internal operations, with their algorithms famously protected by trade secrets. Of course, larger states such as Germany and France can more easily regulate the internet giants even without knowing the intricacies of their operations, as was the case with Germany's 2017 law to compel Facebook to remove hate speech from its platform (Lomas 2017). Nevertheless, the regulation of disinformation faces problems not only of power but also of legitimacy, further diminishing the options of what even big democratic states can do.

A simple definition of legitimacy points to legal validity and conformity with the law. The three key dimensions of legitimacy in democratic states, as outlined in the literature, are 1) democracy, referring to "the structural aspects such as the representation of the population and the separation of powers"; 2) identification, pointing to "the popular acceptance of the project of the political authority that governs"; and 3) performance, defined as "the relation of the political system to the ends or purposes it should serve and the effectiveness of its decision-making procedures" (Beetham and Lord 1998, as quoted in Voermans, Hartmann and Kaeding 2014, 12).

If a powerful authoritarian state such as Russia or China attempts to regulate the internet, they may have the power to coerce cooperation. However, even

authoritarian states face limitations, as the chapters in this volume by Jia, Luo and Lv, and Stadnik show. In contrast, if the EU and its member states attempt to regulate the internet, power is not enough: Democratic legitimacy is also crucial. This is where the main difference from the so-called Chinese model becomes clear. Following the definition of legitimacy presented earlier, in order to be perceived as legitimate, regulatory arrangements on disinformation in the EU are expected to ensure democratic participation, gain popular acceptance, and achieve the goals they set for themselves.

It is because of the demands for legitimacy, coupled with the perception – accurate or perceived – that internet firms have essential, specialised knowledge for the regulation of disinformation, that the EU Commission refrained from attempting state-centred regulation and involved private internet companies in the process of regulation instead. Yet, as the EU's response shows, the composition of state/non-state actors matters in terms of representativeness. The EU's efforts focused too closely on private companies and experts and failed to involve ordinary citizens in a meaningful and sustained way in both defining where the problem with disinformation lies and in devising ways to solve it. The multistakeholder model of decentred governance that the EU Commission fell back on has been often held as a best practice in internet governance, but numerous authors have noticed it leads to window-dressing and the privileging of certain actors over others (Buxton 2019; Donders, Van den Bulck and Raats 2019; Iusmen and Boswell 2016; Schleifer 2019). This chapter shows that this has been very much the case also when it comes to regulating disinformation.

Before moving on to discuss current instances of regulation of disinformation and the legitimacy problems they pose, a short overview of the current state of discussions on disinformation is needed.

Defining "disinformation" and justifying its regulation

In his IGF speech, President Macron claimed that "[O]ur governments, our populations will not tolerate much longer the torrents of hate coming over the internet from authors protected by anonymity which is now proving problematic" (2018). Macron's examples of problematic content in his IGF speech refer above all to hate speech and terrorist speech (see also Santaniello, this volume). The word "disinformation" is not mentioned a single time, while fake and doctored images are mentioned once. Nevertheless, it is very likely that disinformation was on his mind: Only five days after this speech, France introduced a new law targeting fake news (Fiorentino 2018).

Macron's speech is indicative of the fact that in many contexts the regulation of disinformation is justified by analogy to the need to regulate other types of speech. For instance, a 2019 consultative paper of the UK government regarding online content regulation (Department for Digital, Culture, Media & Sport and Home Office 2019) identified as "online harms" not only familiar categories such as terrorism and child sexual abuse but also "revenge porn, hate crime, harassment, promotion of self-harm, content uploaded by prisoners, disinformation, trolling, and

the sale of illegal goods" (Volpicelli 2019). Needless to say, there are massive differences among these different types of content. This inclusion of different types of content (as objectionable as they may each be) together as "online harms" brings to mind the argument of Richard Stallman (2006), the famous founder of the Free Software Foundation, that bundling together trademarks, copyright, and patents under the label intellectual property is a "seductive mirage" that favours the interests of big companies. Similarly, we can claim today that speaking of "harmful content" in general is a "seductive mirage" that could justify state censorship of problematic but not necessarily illegal content "by analogy" with actually illegal content, without actually making the problematic content illegal.

Disinformation is a perfect example of such problematic-but-not-illegal content: It has been used for centuries by political actors to shape or promote particular policy options. Disinformation cannot simply be lumped with "hate speech". Hate speech is regulated in the EU because of the threats it poses to human dignity as a fundamental right, protected by Article 1 of the EU Charter of Fundamental Rights (Belavusau 2012). But there is no such corresponding justification when it comes to disinformation. The European Commission's Action Plan against Disinformation (High Representative of the Union for Foreign Affairs and Security Policy 2018) has justified combatting disinformation above all by asserting its incompatibility with the normal functioning of the democratic process. Furthermore, a key criterion for identifying disinformation has been the intent of content producers to spread disinformation to "intentionally cause public harm or for profit" (High Level Group on Fake News and Online Disinformation 2018b, 10). But how does one decide what constitutes public harm and threatens the democratic process in the absence of concrete criteria? And who decides what these criteria are? For example, the UK's Parliament report on fake news and disinformation points to the removal by Facebook of 289 pages and 75 accounts that "posted about topics like anti-NATO sentiment, protest movements, and anti-corruption" (Digital Culture, Media and Sport Committee 2019, 70). Topics such as anti-NATO sentiment, protest movements, and anti-corruption are certainly highly political and politicised, yet viewed at this high level it is not clear to what extent they may be considered disinformation. The presupposition that it is easy to define "public harm" leaves the door open for censorship and using "fake news" as a label (Egelhofer and Lecheler 2019) to target legitimate political speech that might actually be expressing dissenting views.

While fake news has been part of public debate for centuries (Burkhardt 2017), the qualitative difference we have observed in the 2010s has been the ease with which fake news can spread on online platforms that are designed to maximise users' attention in order to extract revenue. The dominant liberal narrative on disinformation presupposes that foreign actors, such as Russia, spread misleading and inaccurate information online in order to cause public harm and sow division in the EU (High Representative of the Union for Foreign Affairs and Security Policy 2018). What this liberal narrative does is to present disinformation, first, as a problem of *accuracy* above all and, second, one that is caused by external actors. With respect to accuracy, the issue of disinformation is not as clear-cut as "real" versus "fake" news. Recent academic studies of fake news websites in the US context, for

instance, have shown that only a few of the news items published on them can be classified as completely fake, while most involve genre-blending, mixing sensationalism, click-bait, and hyperpartisan political content (Mourão and Robertson 2019). Furthermore, the "accuracy" narrative on disinformation tends to ignore the extent to which the supply of disinformation is driven by economic motives: "fake news" content can be a profitable way for advertising-based social networks to encourage users' attention and thus increase advertising revenues.

With respect to the actors driving the problem, the liberal narrative also tends to ignore that the rising problem in EU politics is actually bottom-up propaganda by domestic far-right actors such as Politically Incorrect News in Germany or VoxNews in Italy that spread highly biased, but not necessarily untrue, political content (Rone 2019). We should not forget that for the rising far-right movement in Europe disinformation is actually spread by mainstream media, as evidenced in the "lying press" chant featured prominently in far-right mobilisations in Dresden, Germany, and beyond (Berntzen and Weisskircher 2016). Thus, the far right offers its own "alternative" media online.

Finally, as has already been noted, the nature and extent of the harms caused by disinformation remain unclear. There is still no conclusive research on the effects of disinformation on voting patterns, either in the United States or in the EU (Nyhan 2019), bringing into question the rhetoric around the issue. Disinformation may be a problem, and there is a consensus that there is a problem, but there is neither consensus nor clarity about what exactly the problem is – is it foreign disinformation, or foreign propaganda, or domestic disinformation, or propaganda, full stop? What effects does it have? The problem is multifaceted, with nuanced effects, which just makes it even more difficult to address in the absence of a solid legal basis.

The implications of all these difficulties around defining disinformation and the resulting potential for undesired censorship are crucial obstacles for securing the legitimacy of democratic government intervention in this area. They are also a key reason that EU regulation in this field to date has tended to take a light touch in the EU and most of its member states. In the next section, we provide an overview of existing public efforts to regulate disinformation before discussing the same issue from the perspective of private actors in the section on preemptive and conflictual cooperation.

Power and legitimacy as limiting factors for EU online disinformation regulation

Different EU states and EU institutions have opted for very different strategies to deal with disinformation. As a result, the current regime of regulation of disinformation has been quite complicated, with no common unifying strategy. While some strategies have involved greater degrees of interventions by the state, in none of the cases considered have states simply told companies what to do. And in all cases, both the capacity of the state to implement its preferred strategy and the need for democratic legitimation with respect primarily to censorship fears have limited the actions they were able to undertake.

One of the first proactive attempts to deal with disinformation in the current context was initiated by the European Council in the aftermath of the Russian military intervention in Crimea in 2014. Created in March 2015, the EastStratComForce focused on proactive communication to support EU delegations in six countries from the EU's Eastern neighbourhood – Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine, and Russia itself. The plan's goal was to provide alternative sources of information different from Russia's sources, communicate and promote "EU Policies and Values", support independent media, and increase awareness of "disinformation activities by external actors" (Jozwiak 2015). Among the products of the EastStratComForce is the fact-checking website EUVsDisinfo (https://euvsdisinfo.eu), which regularly publishes fact checks and flags perceived "disinformation". Nevertheless, the EUVsDisinfo project raised substantial controversy when three Dutch media outlets sued the EU because the fact-checker wrongly accused them of spreading disinformation (Nijeboer 2018). After receiving the subpoena, EUVsDisinfo removed the three articles from their database without informing the relevant media and without providing information about the retraction or apologising for the mistake (Nijeboer 2018). The website continues to function as of July 2020, but as a result of this case it now focuses on fact-checking news produced outside of Europe (BBC Trending 2019). This case demonstrates clearly that fact-checking as a regulatory practice is only as effective as the complaints are accurate and based on clear criteria. In the absence of democratic participation in defining disinformation and a clear consensus on what disinformation is, attempts to remove content flagged as disinformation risks raising serious fears over censorship, threatening the policy's legitimacy.

Aware of such democratic legitimacy challenges with respect to regulating disinformation, the European Commission adopted a more careful approach and attempted to involve different groups in both defining and addressing the problem of disinformation. Such an approach followed the long-established tradition of decentred regulation of the internet, in which private actors have a key role. In late 2017, the Commission announced the creation of a High-level Expert Group that gathered 40 representatives of social media platforms and media organisations, citizens, civil-society organisations, and experts such as journalists and academics to tackle the issue (High Level Group on Fake News and Online Disinformation 2018a). Furthermore, the Commission tasked with drafting a self-regulatory code of practice a multistakeholder forum on online disinformation, composed of online platforms, leading social networks, advertisers, and advertising agencies (Multistakeholder Forum 2018). The code of practice on Disinformation was signed by Facebook, Google, Twitter, Mozilla, and various trade associations, such as the European Association of Communication Agencies, the Interactive Advertising Bureau Europe, and the World Federation of Advertisers. The signatories committed to taking actions in the following five areas:

> Disrupting advertising revenues of certain accounts and websites that spread disinformation; Making political advertising and issue based advertising more transparent; Addressing the issue of fake accounts and online bots;

> Empowering consumers to report disinformation and access different news sources, while improving the visibility and findability of authoritative content; [and] Empowering the research community to monitor online disinformation through privacy-compliant access to the platforms' data.
>
> (Lomas 2018)

In addition to this code of practice, on 5 December 2018 the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the EU's Action Plan Against Disinformation that focused on improved detection; coordinated response; online platforms and industry; and raising awareness and empowering citizens in order to build up the EU's capabilities and strengthen cooperation between member states and the EU (High Representative of the Union for Foreign Affairs and Security Policy 2018). As an implementation of the action plan, the European Commission also launched the European Observatory against Disinformation, bringing together fact-checkers, media organisations, researchers, social media innovators, and policy makers from across the EU. Several campaigns on digital literacy were also launched including the All-Digital Week, held the week of 25 March 2019 (All Digital 2019).

All things considered, it is quite clear from these actions that the Commission refrained from strong unilateral regulation and actively tried to include private companies in defining what is to be regulated and the regulation process itself. This more light-touch approach when it comes to regulating disinformation is in clear contrast to the multiple fines the European Commission imposed on Google for breaking competition rules, for example, in a series of antitrust cases (Scott 2019). Instead of applying unilateral pressure in the case of disinformation as well, the commission acknowledged the legitimacy problems it faces there and reverted to well-known multistakeholder approaches from the past.

At the member-state level, big states encountered the same problems of legitimacy as the Commission and were often accused of censorship by domestic actors, while smaller states had to contend with serious capacity problems that often made them opt for less ambitious strategies focused primarily on media literacy and educating citizens above all. One of the big EU member states that took the lead in regulating disinformation and faced a huge societal backlash was France. On 20 November 2018, five days after Macron's IGF speech, the French Parliament passed a law against the manipulation of information. The law's purpose was to enact stricter rules on the media during electoral campaigns and, more specifically, in the three months preceding any vote (Fiorentino 2018). According to the law, candidates and political parties would be able to appeal to a judge to help stop "false information" and require tech platforms to remove the targeted information within 48 hours (Fiorentino 2018; Rici 2018). Platforms were obliged by the state to cooperate and promote transparency about how their algorithms function, promote content from mainstream press agencies, remove fake accounts that propagate massive misinformation, disclose information about sponsored content, including identity of individuals or organisations that promoted it, and promote media literacy initiatives (Rici 2018).

The law provoked a huge backlash in both the French Senate and French society at large. Before Parliament accepted the law, the French Senate rejected it twice, pointing to the difficulty of ascertaining the veracity of information within 48 hours and the potential dangers arising from the removal of lawful information (Boring 2018). Only a week after the law was approved, more than 50 senators from the French centre-right Republican Party (LR) and the Centrist Union group appealed to the French Constitutional Court over the law, claiming that it fails the principle of proportionality and enters in conflict with the existing penal code (Rici 2018). Furthermore, opposition parties strongly opposed the law on grounds of being "liberticidal", according to the far-right politician Marine Le Pen, or grossly overlooking systemic problems in the media sphere, according to the far-left politician Jean-Luc Mélenchon (ibid).

The United Kingdom encountered similar accusations of censorship with regard to its 2019 consultation paper, "Online Harms White Paper." It proposed a new regulatory model including a statutory "duty of care," a contextual obligation "to exercise reasonable care and/or skill to avoid the risk of injury to relevant others" (Woods 2019, 7). According to an analysis by the digital-rights groups Access Now and the European Digital Rights Initiative (Access Now and EDRi 2019), the duty of care, combined with the prospect of fines for companies, creates the incentives for them to block "legal but harmful" content – that is, content that may cause societal harm but might not be against the law. What is more, to make this possible, companies could opt for content-filtering measures that could result in monitoring of information shared on online platforms, with the boundary between specific and general monitoring being difficult to establish in practice (Woods 2019, 16). Such large-scale monitoring could also illegitimately restrict freedom of expression and lead to online censorship (Woods 2019). As seen in both the examples of France and the UK, disinformation is notoriously difficult to define and getting it wrong easily opens the way to accusations of disproportional actions, censorship, and even abuse of power, thus eroding the legitimacy of any proposed legislation. This is likely not what Macron meant when discussing offering an alternative to both the "Chinese" and the "Californian" model.

Apart from these initiatives of France, the UK, and the EU as a whole, few other countries have undertaken such concerted efforts to convince internet giants to cooperate on disinformation-related issues. Indeed, it remains uncertain to what extent they could successfully implement this type of regulatory framework considering the market power of the US-based corporations, a challenge that Stadnik recognises in her chapter. Most EU member states, in fact, have preferred more proactive and citizen-oriented measures to counter disinformation. Italy set up an online portal where citizens could report misinformation to the police, while Sweden and Spain set up task forces (Funke 2019). Belgium and the Netherlands, on the other hand, initiated media literacy campaigns very much in line with one of the recommendations in the European Action Plan against Disinformation (ibid). Many smaller states lacked the ambition to initiate any proactive measures against disinformation at all.

All in all, if we could speak of the "return of the state" in regulating powerful US companies, it has been the return of the big state. In a move that could be described as an attempt to increase digital sovereignty, EU institutions and some big EU member states have tried to regain control over the flow of information within and across their borders through legislation or control over private intermediaries. But even large, high-capacity states such as France and the UK received a lot of criticism for their efforts and were only partially successful in their attempts to implement their preferred disinformation-regulation frameworks. On the other hand, the EU Commission, also not lacking in capacity, chose to remain cautious in the implementation of its plans and ended up working in close collaboration with other actors in a multistakeholder approach very much in line with the decentred way it had previously followed in the area of internet governance.

The chapter describes in more detail the patterns of preemptive and conflictual cooperation between public and private actors in internet regulation in the next section.

Preemptive and conflictual cooperation

While this chapter has discussed regulation mainly from the perspective of public actors so far, private tech companies' cooperation in combatting disinformation should not be taken as given and non-problematic. Some analysts have suggested that Facebook's readiness to cooperate in regulating disinformation and beyond stems more from public relations considerations than from a deep-seated change of attitude (Scott 2018). While their lobbying strategy until now has been to avoid regulation at all cost, tech firms that have reached monopoly status have realised that their best strategy in the current public climate is *preemptive cooperation* – participating in the lawmaking process in order to end up with laws that are as weak and flexible as possible.

There are multiple examples of platforms' strategies of preemptive cooperation in the EU context. To begin with, participants in the High-Level Group tasked with helping to prevent the spread of disinformation have complained that representatives of Facebook and Google undermined the work of the group and opposed proposals that would have forced them to be more transparent about their business models (Schmidt and Nivet 2018). Monique Goyens, the director of the European Consumer Association, suggested that experts were blackmailed to leave aside the important question of whether tech platforms' business models (based on the use of algorithms to ensure that certain types of content go viral) were crucial in helping disinformation to spread (ibid). The threat was that if discussions about competition policy tools were pushed too far, Facebook could stop its funding for journalistic and academic projects in which some of the High-Level Group experts participated. In other words, Facebook tried to use academic and fact-check funding as a bargaining chip in order to avoid more fundamental questioning of its operations.

Such attempts to move discussions on disinformation away from the topic of platforms' business models is extremely problematic since these business models

have been among the main causes for the rise of disinformation (Access Now and EDRi 2019). The ascent of "attention merchants" (Wu 2016) such as Facebook, Twitter, and Google and their advertising empires has gone hand in hand with the demise of traditional media that have lost advertising revenue and have decreased their investment in investigative journalism, special correspondents, and local news, thus lowering the quality of their content in what has been described as the "de-democratising of news" (Fenton 2012). Not surprisingly, this lowering of journalistic quality has led to a further erosion of public trust in media. What's more, tech platforms and search engines have weakened the direct relationship between readers and publishers: Over half of the combined sample of the Reuters Digital News Report (55 percent) "prefer to access news through search engines, social media, or news aggregators, interfaces where large tech companies typically deploy algorithms rather than editors to select and rank stories" (Newman 2019, 13). This is particularly problematic considering that the very business model of platforms emphasises the distribution of viral content that drives conversation, regardless of whether that content is accurate or not or hate speech or not (Bogost 2019; Wu 2016). Facebook's bottom line is not concerned with whether information is true or false, but with the distinction between content that captures users' attention and content that does not. What social media platforms achieved by being actively involved in the process of defining disinformation in the EU was to devise solutions to the problem that leave as untouched as possible their business models, which are an important reason that the disinformation problem, as it is perceived in the EU, exists in the first place.

Apart from ignoring the elephant in the room, the solutions internet giants offered in terms of content moderation online were quite problematic in themselves – they took place with little oversight or transparency and on the basis of either automated content detection or outsourced fact-checking work (Fisher 2018; Tusikov 2017). Both Facebook and Twitter invested in cost-efficient tech solutions to deal with disinformation. Nevertheless, these efforts revealed the inadequacy of algorithmic approaches to complex societal and media problems. Facebook's tweak of its algorithm from January 2018 that promoted more personal content at the expense of media content threatened the existence of independent alternative media, highly dependent on the platform for distribution (Rone 2018). In an extreme case, Twitter identified as Russian bots and suspended the accounts of multiple Bulgarian users simply because they were using the Cyrillic alphabet. The fact that more countries than Russia use Cyrillic (not to mention that not all Russian accounts are bots) was overlooked both by the designers of the algorithm and by the algorithm as a blunt tool that silenced multiple users just because of the alphabet they happen to use (Savov 2018).

By engaging in preemptive cooperation, platforms avoided questioning of their business model and got the freedom to experiment with solutions that did not cost them too much. But that also meant that the solutions proposed were far from the best for the public, both in terms of legitimacy and in terms of efficiency. For instance, the blunt algorithmic methods to detect disinformation preferred by platforms were not only a suboptimal way to identify cases of disinformation

online with many false-positives but also led to the removal of content without judicial oversight. Ultimately, the code of practice ceded too much power to big tech platforms, with insufficient public oversight or accountability mechanisms (Farrand and Carrapico 2013; Gillespie 2018; Gorwa 2019; Tusikov 2017).

But platforms engaged not only in preemptive cooperation. Sometimes, they flexed their power and entered in open conflict with regulators, subverting proposed regulations by turning them against the regulators themselves. This is what we call in this chapter conflictual cooperation. For example, in April 2019, Twitter blocked a social media campaign by the French government encouraging people to vote. The reason was that Twitter was required by the new French law to provide information on who had sponsored the ad and with what amount of money, but it had not yet updated its services to do this. Thus, the company preferred not to invest the resources to change its policies at that time and blocked the campaign outright (Tidman 2019). In the wake of the 2019 European elections, it turned out that European parties could not have EU-wide communication campaigns on Facebook due to code of practice rule that advertisers should be registered in the country in which they advertise (Alemanno 2019). These two cases are perfect examples of conflictual cooperation that show clearly that in situations of decentred regulation, conflict between actors with diverging interests is subdued but rarely completely ruled out.

To be sure, frictions arise not only in the relations between tech platforms and institutions but also in the relations between civil society and institutions. While the EU has been more than happy to support fact-checkers, many fact-checkers have been wary of co-optation and of being used by EU institutions for political purposes (Funke 2019). Thus, cooperation between nongovernmental organisations (NGOs) and public institutions has also occasionally assumed the character of conflictual cooperation. When it comes to relations between NGOs and tech platforms, cooperation between them has been encouraged by public regulators and has been welcomed by platforms, which are happy to outsource fact-checking whenever possible. Tech platforms have engaged in preemptive cooperation with civil society and academics by funding projects that do not threaten the essence of their business model. For their part, civil society and academics have had frictions with tech platforms mainly with regard to the latter's famous secrecy regarding crucial aspects of their operations. For example, NGOs and scientists have had serious problems in trying to receive data for research from platforms despite attempts to improve coordination (Gibney 2019).

Both the preemptive and the conflictual cooperation between private and public actors show that rather than simply implementing governments' agendas and rules, private actors, most notably tech platforms, have engaged in setting the terms of debate and the rules themselves. EU institutions attempted to regain digital sovereignty with regard to online disinformation coming from Russia by counting on US private platforms such as Facebook, Google, and Twitter and non-elected NGOs to regulate this content. Thus, they ended up caught between a rock and a hard place.

Discussion and conclusion

This chapter has shown that despite the rhetoric of French President Macron in his 2018 IGF speech and Mark Zuckerberg's professed enthusiasm for regulation, in the field of disinformation there has been no shift to strong state legislation and control of private actors by public institutions. To begin with, due to their lack of regulatory capacity and limited ability to compel corporate compliance, smaller EU member states have engaged relatively little in attempting to regulate internet giants. Big EU member states such as France, on the other hand, have indeed tried to introduce strict laws to combat fake news, but these attempts were met with general criticism and accusations of censorship and lack of due process. Finally, aware of the legitimacy challenges ahead, the European Commission did not emulate the French state-led approach focused on legislation but opted instead for decentred regulation, in which private actors partnered with public institutions, often on their own terms and with varying degrees of cooperation. Within this practice of decentred regulation, corporations such as Facebook and Google engaged in complex strategies of preemptive and conflictual cooperation, both of which were suboptimal in terms of realising effective regulation of disinformation in the public interest.

There are two important questions that follow from these developments in the regulation of online disinformation in the EU. The first, narrower question is how can we achieve better regulation of online disinformation in the EU? Second, and related to this, is the broader question of what insights on global internet regulation we can get from the particular case of regulation of disinformation in the EU. Both of these questions touch upon the issues of power and legitimacy that we discussed in this chapter.

Starting with the first question, it is clear that current EU policies have given too much weight to US tech giants to define both what the problems with disinformation are and how to propose solutions, while other actors such as media regulators have remained largely neglected. Media regulation expert Iva Nenadic has emphasised that in order to regulate disinformation more effectively, we need more oversight of tech platforms and a better understanding of their practices of content moderation, both those undertaken by algorithms and those outsourced to workers in low-labour-cost countries.[1] In addition, Nenadic has emphasised the need to give more roles to media authorities that already exist in EU member states and enhance their capacities and cooperation with each other across countries, since disinformation is not a single-country phenomenon but crosses borders easily. To be sure, small EU member states cannot miraculously increase their power vis-à-vis internet giants, but a better understanding of how these companies operate combined with better coordination among EU member states would allow states to address the problem much more comprehensively and adequately. While one small state cannot make Facebook change its policy, a commonly negotiated strategy backed by all EU member states has much greater chances to succeed and thus change Facebook's policies also in smaller states.

Another important step for achieving more effective regulation of disinformation is related to expanding the scope of current measures. Most public attention so far, and this chapter is not an exception, has focused on political disinformation, especially in the run-up to elections. But disinformation is a much more complex phenomenon that goes beyond elections. Jules Darmanin, the coordinator of the FactCheckEU initiative, has emphasised the need to focus on more types of disinformation, especially content related to climate change denial or public health, such as anti-vax conspiracies.[2] The boom of disinformation in relation to the Covid-19 pandemic is another case in point. What's more, more research and investigative reporting is needed on the funding schemes of "alternative" media online.

Third, regulating disinformation should focus not only on the symptoms but also on the root causes for the current media malaise. Trying to regulate disinformation without questioning the business models of tech giants and their monopoly power is doomed to fail. One might go even further than the media sphere and argue that the spread of news classified by the EU as disinformation cannot be understood without paying attention to the radical right movement that has risen to prominence in the aftermath of the 2008 Economic Crisis (Berntzen and Weiskircher 2016; Gattinara and Pirro 2019; Rone 2019). Removing content and teaching media literacy can hardly change the political opinions of an already highly politicised segment of the population.

Fourth, the current configuration of decentred regulation as observed in the actions of the EU Commission reveals state/non-state dynamics in terms of preemptive and conflictual cooperation strategies. The EU's anti-disinformation campaign in this context might curb the spread of disinformation but at too high a cost. The ever-present danger of state censorship is currently made even stronger by giving censorship power also to big tech platforms with dubious methodology for identifying problematic content and no democratic mandate. This is problematic in itself but it is also troubling because the attempts of the EU and its member states to regulate disinformation have been instrumentally used as a justification for harsh laws against "fake news" in authoritarian countries such as Russia and Singapore (Funke 2019). The EU has traditionally prided itself with being a soft power that exports high democratic standards across the world. In the case of regulating disinformation, unfortunately the EU example has been far from "best practice".

One possible solution to these issues involves confronting the thorny question of what counts as disinformation in the first place. Disinformation, in a sense, is in the eye of the beholder, which means that any state definition will require some degree of democratic legitimisation. If the EU and its member states want to get out of the current power and legitimacy impasses in addressing disinformation, and avoid both the Californian and the Chinese models, they could involve the public, the European citizens themselves, in defining the problem and suggesting how to solve it in ways that go beyond current Band-Aid approaches. Some steps have been already made in this direction, but they can be taken much further. The UK's practice of Parliamentary hearings on disinformation, for example, can be expanded with

a more active use of citizen dialogues and citizen consultations, both instruments already used at the European level but often with little effect on policy consequences. Radical proposals might include breaking up tech giants or investing more in ethical innovation in order to design platforms *not* based on exploiting users' attention in order to extract their data. Radical proposals might also have nothing to do with tech platforms but focus on supporting local journalism or more constructive journalism instead (Constructive Journalism Network 2019).

No one knows what proposals might come up and get approval since there have been few inclusive public debates on the issue yet, whether in individual EU member states, or in the EU as a whole. The UK's white paper on online harms has been a welcome exception since it was open to broad public consultation. Public participation could be strengthened through involvement in surveys and focus groups, as well as more innovative forms of citizen participation and deliberation, including public consultations, citizen assemblies, and publicly organised debates, publicised on national mainstream media. More hearings and debates on the issue in the European Parliament but also in national parliaments in each EU country are to be encouraged, as well as more inter-parliamentary cooperation to ensure that there is if not a common then at least a coordinated approach to disinformation in the EU.

In fact, it is precisely this procedural point that goes beyond the narrow question of regulating online disinformation and offers a potential new approach to the field of internet regulation in general. Legitimacy is a central issue to be considered in any attempt to put into practice Macron's call to regulate the internet in a way that goes beyond both the Chinese and the Californian models. If democratic states want to assert their democratic digital sovereignty, a good way to legitimise these attempts would be to encourage much more parliament and citizen participation in discussions on what we want to regulate, how, and why. Legitimacy in democratic states, as discussed in this chapter, is based on democratic participation, popular acceptance of a policy, and efficiency. It is true that proposed solutions to the disinformation problem can be democratically negotiated and still inefficient. Yet, a democratically negotiated regulation can also be much more efficient as citizens will also have ownership of proposed solutions and will not feel arbitrarily censored. Current approaches to disinformation, on the contrary, are neither legitimate nor particularly efficient. We can no longer ignore the striking absence of the "people" when discussing internet regulation, especially considering the increasing demand for popular sovereignty in fields as diverse as trade policy or fiscal policy (Brack, Coman and Crespy 2019). Following this trend, popular and parliamentary sovereignty over digital infrastructure, data, and content could offer the basis for a truly progressive model of digital sovereignty that escapes the pitfalls of the archetypical "Chinese internet" but also the complex and often private interest–driven reality of the "Californian model" of decentred regulation.

At the time of writing the conclusion to this chapter, the coronavirus epidemic is at its peak. EU member states such as Hungary introduced straightforward authoritarian measures to deal with the pandemic including rule by decree, suspension of Parliament and, especially relevant for the chapter, jail terms for up to

five years for "intentionally spreading misinformation that hinders the government response to the pandemic" (Walker and Rankin 2020). It remains to be seen how long-lasting the changes brought about by the epidemic will be. One thing is certain: Considering that both states and internet giants have become more powerful in this situation of emergency, citizen participation and the safeguarding of the democratic process become even more important in order to safeguard both civil liberties and the quality of public debate.

Notes

1 Interview with Iva Nenadic for the current chapter, June 2019.
2 Interview with Jules Darmanin for the current chapter, June 2019.

References

Access Now and EDRi. 2019. *Content regulation – What's the (Online) Harm?* https://edri.org/content-regulation-whats-the-online-harm/. Accessed 5 August 2020.

Alemanno, Alberto. 2019. "Facebook Versus the EU." *Politico*. 24 May. www.politico.eu/article/facebook-european-union-disinformation-elections/. Accessed 5 August 2020.

All Digital. 2019. "Join the Largest Digital Empowerment Campaign in Europe – All Digital Week 2019." *All Digital*. https://all-digital.org/join-all-digital-week-2019/. Accessed 5 August 2020.

Andenas, Mads, and Iris H.-Y. Chiu. 2014. *The Foundations and Future of Financial Regulation*. London: Routledge.

Apuzzo, Matt, and Adam Satariano. 2019. "Russia and Far Right Spreading Disinformation Ahead of EU Elections, Investigators Say." *The Independent*. 12 May. www.independent.co.uk/news/world/europe/eu-elections-latest-russia-far-right-interference-fake-news-meddling-a8910311.html. Accessed 5 August 2020.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R.B.J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–144. https://doi.org/10.1111/ips.12048.

BBC Trending. 2019. "Is Russia Trying to Sway the European Elections?" *BBC News World Service*. 18 May. www.bbc.co.uk/programmes/w3csyvms. Accessed 5 August 2020.

Beetham, David and Christopher Lord (eds.). 1998. *Legitimacy and the European Union*. Longman: Harlow.

Belavusau, Uladzislau. 2012. "Fighting Hate Speech Through EU Law." *Amsterdam Law Forum* 4 (1), 20–35.

Berntzen, Lars Erik, and Manès Weisskircher. 2016. "Anti-Islamic PEGIDA Beyond Germany: Explaining Differences in Mobilisation." *Journal of Intercultural Studies* 37 (6): 556–573. https://doi-org.proxy.library.brocku.ca/10.1080/07256868.2016.1235021.

Black, Julia. 2001. "Decentereing Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-regulatory World'." *Current Legal Problems* 54 (1): 103–146.

Bogost, Ian. 2019. "Facebook's Dystopian Definition of 'Fake'." *The Atlantic*. 28 May. www.theatlantic.com/technology/archive/2019/05/why-pelosi-video-isnt-fake-facebook/590335/. Accessed 5 August 2020.

Boring, Nicholas. 2018. "France: Senate Rejects 'Fake News Bills'." In *Global Legal Monitor*. United States: Library of Congress. 24 September. www.loc.gov/law/foreign-news/article/france-senate-rejects-fake-news-ban-bills/. Accessed 5 August 2020.

Brack, Nathalie, Ramona Coman, and Amandine Crespy. 2019. "Unpacking Old and New Conflicts of Sovereignty in the European Polity." *Journal of European Integration* 41 (7): 817–832. https://doi.org/10.1080/07036337.2019.1665657.

Burkhardt, Joanna. 2017. "Combating Fake News in the Digital Age." *Library Technology Reports* 53 (8).

Buxton, Nick. 2019. *Multistakeholderism: A CRITICAL LOOK. Workshop Report: Corporate Power Project*. Transnational Institute. March. www.tni.org/files/publication-downloads/multistakeholderism-workshop-report-tni.pdf. Accessed 5 August 2020.

Cadwalladr, Carole. 2017. "The Great British Brexit Robbery: How Our Democracy Got Hijacked." *The Guardian*. 7 May. www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. Accessed 5 August 2020.

Christiano, Tom. 2012. "Authority." *Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/entries/authority/. Accessed 5 August 2020.

Constructive Journalism. 2019. *Constructive Journalism Network*. http://constructivejournalism.network/. Accessed 5 August 2020.

Couture, Stephane, and Sophie Toupin. 2019. "What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?" *New Media & Society* 21 (10): 2305–2322. https://doi.org /10.1177%2F1461444819865984.

Department for Digital, Culture, Media & Sport and Home Office. 2019. *Online Harms White Paper*. London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf. Accessed 5 August 2020.

Digital, Culture, Media and Sport Committee. 2019. *Disinformation and 'Fake News': Final Report*. Eighth Report of Session 2017–19. United Kingdom: House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf. Accessed 5 August 2020.

Donders, Karen, Hilde Van den Bulck, and Tim Raats. 2019. "The Politics of Pleasing: A Critical Analysis of Multistakeholderism in Public Service Media Policies in Flanders." *Media, Culture & Society* 41 (3): 347–366. https://doi.org/10.1177%2F0163443718782004.

Egelhofer, Jana Laura, and Sophie Lecheler. 2019. "Fake News as a Two-Dimensional Phenomenon: A Framework and Research Agenda." *Annals of the International Communication Association* 43 (2): 97–116. https://doi.org/10.1080/23808985.2019.1602782.

Farrand, Benjamin, and Helena Carrapico. 2013. "Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators." *Journal of Information Technology & Politics* 10 (4): 357–368. https://doi.org/10.1080/19331681.2013.843920.

Fenton, Natalie. 2012. "De-Democratizing the News? New Media and the Structural Practices of Journalism." In *Handbook of Global Online Journalism*, edited by Eugenia Siapera and Andreas Veglis, 119–134. Chichester: Wiley & Blackwell.

Fiorentino, Michael-Ross. 2018. "France Passes Controversial 'Fake News' Law." *Euronews*. 22 November. www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law. Accessed 5 August 2020.

Fisher, Mark. 2018. "Inside Facebook's Secret Rulebook for Global Political Speech." *The New York Times*. 27 December. www.nytimes.com/2018/12/27/world/facebook-moderators.html. Accessed 5 August 2020.

Funke, Daniel. 2019. *A Guide to Anti-Misinformation Actions Around the World*. *Poynter*. www.poynter.org/ifcn/anti-misinformation-actions/#germany. Accessed 5 August 2020.

Gattinara, Pietro Castelli, and Andrea L.P. Pirro. 2019. "The Far Right as Social Movement." *European Societies* 21 (4): 447–462. https://doi.org/10.1080/14616696.2018.1494301.

Gibney, Elizabeth. 2019. "Privacy Hurdles Thwart Facebook Democracy Research." *Nature*. 3 October. www.nature.com/articles/d41586-019-02966-x. Accessed 5 August 2020.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press.

Gorwa, Robert. 2019. "What Is Platform Governance?" *Information, Communication & Society* 22 (6): 854–871. https://doi.org/10.1080/1369118X.2019.1573914.

High Level Group on Fake News and Online Disinformation. 2018a. *High-Level Group on Fake News and Online Disinformation: Event Report*. 6 February. https://ec.europa.eu/digital-single-market/en/news/high-level-group-fake-news-and-online-disinformation. Accessed 5 August 2020.

High Level Group on Fake News and Online Disinformation. 2018b. *A Multi-Dimensional Approach to Disinformation*. Brussels: European Commission. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271. Accessed 5 August 2020.

High Representative of the Union for Foreign Affairs and Security Policy. 2018. *Action Plan Against Disinformation*. Brussels: European Commission. https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf. Accessed 5 August 2020.

Hill, Jonah. 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders." *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*. https:/doi.org/10.2139/ssrn.2430275.

Iusmen, Ingi, and John Boswell. 2017. "The Dilemmas Of Pursuing 'Throughput Legitimacy' Through Participatory Mechanisms." *West European Politics* 40 (2): 459–478. https://doi.org/10.1080/01402382.2016.1206380.

Jozwiak, Rikard. 2015. "EU to Counter Russian Propaganda by Promoting 'European Values'." *The Guardian*. 25 June. www.theguardian.com/world/2015/jun/25/eu-russia-propaganda-ukraine. Accessed 5 August 2020.

Kayali, Laura. 2019. "Inside Facebook's Fight against European Regulation." *Politico*. 23 January. www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/. Accessed 5 August 2020.

Kukutai, Tahu, and John Taylor. 2016. *Indigenous Data Sovereignty: Toward an Agenda*. Canberra: ANU Press.

Leiser, Mark, and Andrew Murray. 2017. "The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies." In *The Oxford Handbook of Law, Regulation and Technology*, edited by Roger Brownsword, Eloise Scotford, and Karen Yeung. Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199680832.013.28.

Lomas, Natasha. 2017. "Germany's Social Media Hate Speech Law is Now in Effect." *Techcrunch*. https://techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/. Accessed 5 August 2020.

Lomas, Natasha. 2018. "Tech and ad Giants Sign Up to Europe's First Weak Bite at 'Fake News'." *Techcrunch*. https://techcrunch.com/2018/09/26/tech-and-ad-giants-sign-up-to-europes-first-weak-bite-at-fake-news/. Accessed 5 August 2020.

Macron, Emmanuel. 2018. *IGF 2018 Speech by French President Emmanuel Macron*. www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron. Accessed 5 August 2020.

Margolin, Jack. 2016. "Russia, China and the Push for Digital Sovereignty." *The Global Observatory*. https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/. Accessed 5 August 2020.

McNaughton, Anne, and Stewart Lockie. 2017. "Private Actors in Multi-Level Governance: GLOBALG.A.P. Standard-Setting for Agricultural and Food Products." In *Multi-level Governance: Conceptual Challenges and Case Studies from Australia*, edited by Katherine A. Daniell and Adrian Kay, 385–402. Canberra: ANU Press.

Meyer, David. 2019. "Europe Is Starting to Declare Its Cloud Independence." *Fortune*. 30 October. https://fortune.com/2019/10/30/europe-cloud-independence-gaia-x-germany-france/. Accessed 5 August 2020.

Mooney, Brian. 2019. "Coming Soon: the EU's Ministry of Truth?" *Campaign for an Independent Britain*. 8 July. https://campaignforanindependentbritain.org.uk/coming-soon-the-eus-ministry-of-truth/. Accessed 5 August 2020.

Mourão, Rachel R., and Craig T. Robertson. 2019. "Fake News as Discursive Integration: An Analysis of Sites That Publish False, Misleading, Hyperpartisan and Sensational Information." *Journalism Studies* 20 (14): 2077–2095. https://doi.org/10.1080/1461670X.2019.1566871.

Multistakeholder Forum. 2018. *Meeting of the Multistakeholder Forum on Disinformation: Event Report*. European Commission. https://ec.europa.eu/digital-single-market/en/news/meeting-multistakeholder-forum-disinformation. Accessed 5 August 2020.

Newman, Nick. 2019. "Executive Summary and Key Findings of the 2019 Report." *Reuters Digital News Report*. www.digitalnewsreport.org/survey/2019/overview-key-findings-2019/. Accessed 5 August 2020.

Nijeboer, Arjin. 2018. "Why the EU Must Close EU Vs Disinfo." *EU Observer*. 28 March. https://euobserver.com/opinion/141458. Accessed 5 August 2020.

Nyhan, Brendan. 2019. "Why Fears of Fake News Are Overhyped." *Medium*. 4 February. https://medium.com/s/reasonable-doubt/why-fears-of-fake-news-are-overhyped-2ed9ca0a52c9. Accessed 5 August 2020.

Powers, Shawn, and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of internet Freedom*. Chicago: University of Illinois Press.

Rici, Alexander Damiano. 2018. "French Opposition Parties Are Taking Macron's Anti-Misinformation Law to Court." *Poynter*. 4 December. www.poynter.org/fact-checking/2018/french-opposition-parties-are-taking-macrons-anti-misinformation-law-to-court/. Accessed 5 August 2020.

Rone, Julia. 2018. "Collateral Damage: How Algorithms to Counter Fake News Threaten Citizen Media in Bulgaria." *LSE Media Project*. 18 June. https://blogs.lse.ac.uk/mediapolicyproject/2018/06/18/collateral-damage-how-algorithms-to-counter-fake-news-threaten-citizen-media-in-bulgaria/. Accessed 5 August 2020.

Rone, Julia. 2019. "Why Talking About 'Disinformation' Misses the Point When Considering Radical Right 'Alternative' Media." *LSE Media Project*. 3 January. https://blogs.lse.ac.uk/mediapolicyproject/2019/01/03/why-talking-about-disinformation-misses-the-point-when-considering-radical-right-alternative-media/. Accessed 5 August 2020.

Savov, Vlad. 2018. "Twitter is Treating Bulgarians Tweeting in Cyrillic Like Russian Bots." *The Verge*. 22 May. www.theverge.com/2018/5/22/17380630/twitter-moderation-cyrillic-russian-bots. Accessed 5 August 2020.

Schleifer, Philip. 2019. "Varieties of Multi-Stakeholder Governance: Selecting Legitimation Strategies in Transnational Sustainability Politics." *Globalizations* 16 (1): 50–66. https://doi.org/10.1080/14747731.2018.1518863.

Schmidt, Nico, and Daphné Dupont-Nivet. 2018. "Facebook and Google Pressured EU Experts to Soften Fake News Regulations, Say Insiders." *Open Democracy*. 21 May. www.opendemocracy.net/en/facebook-and-google-pressured-eu-experts-soften-fake-news-regulations-say-insiders/. Accessed 5 August 2020.

Scholte, Jan Aart. 2013. "Civil Society and Financial Markets: What is Not Happening and Why." *Journal of Civil Society* 9 (2): 129–147. https://doi.org/10.1080/17448689.2013.788925.

Scott, Mark. 2018. "How Big Tech Learned to Love Regulation." *Politico*. 11 November. www.politico.eu/article/google-facebook-amazon-regulation-europe-washington-brussels-privacy-competition-tax-vestager/. Accessed 5 August 2020.

Scott, Mark. 2019. "Europe Fines Google €1.49B in Third Antitrust Case." *Politico*. 20 March. www.politico.eu/article/europe-google-margrethe-vestager-adsense-antitrust-competition-fine/. Accessed 5 August 2020.

Stallman, Richard M. 2006. "Did You Say 'Intellectual Property'? It's a Seductive Mirage." *Policy Futures in Education* 4 (4): 334–336. https://doi.org/10.2304%2Fpfie.2006.4.4.334.

Tandoc, Edson C., Darren Lim, and Richard Ling. 2020. "Diffusion of Disinformation: How Social Media Users Respond to Fake News and Why." *Journalism* 21 (3): 381–398. https://doi.org/10.1177%2F1464884919868325.

Tidman, Zoe. 2019. "Twitter Rules out French Government Advertising over Anti-Fake News Law." *The Independent*. 3 April. www.independent.co.uk/news/world/europe/twitter-france-fake-news-europe-elections-a8852731.html. Accessed 5 August 2020.

Tucker, Joshua A, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. 2018. *Political Polarization, and Political Disinformation: A Review of the Scientific Literature*. William + Flora Hewlett Foundation. March. https://hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf. Accessed 5 August 2020.

Tusikov, Natasha. 2017. *Chokepoints: Global Private Regulation on the Internet*. Berkeley, CA: University of California Press.

Viner, Katharine. 2016. "How Technology Disrupted the Truth." *The Guardian*. 12 July. www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth. Accessed 5 August 2020.

Voermans, Wim, Josephine Hartmann, and Michael Kaeding. 2014. "The Quest for Legitimacy in EU Secondary Legislation." *The Theory and Practice of Legislation* 2 (1): 5–32. https://doi.org/10.5235/2050-8840.2.1.5.

Volpicelli, Gian. 2019. "All That Is Wrong with UK's Crusade Against Online Harm." *Wired*. 9 April. https://wired.co.uk/article/online-harms-white-paper-uk-analysis. Accessed 5 August 2020.

Wagner, Ben. 2013. "Governing Internet Expression: How Public and Private Regulation Shape Expression Governance." *Journal of Information Technology & Politics* 10 (4): 389–403. https://doi.org/10.1080/19331681.2013.799051.

Walker, Shaun, and Jennifer Rankin. 2020. "Hungary Passes Law That Will Let Orbán Rule by Decree." *The Guardian*. 30 March. www.theguardian.com/world/2020/mar/30/hungary-jail-for-coronavirus-misinformation-viktor-orban. Accessed 5 August 2020.

Woods, Lorna. 2019. "The Duty of Care in the Online Harms White Paper." *Journal of Media Law* 11 (1): 6–17. https://doi.org/10.1080/17577632.2019.1668605.

Wu, Tim. 2016. *The Attention Merchants: The Epic Scramble to Get Inside our Heads*. New York: Penguin Random House.

Zuckerberg, Mark. 2019. "Mark Zuckerberg: The Internet Needs New Rules. Let's Start in These Four Areas." *Washington Post*. 30 March. www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504–521a-11e9-a3f7–78b7525a8d5f_story.html. Accessed 5 August 2020.

9 Varieties of digital capitalism and the role of the state in internet governance

A view from Latin America

Jean-Marie Chenou

Technological change is transforming the global economy. Progress in telecommunications, and particularly the increasingly widespread use of the internet, has strengthened the trend towards the globalisation and transnationalisation of the global economy that marked the end of the 20th century (Gereffi 2001). However, the study of the governance of the technological infrastructure that facilitates the rise of digital capitalism and the analysis of the economic activities that take place on the internet have often been treated as separate issues (for some exceptions, see Fontaine-Skronski and Rioux 2015; Haggart and Jablonski 2017; Simpson 2004; Pickard 2007). Internet governance is generally understood as the management of critical technical resources, without taking into account that technical choices are political and promote certain types of economic arrangements. On the other hand, the burgeoning literature on the current transformation of capitalism largely ignores the governance of the technical underpinnings of the network. This "mutual neglect" is a recent construct. Twenty years ago, Schiller (1999) coined the term "digital capitalism" in order to analyse both technological and economic change in the early years of digitisation:

> In addition to broadening the effective reach of the marketplace, cyberspace is making feasible what Edward S. Herman calls a "deepening of the market." . . . Networks are directly generalising the social and cultural range of the capitalist economy as never before. That is why I refer to this new epoch as one of *digital capitalism*.
>
> (Schiller 1999, xiv)

However, as internet governance studies developed as a specialised field over the last two decades, they largely departed from Schiller's comprehensive perspective. This chapter seeks to reconcile internet governance studies and the analysis of the regulation of digital capitalism by focusing on the role of the state as a key actor in both realms. Although they have rarely been treated as such in academic accounts, internet governance debates have always been about organising the technical infrastructure of global digital capitalism. This chapter argues that the role of the state in the management of internet critical resources and in the regulation of the digital economy have been part of a single global public policy

DOI: 10.4324/9781003008309-13

debate since the first attempts to create an institutional framework to govern the internet in the 1990s in the United States. The analysis of the role of the state in internet governance echoes broader debates about the role of state regulation in contemporary capitalism. While the institutionalisation of internet governance in the 1990s epitomised a mix of cyberlibertarian ideals and neoliberal governance (Chenou 2014), different understandings of the role of the state emerged with the globalisation of digital capitalism. The chapter proposes a perspective based on the Varieties of Digital Capitalism (VoDC) in order to study how the role of the state in internet governance and in the regulation of digital capitalism differs from one country to another. Drawing upon comparative capitalism studies, the chapter uses Latin America as a case study to explore the different national translations of the "return of the state" in internet governance and in digital capitalism. The VoDC approach allows for an understanding of the variegated policy responses to digitisation. In the case of Latin America, different models can be outlined, corresponding to a greater or a lesser degree of state intervention that is consistent with longer-term institutional trajectories. As a result, the chapter offers a reflection on the role of the state in internet governance and in the regulation of digital capitalism beyond the first-movers located mostly in the Global North.

This chapter is organised as follows. The first section explores the history of the intertwining of internet governance and the regulation of digital capitalism in the early years of the digital era and the consequences of the globalisation of the internet. The second section analyses the case of the four major economies in Latin America in order to outline different types of state intervention and projection. The conclusion proposes a reflection on the usefulness of the VoDC approach in order to study the role of the state in the digital era in the Global South.

From internet governance to the regulation of digital capitalism

Internet governance entails the management of an essential asset of digital capitalism: the network that enables the exchange of data flows at a global scale. This is why internet governance debates have always included, albeit implicitly, the issue of the economic model facilitated by the network. Internet governance arrangements have been part of the institutional framework that gave rise to contemporary digital capitalism, which is characterised by datafication (West 2019) and platformisation of the economy (Srnicek 2017). While digital capitalism was first imagined and fomented in the US and to a lesser extent in other countries of the Global North, its globalisation has challenged the original governance arrangements and diversified the perspectives on the appropriate role of the state in these arrangements.

The capitalist origins of internet governance

The prehistory of internet governance provides an example of the relationship between technical governance and modes of economic regulation. During the

"protocol wars" of the 1980s, different technical protocols competed to become the single protocol of a global computer network. The triumph of the TCP/IP (Transmission Control Protocol/Internet Protocol) over the OSI (Open Systems Interconnect) was not only a technical choice (Abbate 1999). The OSI was a centralised computer-networking model based on standards developed by the International Telecommunication Union and supported by most governments and monopolistic European telephone companies. As for the TCP/IP networking model supported by the US and computer manufacturers, it allowed for the creation of a decentralised global computer network, where competition between private carriers could thrive. Thus, the TCP/IP model was a better fit for the development of a privatised and deregulated global telecommunications market. The triumph of the TCP/IP was not the victory of a superior technological solution but rather an illustration and reflection of a neoliberal ideology that inspired the worldwide wave of privatisation and deregulation in the telecommunication sector in the 1980s and 1990s.

The dominance of a neoliberal regulation of computer networks, characterised by the systematic adoption of market-driven solutions over direct state regulation, is further illustrated by the first governmental documents about internet governance that were drafted in the United States. The government that pushed for the adoption of the TCP/IP and promoted the early development of the internet soon began to think about the economic potential of the network. In 1997, an interagency working group led by US Vice President Al Gore published a *Framework for Global Electronic Commerce* (US Government 1997). As indicated by the title, the document established the principle of a governance framework for the "Global Information Infrastructure," and particularly for the internet. Its principles – private-sector leadership, avoidance of undue governmental restrictions, minimalist legal environment – strongly and repeatedly reject the legitimacy of state interventionism, while acknowledging the unique nature of the internet and promoting the globalisation of e-commerce. This regulatory model of digital capitalism was summarised as follows:

> Commerce on the Internet could total tens of billions of dollars by the turn of the century. For this potential to be realised fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce. Official decision makers must respect the unique nature of the medium and recognise that widespread competition and increased consumer choice should be the defining features of the new digital marketplace.
>
> (US Government 1997)

This framework was not just targeted at the content layer of the internet. As an illustration of the intertwining of the economic model and the technical management of the network, the document also rejected state intervention in technical

matters. For example, it praised the bottom-up model that had characterised the governance of the network:

> The genius and explosive success of the Internet can be attributed in part to its decentralised nature and to its tradition of bottom-up governance. These same characteristics pose significant logistical and technological challenges to existing regulatory models, and governments should tailor their policies accordingly.
>
> (US Government 1997)

Although the debates eventually involved a number of actors beyond the US government and the technical community that had been responsible for the bottom-up technical governance of the internet (Mueller 2002), the main principles established by the US government were maintained throughout the process (NTIA 1998a, 1998b). Finally, an Internet Corporation for Assigned Names and Numbers (ICANN) was established in 1998 through a Memorandum of Understanding between the US Department of Commerce and the newly created corporation, represented by the dominant stakeholders, mainly from the US private sector and technical community (ICANN and DoC 1998).

The first ICANN bylaws established a private sector–led corporation to manage core technical functions of the internet. State participation was limited to a Governmental Advisory Committee (GAC) that could be notified by the ICANN Board "of any proposal for which it seeks comments" (ICANN 1998, art. VII, section 3a). Originally, the GAC had no right of initiative and issues had to be referred to the GAC by the ICANN Board.[1]

The institutionalisation of internet governance and the principles for the regulation of digital capitalism were both established in the United States within the particular historical context of the 1990s. The role of the state in both cases was marginalised as a matter of policy. This model allowed for the development of the contemporary form of digital capitalism, but as the internet became more globalised and digital capitalism grew widespread, this minimalist-state approach to internet governance began to clash with different visions of the role of the state, as will be discussed later.

The rise of digital capitalism

As the US administration of Bill Clinton expected, the internet soon became an essential vehicle of global capitalist growth. The internet, commercialised as a consequence of the policy interventions in the 1990s, provided the infrastructure upon which digital capitalism developed (Simpson 2004), leading to the recent trend towards datafication and platformisation of the global economy. Recently, an important literature has emerged that outlines the main characteristics of the current technological transformation of the economy towards digital capitalism, described in turn as a fourth industrial revolution (Schwab 2017), data capitalism (West 2019), platform capitalism (Srnicek 2017), or surveillance capitalism

(Zuboff 2019). Focusing on digital capitalism sheds a different light on the evolution of internet governance as more than a technical matter. Digitisation, when viewed in its economic context, emerges as part of the "constant preoccupation" (Harvey 1985, 129) under capitalism to create social and physical (including technological) infrastructures that support the continuous circulation of capital. Indeed, as Marx noted, the continuous circulation of capital in its different forms, from monetary capital through productive and commodity capitals, is essential in the process of the production of surplus value (Marx 1993). This does not mean that digitisation is determined only by the needs of the capitalist system, but rather that it is shaped by the socio-economic context in which it is developed: Digitisation is constantly shaped and steered into playing a role in the organisation of capitalist production. This is not a one-way process: As critical studies of technology note, technology by its nature is "biased but ambivalent" (McCarthy 2018, 72). It is the object of political struggles and even resistance. There are different ways to organise digitisation, although most of them foment the reproduction of capitalist relations. The following section emphasises the role of (national) political institutions understood as the framework that steers the use of technology towards certain forms of reproduction of capitalist relations in a given context.

A perspective on digital capitalism informed by a Marxist conceptualisation of capitalist relations understands technological change as embedded within social structures of accumulation (for an overview, see McDonough, Reich and Kotz 2010; McDonough 2015). In this view, capitalism structurally tends to continue to expand the boundaries of the capitalist system; to increase the size of large corporations and concentrate the ownership of capital; and to change the labour process towards more segmented forms of work and more divided workers (Gordon, Edwards and Reich 1982). Digitisation is thus not only a technological process but also a continuation and deepening of capitalist structures of accumulation.

Finally, the spatial organisation of digitisation is also part of the geopolitics of capitalism. Digitisation cannot be conceptualised as a universal and homogeneous process. Global digital value chains emerge within a globalised capitalist system that is geographically structured. Against this background, the analysis of digitisation in the Global South necessarily takes into account issues of technological and economic dependency.

The globalisation of digital capitalism: towards VoDC

While the characteristics of digital capitalism outlined in the previous section are global in scope, the responses in terms of regulation and institutionalisation differ between regions and among countries within the same region. In order to apprehend the complexity of digital capitalism and the fundamental role of institutions, it is important to analyse the various forms of regulation that emerge (see Mann and Iazzolino 2019, 13). A perspective from Latin America is useful as a way to illustrate the specific challenges faced by the Global South and to de-centre the point of view away from the cradle of digital capitalism in order to analyse the

importance of the state as a key actor in the regulation of digital capitalism and in internet governance.

Since the beginning of the 21st century, research on comparative capitalism has conceptualised the institutional differences in the globalisation process (Hall and Soskice 2001). A comparative capitalism approach insists on the importance of institutions, particularly national institutions, in the emergence of variegated forms of regulation of capitalism and their relative resilience through time. The seminal work by Hall and Soskice (2001) describes the differences between two ideal types of capitalism: the liberal-market economies (LME) epitomised by the United States and the coordinated-market economies (CME) epitomised by Germany. Early research on Varieties of Capitalism (VoC) underestimated the institutional variety in contemporary capitalism and focused on developed countries from the Global North (Rueda and Pontusson 2000; Hancké, Rhods and Thatcher 2007). More recently, comparative capitalism has evolved to globalise its research agenda and to propose new categories of analysis. For example, by introducing the concept of dependent-market economies (Nölke and Vliegenthart 2009), later work in comparative capitalism has stressed the importance of the structures of global capitalism in the analysis of its different institutional forms at the national level. Along these lines, VoC can be studied from the periphery (Fernández, Ebenau and Bazza 2018) in order to complement existing categories and to better understand the role of the state in the organisation of capitalism from a global perspective.

Drawing upon recent strands of research in comparative capitalism, and especially in critical comparative capitalism (Bruff, Ebenau and May 2015), it is possible to look at the same time at the structural transformations towards digital capitalism that are allowed by technological change and to the variety of institutional responses that have resulted. This variety is shaped by global and domestic forces: on the one hand by the geopolitics of digital capitalism and on the other hand by preexisting national institutions. First, digital capitalism is organised hierarchically on a global scale and reproduces colonialist patterns of value extraction (Ávila Pinto 2018). Second, national institutions shape the way in which digital capitalism is fomented and regulated in different national contexts. These institutions determine key characteristics of digital capitalism such as the role of the state, the capacity to innovate, and the regulation of the transformations of labour markets.

State intervention occurs at two different levels. First, the state plays a more or less important role in the regulation of domestic capitalist relations. Second, the state participates in the organisation of capitalism on a global scale. This participation entails the creation and reproduction of global economic institutions that provides the legal framework for the global economy, but it also includes more technical institutions that are necessary in order to create an infrastructure to enable global flows of goods, services, capital, people, and information. Internet governance is an increasingly fundamental element of the technical governance of global capitalism, and states are participating in it as a necessary source of legitimacy.

In this context, a perspective on VoDC is a way to analyse the heterogeneous and evolving role of the state in digital capitalism at the domestic level and as an actor in global governance. It allows to reconcile the study of the regulation of digital capitalism and that of internet governance, to account for the hierarchical dynamics of the geopolitics of digital capitalism, and to put the digital revolution into perspective by studying the resilience of national institutional trajectories.

VoDC in Latin America

Latin America is an interesting case study of the role of the state in digital capitalism through the lenses of the VoDC. As a peripheral region in global capitalism, it was marginalised during the debates that gave birth to the institutions of internet governance and the principles guiding the development of the digital economy. The state is thus a major actor in the pursuit of insertion and autonomy in the digital age.

VoC in Latin America

As noticed in the previous section, digital capitalism reproduces long-term geopolitics of capitalism. Global value chains of hardware, software, and data are geographically hierarchised. For example, Clarke and Boersma (2017) use the case of Apple products to illustrate how workers and the environment are neglected on production sites while value is extracted in the Global North. Data evidences the same trend: It is produced where the number of internet users is greatest (the Global South) but acquires value mostly in the United States (Katz 2015; Casilli 2017). In its current form, data capitalism produces a new form of colonialism based on digital labour (Ávila Pinto 2018; Couldry and Mejias 2019). The problem, seen from the Global South, is not only the regulation of the data oligopolies but also the search by the state and regional institutions for a development model appropriate for the periphery.

The need for a developmental model that is beneficial to countries of the Global South is not new nor is it limited to digital capitalism. For example, more than four decades ago, Monza proposed an alternative approach on technological change from Latin America (Monza 2011) based on several observations. First, he noted that consumption in the peripheral economies evolves in an imitative way with the consumption pattern of the central economies. Second, peripheral states do not carry out technological creation, but repeat production methods designed in the central economies. Finally, industrialisation processes only take place in conditions of a decreasing degree of openness of the economy. Although this description corresponds to a different economic and political context, it reflects a similar underlying process, with the upshot that the economic development challenges faced by the Global South's repetition of patterns of development established in the North remain a problem. Similarly, despite the triumph of liberalisation since the 1990s and the transnational nature of cyberspace, the dilemma faced by peripheral economies remains the same: They are caught between the push

to open up their economies (global insertion) and the need for public policies adapted to the local context (state autonomy). How countries respond to this dilemma remains one of the main defining characteristics of the various existing models of Latin American (digital) capitalism.

The following analysis of VoDC in Latin America draws upon previous comparative capitalism research. For example, Ben Ross Schneider proposed the concept of hierarchical market economies (HME) to describe a Latin American type of capitalism (Schneider 2009). This concept highlights the key role of the state in peripheral capitalism, where it assumes a much greater regulatory and coordinating role than the state does in liberal market economies. The internet and digitisation are transformations that began in the United States in a more liberal institutional context. Drawing upon the concept of HME, the study of VoDC in Latin America requires a greater focus on the state than what is usually found in the literature focusing on the US and Western Europe. However, the category of HME does not allow for an analysis of variety within the region (Bizberg 2014; Bizberg and Théret 2012). Although the state has a preponderant role, it differs from one country to another in Latin America.

The type of institutional arrangements that exist at a national level are determined in part by the particular history of capitalism in each country. However, it is possible to outline a number of categories based on the national configurations stemming from two key moments in the recent economic history of Latin America.[2] First, the development model based on endogenous industrialisation designed after the Second World War and promoted by the Economic Commission for Latin America and the Caribbean was not implemented uniformly across the region (Sheahan 1987). While the Southern Cone countries (Argentina, Brazil, and Chile) undertook an industrialisation process aimed at the internal market, most countries in Central America, Peru, and Cuba before the 1959 revolution remained committed to a model based on free trade and the exportation of raw material. Mexico, Colombia, and Costa Rica chose a middle way with moderated state intervention and protectionism (Sheahan 1987, 271). This variation can be explained by the economic and demographic history of the sub-regions and by the level of geopolitical pressure from the US. The second key historical moment was the double transition to democracy and neoliberalism in the 1980s and 1990s (Smith, Acuña and Gamarra 1994; Oxhorn and Ducatenzeiler 1998). Chile diverged from the rest of the Southern Cone during the dictatorship of Augusto Pinochet (1973–1990) and constitutes its own variety of capitalism today (see Figure 9.1), aimed at outward-looking development. Brazil and Argentina went through different waves of neoliberal reforms, especially during the 1990s. However, they still evince a strong state interventionism in order to develop domestic markets and an important role for organised labour. They are defined as inward-looking and state-regulated peripheral capitalism by Bizberg and Théret (2012). Mexico and Colombia represent a middle way between inward-looking and state-regulated peripheral capitalisms, sometimes dubbed "passive insertion" (see Ebenau 2015) since they also pursue foreign direct investment and the insertion of their national economy into global markets without the state assuming a

strong regulatory role. Countries depending on oil and natural gas exports such as Venezuela and Bolivia represent yet another type of capitalism: They are sometimes described as petro-states (see Mijares and Jimenez Ruiz 2019).

These varieties of capitalism can be observed empirically. The Economic Freedom Index by the Heritage Foundation compiles different indicators related to state intervention and market deregulation.[3] While the index is often used as a way to "applaud high liberal scores" (Becker 2013, 12), the data can be used as an indicator of different varieties of capitalism since they express the degree of state intervention in different realms (see Figure 9.1 and Table 9.1).

The Economic Freedom Index confirms the historical trend. Based on 12 indicators of the four pillars of economic freedom (rule of law, government size, regulatory efficiency, and open markets), it evaluates the level of state intervention. A higher score on a scale from 0 to 100 means less state intervention. Chile is the most liberal Latin American country with a mean index superior to 70. Colombia, Mexico, Peru, and other smaller countries form a relatively liberal group with a mean index between 60 and 70. Brazil, Argentina, and other smaller countries are more interventionist, with a mean index between 50 and 60; Ecuador and Bolivia score between 40 and 50; and Venezuela and Cuba score higher in terms of state intervention in the economy, with mean indexes between 20 and 30. The combination of the historical analysis of national institutional trajectories and the more recent data on the role of the state in the economy allows for a categorisation of four different types of capitalism in Latin America (see Table 9.1).

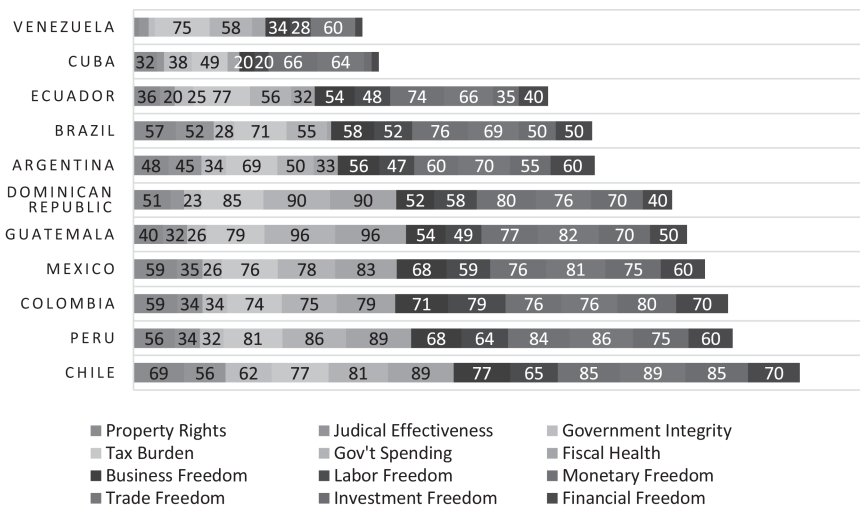


Figure 9.1 Aggregated indexes of economic freedoms of the 12 largest economies in Latin America

Source: Adapted from Index of Economic Freedom Dataset, Miller, Kim and Roberts, 2019.

Table 9.1 Varieties of capitalism in Latin America and case studies of VoDC

Type of regulation	*Economic Freedom Index*	*Label*	*Case study of VoDC*
Liberal	> 70	Peripheral liberal market economy	Chile
↕	Between 60 and 70	Outward-looking peripheral economies	Colombia, Mexico
	Between 50 and 60	Inward-looking peripheral economies	Brazil, Argentina
Interventionist	< 50	Petro-states and Hybrid economies	N/A

Source: Elaborated by the author.

As illustrated in the following sections, these four categories drawn from historical analysis and indicators of general state intervention correspond to different types of participation in global internet governance and of regulations of domestic digital capitalism.

Latin America and internet governance

The institutionalisation of internet governance in the 1990s was based on the vision of the US government and its idea of limited state intervention. As internet usage increased at a global level, many states questioned this model. Between the two phases of the UN-sponsored World Summit on the Information Society (WSIS) that took place between 2003 and 2005, internet governance became a major issue and the ICANN model became the target of harsh criticism focused on the oversight role of the US government and on the leadership of the private sector in internet governance (Kummer 2007).

Far from legitimising the existing minimalist-government approach, WSIS participants expressed diverse visions of the role of the state in internet governance. A majority of representatives from the Global North and some states from the Global South advocated for a multistakeholder model of internet governance consistent with the ICANN model, albeit with a broader definition of internet governance to include non-technical issues and with an increased participation of governments and intergovernmental organisations. A minority of states, mostly authoritarian regimes, rejected multistakeholderism altogether and called for an intergovernmental internet governance, where sovereign states would decide on the rules and institutions of the digital era (Radu 2019). A third group of emerging powers accepted a certain degree of multistakeholderism to ensure the participation of the technical community, the private sector, and civil society but argued that states were meant to have a special and overarching role in governance. They argued for example that multistakeholderism was suited for consultations and consensus-building but that governmental participation was necessary to ensure legitimacy in decision-making (Weber 2014).

The three positions existed among Latin American states, with individual states' positions being highly consistent with what one would expect their positions to be given their VoC categorisation, as outlined in the previous section. Petro-states and hybrid regimes either ignored the issue of internet governance during the WSIS (Bolivia) or insisted on sovereignty and intergovernmentalism (Venezuela, Cuba):

> We propose the creation of a Global Internet Policy Council with the participation of governments. There should also be a body to ensure the proper technical functioning. Both institutions must operate within the framework of the United Nations.
>
> (Venezuela 2005, translated by the author)

Inward-looking peripheral economies, meanwhile, accepted some degree of multistakeholderism but insisted on a preeminent role for the state in internet governance. They called for the "reinforcement of the role of Governments in ICANN decision making with regard to relevant Internet public policy issues" (Argentina 2005) and proposed an alternative vision of multistakeholderism:

> The plan of action . . . should emphasise the state's key role in the formulation and implementation of ICT-related policies, in partnership with international organisations, the private sector, and civil society.
>
> (Brazil 2003, translated by the author)

For their part, outward-looking peripheral economies, and particularly Mexico, endorsed the most consensual solutions promoted by the Working Group on Internet Governance, whose work they "admired and appreciate" (Mexico 2005a, translated by the author).

> We are optimistic about the creation of the Internet Governance Forum, as it opens up opportunities for dialogue from a multi-sectoral perspective and accepts a broad agenda that includes cybersecurity, spam, interconnection arrangements, traffic flows, and routing.
>
> (Mexico 2005b, translated by the author)

Finally, Chile, as a peripheral liberal market economy, hailed multistakeholderism as an innovative form of governance that opened the door for the participation of non-state actors.

> We are pleased to have achieved at this stage the necessary consensus that will allow us to continue advancing, through constructive dialogue, towards new forms and models of cooperation, under a framework that recognises and allows the effective participation of all the actors involved, within their respective roles.
>
> (Chile 2005, translated by the author)

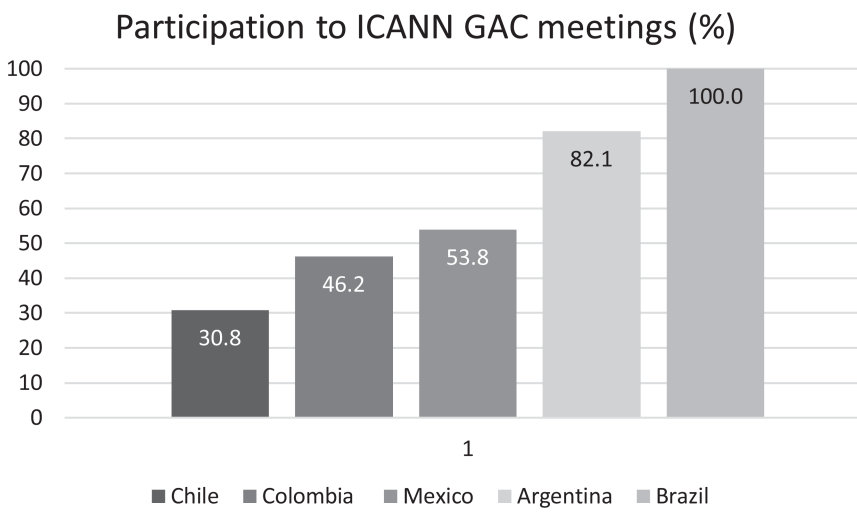


Figure 9.2 Participation of different Latin American governments' representatives to ICANN GAC meetings (1999–2019)

Source: Elaborated by the author based on GAC meeting minutes.[4]

The original statements during the WSIS paved the way for a heterogeneous participation of Latin American states in internet governance in the following years. Supporters of the liberal status quo participated less, whereas advocates of a more interventionist role for the state were actively promoting their vision in different internet governance settings. As illustrated by Figure 9.2, Chile was the least active government from the region in the activities of ICANN's GAC. Colombia and Mexico participated more, without exercising a leadership role in the committee. Argentina and Brazil were not only more active within the ICANN; they were also involved in the promotion of alternative forums and institutions to discuss internet governance issues. In 2014, in the wake of the Snowden revelations, Brazil convened a global multistakeholder conference (NetMundial) to discuss global internet governance in a post-Snowden context. It fomented the creation of the NetMundial Initiative to provide an alternative to current system of US-led internet governance.

The envisioned role of the state in internet governance in Latin America is consistent with historically informed categories of VoC: More liberal and outward-looking states are less likely to question the status quo in internet governance. More interventionist and inward-looking states have been criticising multistakeholderism and promoting alternatives to the US-led neoliberal model of internet governance.

The regulation of digital capitalism in Latin America

Latin America is an interesting case since it represents a middle-income region where digitisation is seen as a source of future growth and where states act in order

Table 9.2 From VoC to VoDC

	Chile	*Colombia*	*Mexico*	*Argentina*	*Brazil*
Labour regulation	Minimal	Government-led projects, mostly declaratory		Labour struggle and judicial decisions	Labour struggle and local authorities' leadership
Taxation	Minimal	Debated in order to strike a balance between FDI attraction and development		Strong	Strong and proactive at the international level
Data protection	Weak	Middle-way between US and EU		Strong	Strong
Variety of capitalism (see Table 9.1)	Peripheral liberal market economy	Outward-looking peripheral economies		Inward-looking peripheral economies	
VoDC	Liberal digital capitalism	Outward-looking peripheral digital capitalism		Inward-looking peripheral digital capitalism	

Source: Elaboration by the author based on press review.

to foster the digital economy. Legislation has been adopted throughout the region to tackle issues such as e-transactions, data protection and privacy, cybercrime, and consumer protection laws for the digital economy (UNCTAD n.d.).

A press review of major newspapers in the region's five most populous countries between 2017 and 2019 (Argentina, Brazil, Chile, Colombia, and Mexico), representing different varieties of capitalism, allows for an analysis of the main debates around the regulation of digitisation in Latin America.[5] Given the structural trend towards the digitisation of the economy and the equivalent peripheral situation of Latin American countries within digital capitalism, Latin American states all face most of the same challenges. Specifically, the most pressing challenges (as evidenced by policy debates in the region) are labour regulations, taxation, and data protection.

As illustrated by summary of the findings of the press review presented in Table 9.2, the debates on the role of the state in the regulation of digital capitalism is consistent with national institutional trajectories. They also echo the diverging positions on the role of the state in global internet governance outlined in the previous section.

Labour regulations

A review of newspaper articles in these five countries suggests that one of the main digital debates in Latin America over the last few years has been over how (or whether) labour regulations should be applied to platform workers. Different visions of the balance between state and the market as it relates to platform-labour

regulation coexist in the region. In Chile, the most liberal country in the region, President Sebastián Piñera presented a reform project on labour modernisation in May 2019 that clearly excluded digital platform workers from the category of employees and from the regulation of the Labour Code. Piñera's project even seeks to imitate the flexibility of platform labour in traditional sectors for example by introducing adjustable working hours and the possibility to suspend temporarily the labour relationship between the worker and the employer (Gobierno de Chile 2019).

Mexico and Colombia epitomise the outward-looking model, with state intervention aimed primarily at attracting foreign investment and global digital platforms. In Mexico, public authorities at the federal and at the state levels have made efforts to guarantee the payment of social security for platform workers (Estrella 2019). However, official institutions such as the tax administration continue to define platform workers as "natural persons who independently provide ground passenger transportation services or delivery of prepared food through technological platforms" (SAT 2019), rather than as employees. In Colombia, the regulation of these platforms will be a central axis of the National Development Plan, based on the recommendations of the International Labour Organisation that urged the ministries of justice, technology, labour, transportation, and interior to work hand in hand in a context of massive Venezuelan migration (Portafolio 2019). However, these efforts conflict with the ICT bill of 2019 that still prioritises investment over quality employment in order to make of "Colombia, a more attractive country for investment, reactivating the ICT sector industry – which has been slowing down" (MinTIC 2019).

Argentina and Brazil have adopted a more interventionist stance on labour regulation of digital capitalism. In Argentina, the world's first union for platform workers was created in order to demand risk insurance, fixed salaries, and safety regulations. The struggle for regulation also takes place in local courts. For example, a Buenos Aires judge banned mobile applications for delivery services until the issues of safety and risks for delivery workers have been resolved (Clarín 2019). In Brazil, conflicting visions have emerged, pitting Brazil's historical institutional trajectory, which involves a strong emphasis on labour protection, against more recent federal government policies, which have been aimed primarily at attracting foreign investment rather than pursuing Brazil's inward-looking and interventionist regulation model. For example, in 2017, Brazil modified federal regulations to make work more flexible. However, some local authorities, such as the city of Sao Paulo, have opted for a dialogue with digital platform companies in order to create new regulatory frameworks at the city level. Despite the government's efforts to remove platform workers from the category of employees, sectors of the judicial branch have taken an opposite stance through rulings that recognise, for example, Uber's partners as employees with benefits (Frias 2018). Moreover, workers' movements are standing up to defend their fundamental rights and to denounce a setback in labour protection matters, including platform-based labour (Putti 2019).

Taxation

In Chile during the period covered, tax-policy discussions for the digital sector have focused more on ensuring fair competition than on collecting new revenues for the state. Consistently with the liberal model of digital capitalism adopted by the country, the government is seeking to guarantee fair competition between traditional businesses and their digitalised counterparts (Montes 2018).

Colombia and Mexico are trying to find new sources of revenue for the state without endangering the growth of the digital economy. Colombia has positioned itself as one of the first countries in the region to collect value-added tax on digital platforms such as AirBnb, Netflix, Spotify, and Uber. Mexico, for its part, reached historic tax agreements with some of the digital platforms operating in the country in 2019. These agreements had become a matter of controversy since the election of President Andrés Manuel López Obrador the year before. While digital companies such as Netflix that had been exempt from taxes had opposed the creation of a tax on digital services, the agreement nevertheless includes the payment of a value-added tax. The Economic Commission for Latin America and the Caribbean strongly supports this type of value-added tax on digital services and argues that any creation of value in a territory should have benefits for the state that administers it (ECLAC 2019).

Argentina, meanwhile, designed a new tax regime that entered into force in June 2018 in order to collect taxes from "digital services" (Congreso de Argentina 2017). For its part, Brazil has played a more proactive role in promoting state intervention at a global level. It is one of the countries leading an offensive within the World Trade Organisation to establish taxation rules for e-commerce platforms, independent of whether they are based in the country of operation. Brazil argues that these resources should be directed to the compensation of workers who are affected by digitisation and to development of countries where platforms generate value (Agência Brasil 2019).

Data protection

As digital capitalism increasingly uses personal data as an asset in the creation of value, the necessity to strike a balance between data-fueled economic growth and the protection of personal data has become an essential aspect of the debate on the extent and role of state regulation. Latin America was one of the first regions in the world to discuss privacy regulations in the digital age. As early as 1992, the Colombian Constitutional Court introduced the idea of a "right to be forgotten" as it ruled in favour of a citizen who demanded the suppression of his personal data from a database of the Colombian Banking Association (Corte Constitucional 1993). Most Latin American countries have adopted *Habeas Data* provisions (literally "you have the data") in their constitutions and legal frameworks in the 1990s.

The debate on data protection was revived after the adoption of stronger privacy regulation in the European Union. However, the region oscillates between

a very liberal data-regulation framework inspired by the US model favouring the exploitation of data by digital platforms and a stricter regulation similar to the European model with stronger privacy regulations.

For example, the Chilean Senate in 2019 spent significant time debating the government's initiative for a comprehensive privacy bill that should be adopted in the first semester of 2020. The objective of the bill is to establish minimum standards, without over-regulating, to prevent increased costs that could have a direct impact on competitiveness (Yuraszeck 2019). Unlike most countries in the region, Chile currently has no Data Protection Agency. The scope and efficacy of the bill has come in for criticism, with many sectors of civil society arguing that the data protection bill is insufficient to protect the rights of citizens (Paz Canales and Viollier 2019).

Despite efforts to tighten its data protection framework, established in 2010, with the adoption of an additional law in 2017 (Mendoza Enríquez 2018), the Mexican government has struggled to fully enforce its framework. For example, Google and Facebook hide behind the fact that the headquarters that handle the data operate outside the country, preventing them (they say) from responding to the requests (LJA 2019). Likewise, Colombia has a strong legal and institutional data-regulation framework but is under pressure from tech giants when it tries to apply it to the digital realm. For example, in 2015, Google successfully advocated against a Colombian "right to be forgotten" in Google search results (La Rotta 2015).

Argentina is one of the most advanced countries in terms of data protection in the region. For example, in 2018, the Argentine Congress cited Facebook's legal representative for the theft of the personal data of 100,000 people. However, Mark Zuckerberg ignored the call and promised to improve protection standards worldwide. In addition, the idea that companies such as Facebook and Google should remunerate users for the use of their data is debated (Krom 2017). In turn, despite the strong intentions expressed in the *Marco Civil da Internet* (Presidência da República Federativa do Brasil, 2014), Brazil did not have a robust data protection and privacy law until the adoption of a General Data Protection Law in 2018. The new regulations aim to protect the national industry from losing opportunities in international competition in cases where Brazilian businesses were not complying with minimum data protection regulations elsewhere, especially in the European Union (Senado Federal 2019).

Overall, the findings from all five of the countries discussed in this section are consistent with the idea developed in the conceptual framework: Digitisation poses challenges for Latin American states, especially because of their peripheral position in global digital value chains. However, Latin American states are reacting differently to these challenges. Long-standing institutions and arrangements between the state and the market are affecting current policy debates on digitisation. While policy discussions are still underway in the region and subject to the political project of governments, historical trends tend to repeat themselves. Whereas Chile has adopted a "hands-off" approach to the regulation of digital markets based on a liberal understanding of technological change and economic

globalisation, Brazil and Argentina evidence struggles and concerns for the future of the national economy in a digitised world. Mexico and Colombia present a middle way with a more balanced discourse on digitisation. However, in these two countries, the state is more passive and primarily relies on discursive resources to foment self-regulation by digital companies (see Table 9.2). The models of regulation of digital capitalism in these countries correspond to their visions of the role of the state in internet governance. States adopting a more liberal variety of digital capitalism envision a free-market approach to the development of digital capitalism and a private sector–led internet governance. More interventionist states seek to regulate their domestic digital markets as well as to promote a stronger role for governments in global internet governance.

Conclusion: varieties of digital capitalism and the role of the state in internet governance in the Global South

A VoDC approach applied to Latin America offer some insights on how to analyse digitisation in the Global South, including both the regulation of digital capitalism at the domestic level and the participation of states in global internet governance. This chapter illustrates in particular how more liberal VoDCs – epitomised by Chile – entail both a *laissez-faire* approach to the regulation of digital markets and the endorsement of a multistakeholder global internet governance, while more interventionist VoDCs – illustrated by Argentina and Brazil – evidence stronger regulations of digital markets and a promotion of the role of governments in global internet governance.

First, state actors are (and have always been) important actors in the creation and reproduction of digital capitalism and in the management of the technical infrastructure of global telecommunication networks. Digitisation first occurred in very liberal institutional settings, such as the US under the Clinton administration and the European Union at the time where the European Commission was trying to set up the most competitive knowledge economy. This explains why the focus on the market and private actors was very strong in the 1990s and early 2000s. However, these institutional settings do not correspond to what exists in the Global South. Digitisation in the Global South occurs in a different institutional context in which the state plays a greater role. Thus, if we reject a technological determinist view and accept the idea that digitisation is at least partly shaped by preexisting institutions, the models of digitisation, and also of internet governance, that prevailed in the Global North in the 1990s are likely either to be transformed or to face competition from other regulatory models as digitisation travels south. While this present contribution is limited to a short description of the Latin American context, the literature on comparative capitalisms suggests that other regional contexts should also evidence the same importance of the state. It should therefore come as no surprise that actors from the Global South continue to advocate for alternative global internet governance models based on a different and more state-led understanding of multistakeholderism (see, e.g., Chenou and Rojas 2019).

Second, global and structural trends shaping digital capitalism should not be treated as homogenous processes. Even though they operate at a global scale, they evince different translations in different regional and national contexts. The relative position of countries in the global capitalist system foments an international division of labour that tends to reinforce existing global structures of accumulation. The description of the Latin American case in this chapter is an illustration of a global phenomenon. Digital capitalism tends to foment the emergence of two main poles of accumulation in the US and China and to create peripheries that correspond to historically marginalised regions but that also increasingly include Global North economies (Nieborg, Young and Joseph 2019). Moreover, even in the same region, the histories of different countries trigger variegated institutional responses to digitisation. The respective role of the state and the market differ from one country to another. The arrangements that allow for the emergence of digital markets depend largely on the role of public authorities, of trade unions, of national companies, and of transnational capital that have been historically forged in different countries. The description of current debates in Latin America on the regulation of digitisation offers evidence of the existence of three VoDC. The first is the market-led liberal capitalism that sees technological change as an opportunity to generate growth and foreign direct investment (FDI). This model is epitomised by Chile. The second is an outward-looking peripheral capitalism that also seeks to attract FDI but sees its peripheral position as generating domestic conflict that needs to be solved by the state. Colombia and Mexico illustrate this type of capitalism. Finally, an inward-looking peripheral capitalism tries to defend domestic companies and national institutional arrangements through regulatory struggles, both within state institutions and through trade unions' struggles. Brazil and Argentina still evidence the role of long-standing institutions despite recent ideological orientations of their respective governments.

Third, it is not enough to focus on material conditions if one wants to study the digitisation of the economy. Whereas indicators of economic digitisation focus on access to information and communications technologies or on the contribution of the digital sector to the gross domestic product (for a discussion, see Brynjolfsson and Collis 2019), a critical perspective requires an analysis of the institutional framework that shapes the use of these technologies. In order to study the effects of digitisation in the Global South, a focus on institutional elements is essential. The VoDC approach allows for a critical perspective on technology that accounts for the bias towards dynamics of capitalist reproduction through technological change. However, it also permits an analysis of the ambivalence of technological change and of the role of institution in shaping the digital future.

These insights on the study of digitisation in the Global South pave the way for a more heterogeneous understanding of the effect of current technological transformations on the national, regional, and global forms of organisation of digital capitalism. They also contribute to the understanding of the evolving relation between states and markets in the digital era, with a special focus on the Global South and its diversity.

Acknowledgements

The author would like to thank Juan Felipe Arias Rodríguez, Abdelaziz Malaver Tatar, and Paula Henao Aristizábal for their research assistance.

Notes

1 For a further discussion of governments' role in ICANN, see Cavalli and Scholte, this volume.
2 I am thankful to Luis Javier Orjuela for pointing out the importance of these two moments in the definition of the varieties of Latin American capitalism.
3 The Heritage Foundation measures economic freedom based on 12 quantitative and qualitative factors, grouped into four broad categories, or pillars, of economic freedom: Rule of Law (property rights, government integrity, judicial effectiveness); Government Size (government spending, tax burden, fiscal health); Regulatory Efficiency (business freedom, labour freedom, monetary freedom); and Open Markets (trade freedom, investment freedom, financial freedom). Each of the 12 economic freedoms within these categories is graded on a scale of 0 to 100.
4 Available at https://gac.icann.org/contentMigrated/icann65-gac-marrakech-minutes, accessed 20 September 2019. Based on 39 meetings' minutes available online and containing a participants' list.
5 For each country, five or six newspapers of national reputation were systematically reviewed in order to identify the most relevant policy debates. Existing and future regulations mentioned in the articles allowed for a classification of (expected) state intervention in each debate.

References

Abbate, Janet. 1999. *Inventing the Internet*. Cambridge, MA and London: MIT Press.

Agência Brasil. 2019. "OMC começa a discutir regras internacionais para comércio eletrônico [WTO Starts to Discuss International Rules for Electronic Commerce]." *Agência Brasil*. 19 May. http://agenciabrasil.ebc.com.br/economia/noticia/2019-05/omc-comeca-discutir-regras-internacionais-para-comercio-eletronico. Accessed 17 June 2019.

Argentina. 2005. *Statement of Argentina during the third Preparatory Committee (PrepCom 3). Subcommittee A*. 30 September. www.itu.int/net/wsis/index.html.

Ávila Pinto, Renata. 2018. "Digital Sovereignty or digital colonialism?" *Sur International Journal on Human Rights* 15(27): 15.

Becker, Uwe. 2013. "Measuring Change of Capitalist Varieties: Reflections on Method, Illustrations from the BRICs." *New Political Economy* 18 (4): 503–532. https://doi.org/10.1080/13563467.2012.717611.

Bizberg, Ilan. 2014. "Types of Capitalism in Latin America." *Revue Interventions Économiques. Papers in Political Economy* 49. https://doi.org/10.4000/interventionseconomiques.1772.

Bizberg, Ilan, and Bruno Théret. 2012. "La diversité des capitalismes latino-américains : les cas de l'Argentine, du Brésil et du 'exique' [The diversity of Latin American capitalisms: the cases of Argentina, Brazil and Mexico]." *Revue de la régulation. Capitalisme, institutions, pouvoirs* 11.

Brazil. 2003. *Brazilian Comments on the Draft Plan of Action*. 31 May. www.itu.int/net/wsis/index.html.

Bruff, Ian, Matthias Ebenau, and Christopher May. 2015. "Fault and Fracture? The Impact of New Directions in Comparative Capitalisms Research on the Wider Field." In *New Directions in Comparative Capitalisms Research: Critical and Global Perspectives*, edited by Matthias Ebenau, Ian Bruff, and Christopher May, 28–44. London: Palgrave Macmillan. https://doi.org/10.1057/9781137444615_3.

Brynjolfsson, Erik, and Avinash Collis. 2019. "How Should We Measure the Digital Economy?" *Harvard Business Review*. https://hbr.org/2019/11/how-should-we-measure-the-digital-economy. Accessed 7 August 2020.

Casilli, Antonio. 2017. "Digital Labor Studies Go Global: Toward a Digital Decolonial Turn." *International Journal of Communication* 110: 21.

Chenou, Jean-Marie. 2014. "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalization of Internet Governance in the 1990s." *Globalizations 11* (2): 205–223. https://doi.org/10.1080/14747731.2014.887387.

Chenou, Jean-Marie, and Juan Sebastián Rojas Fuerte. 2019. "The Difficult Path to the Insertion of the Global South in Internet governance." In *Internet Governance in the Global South*, edited by Daniel Oppermann, 42–73. Sao Paulo: NUPRI.

Chile. 2005. *Statement of Mexico during the Tunis Summit*. 17 November. www.itu.int/net/wsis/index.html.

Clarín. 2019. "Fallo polémico: prohíben a Rappi, Glovo y Pedidos Ya hacer Delivery en Bicicleta [Controversial Ruling: Rappi, Glovo and Pedidos Ya are Forbidden to Deliver by Bicycle]." *Clarín.com*. 10 April. www.clarin.com/ciudades/fallo-polemico-prohiben-empresas-delivery-bicicleta_0_OUmlzF47F.html. Accessed 17 June 2019.

Clarke, Thomas, and Martijn Boersma. 2017. "The Governance of Global Value Chains: Unresolved Human Rights, Environmental and Ethical Dilemmas in the Apple Supply Chain." *Journal of Business Ethics* 143 (1): 111–131. https://doi.org/10.1007/s10551-015-2781-3.

Congreso de Argentina. 2017. *Ley 27430. Impuesto a las ganancias* [*Law 27430. Income Tax*]. http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/305262/norma.htm. Accessed 4 March 2020.

Corte Constitucional. 1993. *Banco de datos/Acción de tutela/Asociación Bancaria. Sentencia No. T-022–93* [*Databases/ Remedy of protection action/Banking Association. Judgment No. T-022–93*]. www.corteconstitucional.gov.co/relatoria/1993/t-022-93.htm. Accessed 4 March 2020.

Couldry, Nick, and Ulises A. Mejias. 2019. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20 (4): 336–349.

Ebenau, Matthias. 2015. "Directions and Debates in the Globalization Of Comparative Capitalisms Research." In *New Directions in Comparative Capitalisms Research: Critical and Global Perspectives*, edited by Matthias Ebenau, Ian Bruff, and Christopher May, 45–64. London: Palgrave Macmillan. https://doi.org/10.1057/9781137444615_4.

ECLAC. 2019. *Panorama Fiscal de América Latina y el Caribe 2019. Políticas tributarias para la movilización de recursos en el marco de la Agenda 2030 para el Desarrollo Sostenible* [*Fiscal Panorama of Latin America and the Caribbean 2019. Tax policies for the mobilization of resources in the framework of the 2030 Agenda for Sustainable Development*]. LC/PUB.2019/8-P. Santiago, 2019.

Estrella, Viviana. 2019. "Querétaro busca regular condiciones laborales de repartidores de servicios como Rappi [Querétaro Seeks to Regulate Working Conditions for Delivery Services Such as Rappi]." *El Economista*. 13 March. www.eleconomista.com.mx/estados/Queretaro-busca-regular-condiciones-laborales-de-repartidoresde-servicios-como-Rappi-20190313–0121.html. Accessed 17 June 2019.

Fernández, Victor Ramiro, Matthias Ebenau, and Alcides Bazza. 2018. "Rethinking Varieties of Capitalism from the Latin American Periphery." *Review of Radical Political Economics* 50 (2): 392–408. https://doi.org/10.1177%2F0486613417690139.

Fontaine-Skronski, Kim, and Rioux, Michèle, eds. 2015. *Global Governance Facing Structural Changes: New Institutional Trajectories for Digital and Transnational Capitalism*. New York: Palgrave Macmillan.

Frias, Maria Christina. 2018. "La justicia brasileña decide que los conductores de Uber son empleados de la empresa [Brazilian Justice Decides That Uber Drivers Are Employees of the Company]." *Folha de S.Paulo*. 27 August. https://www1.folha.uol.com.br/internacional/es/economia/2018/08/la-justicia-brasilena-decide-que-los-conductores-de-uber-son-empleados-de-la-empresa.shtml. Accessed 5 August 2020.

Gereffi, Gary. 2001. "Shifting Governance Structures in Global Commodity Chains, With Special Reference to the Internet." *American Behavioral Scientist* 44 (10): 1616–1637. https://doi.org/0.1177/00027640121958087.

Gobierno de Chile, 2019. *Modernización Laboral* [*Labor Modernization*] www.gob.cl/modernizacionlaboral/. Accessed 4 March 2020.

Gordon, David, Richard Edwards, and Michael Reich. 1982. *Segmented Work, Divided Workers: The Historical Transformation of Labor in the United States*. Cambridge and New York: Cambridge University Press.

Haggart, Blayne, and Michael Jablonski. 2017. "Internet Freedom and Copyright Maximalism: Contradictory Hypocrisy or Complementary Policies?" *The Information Society* 33 (3): 103–118. https://doi.org/10.1080/01972243.2017.1294128.

Hall, Peter A., and David Soskice, eds. 2001. *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press.

Hancké, Bob, Martin Rhods, and Mark Thatcher, eds. 2007. *Beyond Varieties of Capitalism: Conflict, Contradictions, and Complementarities in the European Economy*. Oxford: Oxford University Press.

Harvey, David. 1985. "The Geopolitics of Capitalism." In *Social Relations and Spatial Structures*, edited by Derek Gregory and John Urry, 128–163. London: Palgrave. https://doi.org/10.1007/978-1-349-27935-7_7

ICANN. 1998. *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*. 21 November. Los Angeles, CA: ICANN.

ICANN and Department of Commerce. 1998. *Memory of Understanding between the U.S Department of Commerce and Internet Corporation for Assigned Names and Numbers*. Los Angeles, CA: ICANN.

Katz, Raúl L. 2015. *El ecosistema y la economía digital en América Latina* [*The ecosystem and the digital economy in Latin America*]. Madrid: Fundación Telefónica.

Krom, Andrés. 2017. "Facebook hace millones con tus datos. Este argentino quiere darte tu tajada [Facebook makes millions with your data. This Argentine Wants to Give You Your Share]." *La Nación*. 26 December. www.lanacion.com.ar/economia/facebook-y-google-hacen-millones-con-tus-datos-este-argentino-quiere-darte-tu-tajada-nid2094838 Accessed 5 August 2020.

Kummer, M. 2007. "The Debate on Internet Governance: From Geneva to Tunis and Beyond." *Information Polity* 12 (1): 5–13. https://doi.org/10.3233/IP-2007-0107.

La Rotta, Santiago. 2015, "Derecho al olvido a la colombiana [Right to be Forgotten, the Colombian Way]." *Elspectador.com*. 4 July. www.elespectador.com/tecnologia/derecho-al-olvido-colombiana-articulo-570227. Accessed 5 July 2020.

LJA. 2019. "¿Qué tan eficaz es la protección de datos personales en México?" ["How Effective Is Personal Data Protection in Mexico?"]. *La Jornada Aguascalientes*. 30 May.

www.lja.mx/2019/05/que-tan-eficaz-es-la-proteccion-de-datos-personales-en-mexico/. Accessed 17 June 2019.

Mann, Laura, and Gianluca Iazzolino. 2019. "See, Nudge, Control and Profit: Digital Platforms as Privatized Epistemic Infrastructures." *Platform Politick: A Series*. IT for Change. March. https://itforchange.net/platformpolitics/wp-content/uploads/2019/03/Digital-Platforms-as-Privatized-Epistemic-Infrastructures-_5thMarch.pdf. Accessed 5 August 2020.

Marx, Karl. 1993. *Capital: Volume 2: A Critique of Political Economy*. New York: Penguin.

McCarthy, Daniel R. 2018. *Technology and World Politics: An Introduction*. Abingdon: Routledge.

McDonough, Terrence. 2015. "Social Structures of Accumulation: A Marxist Comparison of Capitalisms?" In *New Directions in Comparative Capitalisms Research: Critical and Global Perspectives*, edited by Matthias Ebenau, Ian Bruff, and Christopher May, 118–133. London: Palgrave Macmillan. https://doi.org/10.1057/9781137444615_8.

McDonough, Terrence, Michael Reich, and David M. Kotz. 2010. *Contemporary Capitalism and Its Crises: Social Structure of Accumulation Theory for the 21st Century*. Cambridge: Cambridge University Press.

Mendoza Enríquez, O.A. 2018. "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: Desafíos y cumplimiento [Legal Framework for the Protection of Personal Data in Service Companies Established in Mexico: Challenges and Compliance]." *Revista IUS* 12 (41): 267–291.

Mexico. 2005a. *Statement of Mexico during the third Preparatory Committee (PrepCom 3)*. Subcommittee A. 21 September. www.itu.int/net/wsis/index.html.

Mexico. 2005b. *Statement of Mexico during the Tunis Summit*. 16 November. www.itu.int/net/wsis/index.html.

Mijares, Víctor, and Laura Jimenez Ruiz. 2019. "Mezclas explosivas: condicionantes de la represión en petroestados [Explosive Mixtures: Conditions for Repression in Petro-States]." http://dx.doi.org/10.2139/ssrn.3337112.

Miller, Terry, Anthony B. Kim., and James M. Roberts, 2019. *Index of Economic Freedom*. Washington, DC: The Heritage Foundation.

MinTIC. 2019. *Proyecto de ley para modernizar el sector TIC* "*Bill to modernize the ICT sector*]. www.mintic.gov.co.

Montes, Sebastián. 2018. "Piñera no bajará el impuesto corporativo, pero le pondrá una tasa a Netflix y Airbnb [Piñera Will Not Lower the Corporate Tax, But Will Put a Tax on Netflix and Airbnb]." *La República*. 23 August. www.larepublica.co/globoeconomia/pinera-no-bajara-el-impuesto-corporativo-pero-le-pondra-una-tasa-a-netflix-y-airbnb-2762467. Accessed 5 August 2020.

Monza, Alfredo. 2011. "La teoría del cambio tecnológico y las economías dependientes [The Theory of Technological Change and Dependent Economies]." In: *El Pensamiento latinoamericano en la problemática ciencia-tecnología-desarrollo-dependencia* [*Latin American thinking on the problématique of science-technology-development-dependency*], edited by Jorge A. Sábato, 171–194. Buenos Aires: Ediciones Biblioteca Nacional.

Mueller, Milton. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Nieborg, David B., Chris Young, and Daniel Joseph. 2019. "Lost in the App Store: The State of the Canadian Game App Economy." *Canadian Journal of Communication* 44 (2): 57–62. https://doi.org/10.22230/cjc.2019v44n2a3505.

Nölke, Andreas, and Arjan Vliegenthart. 2009. "Enlarging the Varieties of Capitalism: The Emergence of Dependent Market Economies in East Central Europe." *World Politics* 61 (4): 670–702.

NTIA. 1998a. *A Proposal to Improve the Technical Management of Internet Names and Addresses*. 20 February. Docket Number: 980212036–8036–01.

NTIA. 1998b. *Statement of Policy on the Management of Internet Names and Addresses*. 5 June. Docket Number: 980212036–8146–02.

Oxhorn, Philip D., and Graciela Ducatenzeiler, eds. 1998. *What Kind of Democracy? What Kind of Market? Latin America in the Age of Neoliberalism*. University Park, PA: Pennsylvania State University Press.

Paz Canales, Maria, and Pablo Viollier. 2019. "Chile necesita una regulación de protección de datos con dientes [Chile Needs a Data Protection Regulation with Teeth]." *Derechos Digitales*. 12 July. www.derechosdigitales.org/13443/proteccion-de-datos-con-dientes/. Accessed 5 August 2020.

Pickard, V. 2007. "Neoliberal Visions and Revisions in Global Communications Policy From NWICO to WSIS." *Journal of Communication Inquiry* 31 (2): 118–139. https://doi.org/10.1177%2F0196859906298162.

Portafolio. 2019. "¿Qué se está haciendo en Colombia Para Regular el trabajo Digital? [What Is Being Done in Colombia to Regulate Digital Labour?]." *Portafolio.co*. 20 May. www.portafolio.co/economia/empleo/que-se-esta-haciendo-en-colombia-para-regular-el-trabajo-digital-529742. Accessed 5 August 2020.

Presidência da República Federativa do Brasil. 2014. *Marco Civil da Internet* [Brazilian Civil Rights Framework for the Internet]. Lei N°12.965, 23 April 2014.

Putti, Alexandre. 2019. "Apps são os maiores empregadores, mas precarização dá o tom nos trabalhos [Apps Are the Biggest Employers, But Precariousness Sets the Tone in Jobs]." *Carta Capital*. 7 May. www.cartacapital.com.br/economia/proletariado-digital-apps-promovem-trabalhos-precarios-a-brasileiros/. Accessed 17 June 2019.

Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford and New York: Oxford University Press.

Rueda, David, and Jonas Pontusson. 2000. "Wage Inequality and Varieties of Capitalism." *World Politics* 52 (3): 350–383. https://doi.org/10.1017/S0043887100016579.

SAT. 2019. *Presenta tu declaración de retenciones por el uso de plataformas tecnológicas – Declaraciones – Portal de trámites y servicios – SAT [File Your Tax Return for the Use of Technological Platforms – Declarations- Procedures and Services Portal]*. www.sat.gob.mx/declaracion/82614/presenta-tu-declaracion-de-retenciones-por-el-uso-de-plataformas-tecnologicas. Accessed 17 June 2019.

Schiller, Dan. 1999. *Digital Capitalism. Networking the Global Market System*. Cambridge, MA: MIT Press.

Schneider, Ben Ross. 2009. "Hierarchical Market Economies and Varieties of Capitalism in Latin America." *Journal of Latin American Studies* 41 (3): 553–575. https://doi.org/10.1017/S0022216X09990186.

Schwab, Klaus. 2017. *The Fourth Industrial Revolution*. New York: Penguin.

Senado Federal, Brazil. 2019. "Senado aprova MP que recria órgão para proteção de dados pessoais [Senate Approves MP That Recreates Body for Personal Data Protection]." *Senado Notícias*. 29 May. https://www12.senado.leg.br/noticias/materias/2019/05/29/senado-aprova-mp-que-recria-orgao-para-protecao-de-dados-pessoais. Accessed 17 June 2019.

Sheahan, John. 1987. *Patterns of Development in Latin America: Poverty, Repression, and Economic Strategy*. Princeton, NJ: Princeton University Press.

Simpson, Seamus. 2004. "Explaining the Commercialization of the Internet: A Neo-Gramscian Contribution." *Communication and Society* 7: 50–68. https://doi.org/10.1080/1369118042000208898.

Smith, William C., Carlos H. Acuña, and Eduardo Gamarra, eds. 1994. *Latin American Political Economy in the Age of Neoliberal Reform: Theoretical and Comparative Perspectives for the 1990s*. Coral Gables, FL and New Brunswick, NJ: North-South Center, University of Miami.

Srnicek, Nick. 2017. *Platform Capitalism*. Hoboken, NJ: John Wiley & Sons.

UNCTAD. n.d. *Summary of Adoption of E-Commerce Legislation Worldwide*. Web page. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx. Accessed 13 August 2020.

US Government. 1997. *Framework for E-Commerce*. Washington, DC: White House. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

Venezuela. 2005. *Statement of Venezuela during the Third Preparatory Committee (PrepCom 3)*. Subcommittee A. 27 September. www.itu.int/net/wsis/index.html.

Weber, R.H. 2014. "Visions of Political Power: Treaty Making and Multistakeholder Understanding." In *The Evolution of Global Internet Governance Principles and Policies in the Making*, edited by Roxana Radu, Jean-Marie Chenou, and Rolf H. Weber, 95–113. Berlin: Springer.

West, Sarah Myers. 2019. "Data Capitalism: Redefining the Logics of Surveillance and Privacy." *Business & Society* 58 (1): 20–41. https://doi.org/10.1177%2F0007650317718185.

Yuraszeck, Nicholas. 2019. "Ley de Protección de Datos: Regular, pero no sobre Regular [Data Protection Act: Regulate, But Not Over-Regulate]." *El Mostrador*. 28 April. www.elmostrador.cl/noticias/opinion/columnas/2019/04/28/regular-pero-no-sobre-regular/. Accessed 5 August 2020.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

10 Seeing through the smart city narrative

Data governance, power relations, and regulatory challenges in Brazil

Jhessica Reia and Luã Fergus Cruz

Introduction

The "smart city" is one of those concepts that simultaneously embodies multiple meanings and engenders endless controversies. The flavour of the moment in urban-development circles, more than anything it represents a corporate-driven narrative (Söderström, Paasche and Klauser 2014; Sadowski and Bendor 2019) focused on achieving efficiencies through the use of data and surveillance. It has become the focus of attention within such wide-ranging policy- and decision-making spaces as the United Nations' biannual World Urban Forum (WUF) and the annual Internet Governance Forum (IGF). Its inclusion in such diverse policy spaces reflects the dual nature of what the "smart city" (in all of its definitional complexity) entails, not only as a form of urban infrastructure but also as a specific case of internet governance. As the UN forums widened their topics to include the role of new technologies and the emergent smart city market, so did the IGF, broadening its approach to cover the impacts of smart cities in a myriad of topics related to the community.[1]

It is important to study the smart city because, far from being the imagined utopia of a few years ago, it is a reality in many cities around the world. Cities are implementing technologies framed in a specific narrative of "smartness" that fails to take into account critical questions of privacy, data governance, and the right to the city. They are also failing to pay sufficient attention to the increased corporatisation of municipal governance entailed by most "smart city" proposals, as we will discuss later. We see smart cities' incorporation of networks, data, and infrastructure as the physical embodiment of the "last mile" of internet governance, hence the importance of analysing smart cities related to – and beyond – internet governance, in order to understand power relations in the intersection of infrastructure (materialities), policy, and politics. The convergence of these agendas needs more attention.

This chapter offers a much-needed critical, Global South perspective on the smart city ecosystem in Brazil, focused specifically on power relations between state and non-state actors. It assesses the implications of different – or absent – regulatory frameworks for data governance in smart cities. Brazil is an important case study, not only for the leadership role that it has played over the past few

DOI: 10.4324/9781003008309-14

decades in global digital policy and the right to the city movement but also for what we can learn from the historical inequalities being exacerbated by technology and the current authoritarian government shaping the (lack of) public debate in the country.

The smart city debate has been active in Brazil, as in many other countries. In 2014, Brazilian specialists presented a series of comments to the preparatory documents that were going to shape the New Urban Agenda (NUA), a multistakeholder agreement designed to serve as a guideline for urban development for the next twenty years; it was signed in Quito in 2016 during the United Nations Conference on Housing and Sustainable Urban Development (HABITAT III).[2] Brazilian representatives offered relevant criticism throughout the process, on a variety of topics,[3] but one is particularly relevant to the discussion developed in this chapter: the inclusion of the "smart city" concept in the NUA, on its 66th item – as a commitment to adopt it – is seen as problematic by some scholars (Balbim 2017; Reia 2019), confirming the officialisation of a corporate narrative (Söderström, Paasche and Klauser 2014) on urban efficiencies as part of a broader effort to plan the future of our cities.

Prior to the final NUA document signing, an intricate framework of policy units and issue papers were designed by numerous specialists. Issue paper 21, connected to the subject of "Urban Housing and Basic Services," is dedicated specifically to smart cities (United Nations 2015). Smart cities were presented as "a viable option for the future," although tellingly privacy, data governance, and data protection are not mentioned once in this document. The neglect of these central issues to public policy is particularly significant in the face of mass surveillance and recurrent data breaches, often involving public-private partnerships, around the world.

During the first two decades of this century, Brazil assumed an essential role in many discussions related to digital culture, free software, free culture, internet governance, copyright, and data protection. The country's unique pathbreaking role in promoting multistakeholderism in regard to digital issues drew "a path between the tightly regulated European international system, the American business-driven system, and the authoritarian online world of government censorship, surveillance, and control" (Arnaudo 2017, 38). However, a significant proportion of these collective efforts are being sidetracked. Since 2016, Brazilian civil society has seen their channels of communication with the government increasingly closed off, with windows of opportunities to influence government decisions disappearing. As a result, civil society's energies are being increasingly redirected to damage control (instead of the possibility for agenda setting). The fluid and complex political situation in Brazil reached a turning point during the 2018 elections: Following a controversial campaign fueled by misinformation (Folha de S. Paulo 2019a) and hate speech, Jair Bolsonaro, the far-right candidate, was elected with 55.1 percent of the valid votes, threatening the recent re-democratisation process being built in the country. Although Brazilian civil society had played a significant and positive role in copyright reforms (Reia and Mizukami 2015), the civil rights framework for the internet (Souza, Maciel and Francisco 2010; Papp 2014), and data protection regulation[4] in the earlier parts of this century, this

type of engagement with the government about the smart city agenda has become significantly more difficult since the 2018 presidential election that brought Jair Bolsonaro to power. These changes highlight the extent to which progressive Brazilian digital policy is subject to political contestation and can be reversed depending on who or which party is in power.

The increasing relevance of the urban areas and the higher penetration rates of technologies in the country, allied with global demand for sustainability and efficiency, have put the relations between corporate actors pushing this smart city agenda and Brazilian municipalities in the spotlight. In bringing to light the impact of a corporate narrative on the deployment of technological devices in urban spaces, the Brazilian experience offers valuable lessons, not only for the global internet governance community but for everyone concerned about the role of technologies and transnational corporations in shaping the future of our cities.

To better understand the interplay among corporate, governmental, and civil society voices and the extent to which public-interest concerns are being addressed, this chapter was written based on fieldwork conducted between March 2018 and June 2019, with three cities serving as case studies: São Paulo, Curitiba, and Rio de Janeiro. All three were designated as the "smartest" cities in Brazil in 2017. They are located in some of the wealthiest regions of the country: the Southeast (Sao Paulo and Rio) and the South (Curitiba).[5] We employ a regulatory framework and policy analysis as well as in-depth interviews with government representatives, companies, and researchers; participant observation in three of the largest smart city forums and expos in Brazil; and access to information requests. Overall, we found that the so-called Brazilian smart cities ecosystem – which involves all the actors, services, and products offered within the smart city agenda – is fragmented, hard to grasp, and complex. Most importantly, we found that while Brazil, with its size and historical urban issues, offers a rather attractive market for smart solutions, most of these social issues do not feature in the corporate-dominated discourses of the smart city.

This chapter is structured in four sections. In the first section, we briefly examine the conceptualisation of the "smart city" and present the definition that guides our work. The second section presents our findings in relation to the institutional, regulatory, and policy context affecting the smart city ecosystem, including topics such as the congressional agenda, public-private partnerships, and data governance. The third section is centred on the industry-focused smart city expos and forums in which technologies are showcased and policies are discussed. Lastly, the fourth section briefly addresses the question of power relations and whose voices are heard in the Brazilian smart city governance debate before offering some concluding thoughts.

Defining "smartness"

The various conceptualisations of what a smart city should be are all attempts to make sense of the relations between technologies and urban spaces, often

disregarding a longer history that highlights the role of technology and information in these spaces.[6] As Shannon Mattern (2017a) argues, urban intelligence is a relevant aspect of urban planning that has been part of our cities for millennia:

> [Urban] intelligence is simultaneously epistemological, technological, and physical; it's codified in our cities' laws and civic knowledges and institutions, hard-wired into their cables and protocols, framed in their streets and architectures and patterns of development. The city mediates between these various materialities of intelligence, between the ether and the iron ore. Clay and code, dirt and data intermingle here, and they always have.
>
> (Mattern 2017a, xii)

In another piece, Mattern (2017b) affirms that we see new metaphors to rationalise our cities, and "our current paradigm, the city as computer, appeals because it frames the messiness of urban life as programmable and subject to rational order." The predominant smart cities narrative – which has gained ground first in the private sector, when "smarter cities" was trademarked by IBM in 2011 (Söderström, Paasche and Klauser 2014, 307), followed by municipal governments, academia, and civil society – is used to describe data-centric initiatives around the world. The discourse promises that big data enables cities to adopt a more sophisticated, real-time understanding of their spaces and people. However, in terms of data governance, equality, and the right to the city, current smart city initiatives can raise more questions than deliver solutions.

As has been widely noted, there is no single definition of what a "smart city" is or what it is supposed to look like. What exists are fragmented efforts from numerous state and non-state actors to build agendas aligned with their interests amidst complicated relations among technology, innovation, and power dynamics. This chapter draws from critical theory on smart cities (Townsend 2013; Söderström, Paasche and Klauser 2014; Kitchin 2014, 2015; Kitchin, Lauriault and Cardle 2018; Cardullo and Kitchin 2019; Niaros 2016) and reports on the impacts of the indiscriminate adoption of the smart cities agenda (such as Privacy International 2017; Morozov and Bria 2018).

Since there is no consensus on a single definition of a smart city, one of the first challenges of this research project was to come up with a theoretical and conceptual framework for the topic being studied. Based on our analysis of the relevant literature and our fieldwork, we adopt in this chapter the notion of the smart city as a technopolitical agenda (Kurban, Peña-López and Haberer 2017; Winner 1980). This approach does not treat the "smart city" as a consolidated concept, but rather as an ongoing process of transformation of urban spaces based on the articulation among actors, devices/technologies, and politics. The smart city technopolitical agenda is already a reality in Brazil, with a proliferation of rankings, corporate-sponsored expos, controversial legislation, and top-down smart-focused policies driven mostly by the private sector (especially through consulting firms), with few exceptions.

The institutional context and regulatory framework in a time of change

The smart city regulatory and institutional framework presented here involves, mostly, the federal and the municipal levels. Brazilian federalism provides municipalities with political and administrative autonomy (Pires 2005), which allows cities to legislate on matters of local interest. This type of arrangement means that states have residual – nonetheless important – obligations, such as tax collection and metropolitan and intermunicipal policies.

Brazil's relevance to the global smart city debate is rooted in its experiences in previous landmark digital-policy issues. It assumed a leadership role in policies related to the digitisation in the early 2000s, and it was internationally recognised for its pioneering spirit when it comes to social participation and engagement in formulating, implementing, and evaluating digital policies. According to Arnaudo (2017):

> Brazil played a unique role in debating several digital issues, drawing a path between the tightly regulated European international system, the American business-driven system, and the authoritarian online world of government censorship, surveillance, and control. Its model is driven and nurtured by the multistakeholder vision of the Internet Steering Committee, the Civil Rights Framework for the Internet, new democratic online systems, and several other internet regulations – and has become an example to the world. It remains to be seen whether the current government will continue to follow the path taken by the previous one – maintaining and promoting this model internally and internationally – or whether it will try to develop an alternative policy more in tune with the free market. Initial indicators, such as the government's decision to emphasise private internet infrastructure development and to withdraw resources from public initiatives, suggest that it will opt for the latter.
>
> (Arnaudo 2017, 38, translated by the authors)

For years, Brazil fostered a vibrant environment for multistakeholder discussions in which civil society had a real voice. Among its best-known accomplishments are the establishment of a multistakeholder Internet Steering Committee (*Comitê Gestor da Internet*, CGI.br), which democratically elects representatives from the government, the corporate sector, the third sector, and the academic community to participate in discussions regarding internet governance with the government. In addition, there's been the early adoption of Creative Commons licenses by the federal government and for holding online public consultations for the Civil Rights Framework for the Internet (*Marco Civil da Internet*), the Copyright Law Reform (*Reforma da Lei de Direitos Autorais*), and the General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais*, LGDP). For several years, civil society articulated its actions towards a positive digital policy agenda, dealing with challenges along the way and proposing bottom-up policies – to see many of them

implemented or at least considered by the federal government. However, the situation has been changing since the controversial impeachment of President Dilma Rousseff in 2016, who was succeeded by Michel Temer and shortly thereafter by Jair Bolsonaro in 2018. Over the last decade, and increasingly since Rousseff's impeachment, it became more difficult for civil society to influence policy at the federal level, and many actors have had to spend significant amounts of time and resources putting out (metaphorical) fires and simply trying to guarantee fundamental rights. The current disputes around data governance, which we discuss later, are a good example of these changes.

Debates on how to foster a regulatory framework in which smart cities can thrive are becoming common in Brazil, and they are supported by development agencies, mayors, and companies. One example of this kind of collective effort, driven mostly by the private sector, is the 2nd Curitiba Commitment (*2o Compromisso de Curitiba*),[7] a document signed by companies and mayors at the Smart City Business America Congress and Expo in 2015 and presented to the UN-HABITAT. This document focused on strengthening public-private partnerships within a smart city framework.

It is common for stakeholders to present their perceptions on regulatory changes that are necessary to promote a legal framework aligned with their interests through official reports to the government. The strategy is to influence the potential review and drafting of current regulations, as we can see in the industry-oriented report "*Cidades Inteligentes: Oportunidades e Desafios para o Estímulo ao Setor no Brasil*" ("Smart Cities: Opportunities and Challenges for Stimulating the Sector in Brazil"), published in 2018 by the Brazilian Agency for Industrial Development (*Agência Brasileira de Desenvolvimento Industrial*, ABDI).[8] It lists a few regulatory bottlenecks for the development of the smart city agenda, from the perspective of companies and politicians: public procurement rules; the lack of innovation-friendly laws; the regulation concerning land planning and use, the use of airspace in cities, and digital infrastructure (ABDI 2018, 36). This document argues in favour of the need to make legislative changes that would be corporate-friendly, favouring the acquisition and the use of technology through public-private partnerships, rather than via other forms of policymaking that could take social participation and safeguarding rights into account.

Framing regulations and public-private relations

Significant parts of the current smart city regulatory framework presented here were discussed and approved during the Workers' Party government in Brazil (2003–2016). On specifically internet governance topics, Presidents Lula da Silva and Dilma Rousseff organised public consultations and public hearings, opening up the possibility to draft bills with great support from civil society, such as the Civil Rights Framework for the Internet (*Marco Civil da Internet*) in 2014 and the General Data Protection Law (LGPD) in 2018 (which came into force in 2020). These legislative projects, created in a more collaborative fashion, were

celebrated as milestones by the international community. Several principles and practices incorporated into these legal instruments seemed, at least in the surface, hard to reverse. Nevertheless, since 1 January 2019, at the start of his mandate, Jair Bolsonaro has been rearranging the institutional framework of the federal government, usually in a controversial way, prioritising an overall approach of privatisation and deregulation, combined with a consistent disrespect for democratic institutions such as the Congress and the Supreme Court.

Policymaking infrastructure has also changed drastically under Bolsonaro. Besides a weakened bureaucracy, poorly regulated lobbying, and a heavier reliance on the private sector, the current government also has been pursuing an agenda that seeks to tackle so-called gender ideology in domestic and foreign policy (Folha de S. Paulo 2019b) and policies seem as leftist. It is necessary to highlight that although formally considered a democratic country as of December 2020, democracy in Brazil has been weakened and is under threat (Waldron 2019; Neiburg and Thomaz 2020; Pinheiro-Machado and Scalco 2020), with local communities claiming the clear transition to an authoritarian regime is in the offing, characterised by rampant censorship, critical budget cuts, and an ongoing institutional crisis. Bolsonaro has been issuing hundreds of decrees; among the measures taken we can highlight the creation of a national database with citizens' data, the increasing levels of confidentiality for public data, and the extinction of federal councils featuring civil society participation. A coalition of organisations affirm that "legislating through decrees, undermining the role of the Congress in a democratic regime, is a way of undermining democracy from within" (Rede Brasil Atual 2019).

One of the most notable examples of these tendencies, and one which touches directly on the topic of smart city regulation, is Bolsonaro's decision to discontinue the Ministry of Cities (*Ministério das Cidades*) on his first day in office, as part of a larger move to "undo many of his predecessors' legacies" (Scruggs 2019). The Ministry of Cities was created to fight urban inequalities and, before it was terminated (alongside other portfolios that were shuffled into "larger bureaucracies" (Scruggs 2019), it was responsible for institutionalising, at the federal level, a regulatory framework and a broader view of the municipalities in the country. Its destruction was heavily criticised: An opinion article in the United Kingdom's *The Guardian* newspaper called it the end of an "urbanist dream" (Scruggs 2019). In addition, the president has been financially suffocating regions that publicly oppose his government. Politics around city budgets have always existed, only not with such direct threats. This is a sensitive issue, especially in a country where most of the municipalities cannot thrive without provincial and federal funding, thus forcing them to look for private partnerships. And without the guidance and financial support from the Ministry of Cities, smaller municipalities will face even more challenges during the next years of Bolsonaro's mandate.

As will be discussed later, one of the main issues pointed out by interviewees in all sectors is the lack of continuity of policies when the federal, state, or municipal government change hands. This non-continuity affects programs that are already

running and staff who are removed from their positions, interrupting political agendas or even established projects.

The congressional agenda

The Brazilian urban ecosystem within which the smart cities agenda emerged is quite fragmented. It is composed of several actors, often with conflicting interests, which makes it challenging for governments to develop broader regulatory frameworks. One example worth mentioning is the Joint Parliamentary Front in Support of Smart and Human Cities (*Frente Parlamentar Mista em Apoio às Cidades Inteligentes e Humanas*), established in November 2016 at the Brazilian National Congress. Parliamentary fronts are formed by parliamentarians from various parties to debate a particular topic of interest to society and last for four years. Political lobbying in Brazil is largely unregulated, a reality that allows Parliamentary Fronts to often end up as bridges between Congress and non-state actors; many Fronts are actually created with significant moral and sometimes indirect financial support from companies and interest groups (Boldrini 2019). Legally, Parliamentary Fronts cannot access public money to fund their activities, as they have a reduced power compared to other congressional structures, such as committees.[9] In fact, the only power conferred to them by the regulation of the Chamber of Deputies is to require physical spaces for holding meetings. This situation offers industry and other well-funded groups an opportunity to influence Congress; experts warn that Brazil should properly regulate lobby to scrutinise how expenses, from dinners to research, are paid with money from companies whose stand to gain from what parliamentarians in these fronts decide (Simão 2019).

The Joint Parliamentary Front in Support of Smart and Human Cities, with 257 members, emerged as an effort to review current legislation, especially on topics concerning the public-private partnership law and possibilities of tax exemptions. All the smart city draft bills (PL 1.650/2015; 2.039/2015; 3.861/2015; 7.406/2014) supported by the Parliamentary Front as of this writing are still before Congress, with no final outcome in sight in the coming months. All of these bills were already at an advanced stage of processing and therefore, according to the Chamber's internal regulations, were not dismissed at the end of the last legislature (2015–2019). Its four-year mandate expired in January 2019. Despite the reelection of the leader of the Parliamentary Front in Support of Smart and Human Cities, it was discontinued, and the possibility of creating a New Parliamentary Front to deal with pressing smart cities issues has been under discussion.[10] A special subcommittee on smart cities seems to have taken advantage of the expiration of this Parliamentary Front.[11] Even if the initial discussions look promising, it is too early to evaluate their relevance or whether they will follow up on work from the previous front.

The case of the Parliamentary Fronts is but one example of how relations between state actors and the private sector take place, often without regulation, and with some interests hidden from the public eye. Another lesson to be taken

from this example is the ephemerality of certain legislative efforts, subject to specific mandates and multiple actors, making it more difficult to shape the agenda in the long term.

Public-Private Partnerships (PPPs)

In terms of power relations between state and non-state actors, a considerable amount of effort has been put into the flexibilisation of certain rules by companies willing to provide smart city services to municipal governments. The PPP Law has been one of the main priorities for the private sector when it comes to discussing smart cities in the country. The Brazilian public administration has engaged in PPPs for many years, but this practice was only made subject to specific regulations in 2004.

Brazilian smart cities have relied on PPPs for three primary reasons (Antunes 2017). The first is financial sustainability. That most of the country's municipalities cannot thrive without funding from the federal government and lack a sufficient tax base of their own creates room, or need, for greater private investment and involvement. The second reason revolves around the issue of technological integration: If local governments spread their purchases of smart city goods and services across different companies, they might run into interoperability issues. Implementing smart city policy and infrastructure via a PPP, in contrast, helps to circumvent these issues, because they will be working with a single vendor. Third, meanwhile, is the different speeds at which the public and private sectors operate: While the private sector can move quickly, public bureaucracies are slower; moreover, the government will only pay for the service once it is completed, creating a sense of urgency on the company's end.

In an interview, Henrique Frota, the executive coordinator of Instituto Polis, one of Brazil's leading organisation conducting public-interest research and advocacy on cities,[12] says that he believes the government's emphasis on PPPs has been

> disastrous, since it follows a logic of profitability, conflicting with the purpose of a public policy. . . . People usually try to frame PPPs through an econometric argument, presenting them as financial and regulatory designs that will cost less for municipalities. However, this design goes beyond the mere economic issue; it determines who is going to have access to the services being offered, or how the service will be integrated (or not) with the city.
>
> (Online interview, 9 May 2019).

In our research, we observed how PPPs are generally presented as the main instrument for the development of smart cities in Brazil, creating a direct exchange channel between the public and private sectors. Companies often approach mayors and public servants with offers to foster efficiency and smartness, which ends up generating top-down policies that exclude social participation. Without much social participation, this mechanism can lead to technologies and services being hired without a public debate as well as problematic consequences for the city in the long term, such as obsolescence, lack of maintenance, or even a dismissal of what would be considered a priority by its citizens.

Data governance: uncertainty and regulatory challenges

Beyond concerns about processes that lean heavily towards a disproportionate role for business in setting smart city policy, there are also individual policy issues at play. Privacy and data protection are often overlooked elements of smart city policy and the Brazilian data-governance policy as it will relate to smart cities remains a work in progress. In considering that status of Brazilian data governance, we can see how Brazil's previously strong record on public interest-focused, multistakeholder-led digital governance is being challenged by the political upheaval affecting the country as a whole.

Generally speaking, Brazil, however, has been making great strides with respect to data governance. Unlike much of the world outside of the European Union, Brazil was well-prepared to strengthen its data-governance measures following the March 2018 revelations of the Facebook–Cambridge Analytica scandal. The LGPD was approved in 2018 and came into force in 2020; it was the culmination of over a decade of Congressional and public debate and multistakeholder consultations. In the context of this chapter, the LGPD is significant because it has a section exclusively dedicated to the regulation of personal data processing by the government. Since the government is, in theory, responsible for formulating and implementing public policies for smart cities, this section in the law is relevant for data governance and for structuring further smart city initiatives.

Doneda and Mendes (2019, 336) write an engaging analysis of the Brazilian LGDP, in a broader context, highlighting how it fills an existing gap:

> The General Data Protection Law (LGDP) inaugurates in Brazil a general regime of personal data protection, complementing the Brazilian regulatory framework for an information society, together with the Access to Information Law, the Civil Rights Framework for the Internet, and the Consumer Defense Code [*Código de Defesa do Consumidor*] – thus modernising the information treatment in Brazil.
>
> (translated by the authors; see also Belli, Barros and Reia [2018] assess the previously existing Brazilian data-governance framework)

The process that led to the LGDP signed by former President Michel Temer in August 2018 involved years of debate among stakeholders. The section mentioned earlier, on the guidelines for personal data processing by the government, emerged amid a battleground between legislative and executive powers, with various vetoes and overrides (Agência Senado 2019). By the end of this process, four provisions addressing the guidelines for sharing data among public authorities were discarded, largely because officials argued that sharing data is a recurring and essential practice for the daily operation of the public administration; that is, including city halls that also suffer from queues and bureaucracy and see database integration as a solution.[13]

In addition, the LGDP includes principles of necessity, purpose, nondiscrimination, and transparency, with respect to data collection, as well as the obligation to adopt appropriate technical and administrative security measures when processing data. This means that data-driven projects should be designed to process as little personal data as possible, taking the necessary measures to perform it safely, while establishing clear communication with citizens.

The data protection authority, whose main goal is to safeguard and enforce data protection rules, may request public agents to publish personal data protection impact assessment reports and can suggest the adoption of standards and good practices for personal data processing by the government. Enforcement of these provisions, however, may not be as efficient because the creation of a National Data Protection Authority (*Autoridade Nacional de Proteção de Dados Pessoais*, ANPD) has been weakened by both Temer's and Bolsonaro's vetoes on some key measures. In this new text, the Authority will not be as independent as the first version envisaged. In its first two years, the ANPD will have a transitory structure being hierarchically subordinate to the cabinet of the presidency, thus endangering its autonomy. However, it may be transformed, at the discretion of the government, into an independent institution after the two-year trial period.

As currently envisioned, the ANPD will consist of a board of directors with five professionals appointed by the president. The Authority should be part of a multistakeholder[14] body set up to enforce the law and punish any abuses, such as data leakages, but its legitimacy and representativeness are in danger. In July 2020, less than one year before it was supposed to come into being, its members had yet to be appointed (Alves and Vieira 2020). Experts argue that the technical skills and plurality of ANPD Board members are critical for a successful data governance implementation and that each stakeholder group should be able to nominate its representative, thus ensuring legitimacy and representation of interests. More than 60 institutions, including business and academic associations, civil society organisations, and experts have issued a manifesto in defense of the composition of the ANPD (Urupá 2019).[15]

In parallel to the LGDP, the Senate approved, in July 2019, the Proposed Amendment to the Constitution (*Proposta de Emenda Constitucional*, PEC) 17/19, which expressly adds the right to the protection of personal data to the Brazilian Constitution. The PEC 17/19 is still being debated in the Chamber of Deputies; it proposes the inclusion of personal data protection as a fundamental right in the Constitution guaranteed to Brazilian citizens, a symbolic move to recognise the importance of this matter. More problematically, however, the proposal also reserves the power to legislate on personal data protection and processing exclusively to the federal level in order to avoid fragmentation, as well as it is necessary to avoid overlapping norms and legal uncertainty (Câmara dos Deputados 2019). As a result, municipalities and states will not be able to legislate about either the processing or the protection of personal data, thereby centralising and homogenising the efforts at the federal level in order to avoid "fragmentation and pulverisation" of the topic.

On 9 October 2019, Bolsonaro issued the controversial Decree 10.046, which provides regulation for data sharing within the federal public administration, and creates the Citizen Database Register (*Cadastro Base do Cidadã*), centralising several critical databases, such as citizens' biographical data, social insurance numbers, biometrics, among many others (Mari 2019a, 2019b). This initiative has drawn much criticism, from technical details to its conflicts with the LGPD. A database this large can become a source of concern if used to monitor or repress opponents by an authoritarian government, for instance. Also, this decree was created without further dialogue with civil society, going against a tradition in the country of debating digital culture with specialists and stakeholders.

The (de)centralisation of data governance is a subject that divides privacy advocates: On the one hand, we have those who affirm decentralisation can incentivise data companies to settle in cities where regulation is more lenient; on the other hand, specialists affirm that adherence of certain laws depends on specific regulations at the municipal level, where everyday life takes place and personal data governance is directly impacted. The latter is aligned with the fact that municipalities are already facing regulatory challenges with emergent technologies, such as ride-sharing apps, video monitoring, and live facial recognition. However, by leaving such regulation to the federal government, this situation effectively creates a regulatory roadblock when it comes to smart city data governance. Given the current composition and direction of the federal government, progressive changes are unlikely to happen in the short term as it relates to municipal smart city policies.

As the LGDP was just implemented as of this writing (in 2020), it is far too early to make a definitive statement about whether the LGDP and the PEC have the potential to create a progressive data-governance policy for Brazilian smart cities. The LGDP in particular reflects the multistakeholder nature of previous Brazilian digital policymaking. However, its delay – combined with the fact that the implementation of smart city technologies is already happening and the current government's contempt for engaging civil society – provides more than sufficient reason to temper optimism regarding the potential effectiveness of these new regulations on smart city development.

Local governance: corporate vs. citizen-led smart city policies

Below the federal level, and despite the governance challenges described earlier, some cities are investing in smart city regulation, including master plans, usually partnering with private consulting firms and companies. Three different examples worth highlighting are the municipal plans recently developed in Juazeiro do Norte, in the state of Ceará (a business-led process), and Campinas in São Paulo state (government-led with social participation), and the public wi-fi policy in the city of São Paulo (government-led with social participation).

A key example of a corporate actor partnering with a city on smart city governance is that of the SPin – a private consultancy firm specialising in smart cities solutions and PPPs – in the development of Juazeiro do Norte's Master Plan of Technologies for the Smart City (*Plano Diretor de Tecnologias da Cidade Inteligente*

de Juazeiro do Norte), which was approved by the city council in June 2018 as the Complementary Law 117/2018.[16] The plan lists priority areas such as urban mobility, public lighting, and basic sanitation; stipulates strategies for attracting investments; and mentions the importance of improving public services through the use of data-driven technologies. SPin's representatives and other consulting firms publicly affirmed they expected to create and implement similar plans in other cities in Brazil in the near future.

The Juazeiro-SPin plan focuses on PPPs, innovation, research, and technologies. It has an interesting approach to the smart city governance, such as stipulating various mechanisms for interactions among stakeholders (advisory councils, development funds, and infrastructure sharing) and, in particular, the provision of wi-fi connectivity (a source of valuable data for the service provider) as a municipal public service. However, in a glaring absence, despite the references to big data and the Internet of Things, there is not a single mention of privacy or data protection in the plan, showing it is not a priority for the private partners behind the legislation. Instead, the desire to maximise efficiency permeates the plan. For example, according to Article 28 of the Master Plan, services, such as public security, need to be provided to citizens and tourists and might be optimised through the creation of an Operational Control Centre (*Centro de Controle Operacional*, CCO). Operation centres usually rely on urban dashboards (Mattern 2015) and control rooms, in which screens allow real-time monitoring of the city. Public security is one of the main selling points of the smart city agenda, normally through video monitoring and live facial recognition technologies. Although such technologies are sold on the basis that they will help fight crime, it is well documented that the use of these kinds of apparatuses can promote segregation (Firmino et al. 2013; Evangelista et al. 2018).

Article 29 of the plan, meanwhile, focuses on funding in ways that create concerns regarding data collection and services. Among the foreseen means to fund smart city solutions are data mining, ads, or even charging fees from the users of these solution-oriented services. These measures reinforce the perception (and the choice to frame) data as a source of revenue for largely corporate gain rather than the broad benefit of the public.

In contrast to Juazeiro, the city of Campinas followed a different path in its attempt to join the smart cities agenda and engage the relevant stakeholders. It recently developed the Strategic Plan Campinas Smart City (*Plano Estratégico Campinas Cidade Inteligente*, PECCI), which was open for public consultation for almost two months (February and March) in 2019.[17] All stakeholders could submit their contributions to the plan by email, a practical attempt to engage all the actors involved in the formulation and implementation of a smart cities' agenda in the city. While Juazeiro do Norte's plan lacked any references to data protection, Campinas' plan, which again was the product of a multistakeholder consultation and not dominated by industry interests, contains measures relating to data protection, privacy, and cybersecurity. As well, Campinas' plan adopted "open source software that uses standards internationally accepted and validated by other municipalities" (Prefeitura Municipal de Campinas 2019, 38).

These two different cases show how cities in Brazil have a considerable degree of legislative autonomy and freedom to shape their regulatory frameworks. As different outcomes in these two cases suggest, the active participation of stakeholders in the formulation and implementation of smart city public policies can change how data governance is addressed. One of our interviewees, who worked at the Municipal Department of Innovation and Technology (*Secretaria Municipal de Inovação e Tecnologia*, SMIT) of the city of São Paulo, explained how the staff teamed up with the Brazilian Institute of Consumer Protection (*Instituto Brasileiro de Defesa do Consumidor*, IDEC), local law firms, and other advocacy groups while creating the public wi-fi policy for the municipality in 2019, called WiFi Livre SP (Interview, São Paulo, 2 May 2019).[18] This programme provides public, free access to the internet in more than 600 spots, especially in lower-income regions. Importantly, it respects the Civil Rights Framework for the Internet (*Marco Civil*) and the LGPD, as well as open-data initiatives.

Conferences and policymaking: from transnational corporations to local actors

The earlier section discussed the constraints and opportunities for cities in the face of the current Brazilian regulatory framework and policymaking process, with a prominent presence of corporate power shaping the smart city agenda. This section addresses the incentives for companies providing the smart city products and services.

The increase in the urban population over the last decades has drawn attention to the many challenges cities of all sizes face daily. Intra-country migration from rural to urban areas, a global challenge, is a relevant phenomenon in Brazil, which saw an increase in these migration trends after the 1970s. Some regions are more urbanised than the others, and Brazil has one of the largest cities in the world: São Paulo, whose metropolitan region has around 22 million inhabitants and is characterised as a megacity by the United Nations (2018).

Brazil's complexity – its 5,570 municipalities range in size from two megacities with more than 10 million inhabitants to small towns with fewer than 900 inhabitants each – drive a huge market for techno-solutionism and data-driven initiatives. Nonetheless, as expected with such diversity, there are no one-size-fits-all policies and products that would benefit Brazilian cities. A proper analysis of this multifaceted reality gets even trickier if one considers other variables, such as gender, race, access to the internet and to basic public services.

Brazil's digital divide remains a significant problem, as evidenced by the country's stubbornly low internet penetration rates. In 2019, around 71 percent of Brazilian households had access to the internet, according to the Regional Centre for Studies on the Development of the Information Society (*Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação*, Cetic.br). Digital divides remain marked in urban vs. rural areas (75 and 51 percent, respectively), in across regions, and by income – only 55 percent of the population whose monthly income is lower than the minimum wage has internet access at home. Eighty-five percent

of the population report having a cellphone (87 percent in urban areas; 69 percent in rural areas), but most of them have a pre-paid, cheaper option (62 percent), with only 33 percent of respondents holding a monthly plan (Cetic.br 2019).

Brazil's socio-economic gaps and troubling digital divides are an important backdrop against which the country's smart city industry operates. The business expos and conferences on smart cities in Brazil are crucial elements to understand the power relations among actors, from transnational corporations to local companies, allowing us to grasp the influence of corporate agendas on Brazilian smart city policy and outcomes. They are not only a space to showcase new products; these expos and conferences exist to create markets and demand.

In order to gain a deep understanding of the dynamics among participants, the corporate gatekeeping, and the priorities relating the Brazilian smart cities agenda, we conducted observation research and interviews at three expos and conferences: twice at Smart City Expo Curitiba (2018 and 2019); once at the Smart City Business America Congress and Expo (2018 in Sao Paulo); and once at the Connected Smart Cities (2018 in São Paulo). These smart cities events are sponsored mainly by both the private sector and state-owned enterprises. They normally happen once a year; we chose the ones we considered more relevant in terms of attendance, number of sponsors, the presence of mayors, and outcomes, such as smartness rankings.

The Smart City Expo Curitiba usually takes place annually around March at the Expo Barigui, a convention centre. It started in 2018, and it is co-organised by the company iCities, and Fira Barcelona, with Curitiba and Vale do Pinhão as the host city. The central role of companies and planning in organising the SCE Curitiba is remarkable; a representative of one of the organisers affirmed that his company established a partnership with Fira Barcelona in order to organise the Expo in Curitiba and successfully convinced the municipality to host the event (online interview, 30 April 2019).

The 2019 SCE Curitiba was sponsored and partnered by the federal and provincial governments, provincial state-owned enterprises (such as Copel and Sanepar), transnational companies (Cisco, Mastercard, Huawei), and several local companies. The cost of the tickets to access the event was high: The average price of admission to participate in workshops and talks was BRL 1,200 (US$225). This is unaffordable to most when one considers that the minimum wage in Brazil in 2019 was BRL 998 (US$187). The exhibition, however, where companies and other actors had their booths and showcased products and services, was free and open to the public. While anyone in theory can go and experiment with the new smart city technology, in practice the high admission costs means that the opportunity to hear and participate in the talks is out of range for most Brazilians.

In addition to the problem of affordability, when it comes to the workshops and presentations, both years of the Smart City Expo Curitiba lacked diversity in terms of gender, race, and ethnicity among its speakers, especially in the main sessions.[19] While the nuances and complexities of gender identity make it difficult to measure the average participation of women on panels, a general analysis of the programme shows for both years suggests that at least 70 percent of the speakers

were men. Our participant observation at the events also revealed a lack of participation by minority groups, such as LGBTQIA+ groups, people of colour, and Indigenous peoples in discussions that are supposed to shape the future of Brazilian cities. The high registration prices and the inaccessibility of these conferences to broader segments of the Brazilian society result in a lack of diversity of opinions, approaches, and a critical perspective on smartness.

Another issue encountered was the gatekeeping of important discussions, since these expos also offer the opportunity for meetings between companies and mayors in closed-door, invitation-only-access VIP rooms. As researchers, we did not have access to these meetings, nor did some of the civil society representatives whom we interviewed for this study. With few exceptions, decision making for smart cities in fora such as these leave segments of civil society out of the discussions and with them the ability to raise concerns in the public interest. According to Henrique Frota from Instituto Pólis:

> In my personal opinion, most of these [smart city] events operate as large markets to sell products and services. Technology corporations dealing with public security, surveillance, apps, from planning to health services, they want to sign contracts with the government. These events are not a priority for us, since they are shielded from our interventions, or even interventions from civil society. We are never invited to sit at their table.
>
> (Online interview, 9 May 2019)

The Smart City Business America Congress and Expo (SCBBr), meanwhile, took place in Sao Paulo in 2018, where its namesake organising institution is based. The SCBBr is the oldest smart cities event featured in this study and has been held in three cities in different regions of the country. The conference name changed slightly over the last few years, and the findings here draw from fieldwork conducted in 2018. The Smart City Business America Institute claims to be a not-for-profit organisation, constituted mostly by the private sector, with a focus on business and entrepreneurship for the smart cities ecosystem. It has branches throughout the Americas, and the Brazilian branch has Microsoft as one of its main sponsors. Its membership consists essentially of private-sector companies interested in the smart city market. The first edition of this expo was held in the city of Recife in 2012 with 250 participants. The expo has enjoyed remarkable growth: in the 2018 edition of the expo one covered in this study, organisers claimed 5,000 attendees. Similar to the lack of diversity among speakers in their conferences, the board and the technical board lack diversity – of its 31 representatives, only three are not men; most are white.[20] The lack of gender diversity was also evident in the panels that we observed, including several all-male panels. In one case, from four simultaneous parallel sessions, only 10 percent of the panelists were not men. The lack of diversity in these spaces of reflection and decision making reinforce exclusion and reproduce oppressions.

The Sao Paulo event revolved around showcasing products and services to potential buyers – especially mayors – and, since average people had little chance

to meaningfully participate, the weight of social participation or public interest was almost nonexistent. Between the main sponsors and partners, it is worth pointing out the presence of transnational corporations (Microsoft, Cisco, Intel, Engie), the federal government, "technoparks" (spaces dedicated to testing new smart city tech), and several companies (such as SPin). The prices to access the event were even more restrictive than those from Smart City Expo Curitiba; however, access to the exhibition area was not free and open to the public.

One other expo we covered in the course of our research was the annual Connected Smart Cities in São Paulo. Like the other expos, Connected Smart Cities promotes workshops and features an exhibition area for actors to showcase their products, services, and solutions. Admission prices were similar to the other two events. The structure of sponsorship of the expo was also similar to the other expos, with transnational corporations (Philips, Engie), ABDI, and domestic companies, including SPin, playing a prominent role. Unlike the other expos, this event offered more spaces for discussion with civil society and featured a call for papers for its workshops and panels. However, like the other expos, gender parity was far from ideal, with 74 percent of speakers featured by the expo being men.

All these events are relevant to comprehend the dynamics between state and non-state actors, as well as visibility and consolidation of the smart city agenda in Brazil. They provide rankings, showcase the technological novelties, create spaces for decision making, and reaffirm the corporate approach to smartness being implemented in our cities. Thousands of people every year attend these conferences, garnering them intense media coverage and fostering a smart city debate while civil society has been gradually excluded. Rodrigo Firmino, professor of Urban Management at PUCPR (Pontifical Catholic University of Paraná), in Curitiba, and a specialist in the relations between technology and politics, argues that "Most of these municipal projects are more concerned about efficiency than the right to the city" (online interview, 27 March 2019). He highlights that these conferences are facilitating the intense privatisation of spaces and services that should instead be preserved as a public good. In practice, by effectively excluding civil-society voices from these spaces, these expos and conferences exacerbate a corporate narrative of the smart city, leaving almost no room to reimagine that other notions of smartness and efficiency, more balanced and equal, are possible.

Whose voices are heard in the current smart city agenda?

The regulatory framework focused specifically on the smart city agenda is still incipient in the country; there are sparse initiatives, and both the Congress and the federal government are still struggling to address the subject. Brazil is likely to have, for now, a fragmented smart city governance, dependent on local efforts and stakeholders, thus creating room for large influence from the corporate narrative about what smartness should look like in a city. A narrow-minded view of technology has the potential to impact several municipal activities, and these impacts should be taken into account when discussing urban governance and smart cities. Top-down policies and regulatory frameworks detached from reality

will not contribute to tackling the challenges faced by Brazilian cities. Historical inequalities are still not being addressed by the current smart city agenda, such as access to housing, education, and sanitation; internet access; and police violence. Marginalised communities are often not benefiting from this corporate narrative, and they are negatively impacted, rarely being heard.

These problems are exacerbated by the trend of smart city technologies usually being implemented first, followed by conflicts, concerns and, only after all of this, regulation. In the absence of adequate regulation, cities have taken a reactive approach to the problems caused by smart city-style projects. In the near future, cities will have to deal with a myriad of regulatory and ethical challenges concerning tech policy and data governance. This future can be glimpsed in a couple of areas. The introduction of electric scooters in Rio and São Paulo forced the municipal governments to deal with the devices, accidents, and complaints, mobilising several city departments to control the issues that emerged less than a month after the private companies, Grow and Lime, had come to the respective towns. Specific regulation was created, and the companies decided to leave most of the Brazilian cities (Felix 2019). Another highly relevant example is the deployment of live facial recognition (LFR) technologies in cities across the country. LFR can be seen as the operationalisation of data regulation in Brazil, leading to privacy concerns connected to the smart cities agenda that are no longer new, which were broadly analysed in publications over the last years (Privacy International 2017; Gaffney and Robertson 2018). These issues are probably going to be exacerbated by the Covid-19 pandemic, as cities face the temptation to depend increasingly on surveillance technologies to control outbreaks. The use and anticipated spread of LFR in Brazil suggests why it is so problematic that data governance and privacy issues are often ignored in corporate-driven smart city initiatives, as in Juazeiro.

Hope lies in civil society organisations and qualified public servants whose jobs do not necessarily depend on elections – neither the transition of governments nor mandates. As affirmed by Luciana Pascarelli Santos, coordinator of the Geoinfo Program at the Municipal Department of Urbanism and Licensing (*Secretaria Municipal de Urbanismo e Licenciamento*, SMUL), it is crucial to bring together citizens to collaborate, since "a public administration is not the mayor defining what to do based on our information, but the population bringing ideas and helping to create solutions" (interview, São Paulo, 3 May 2019). Frota, from Instituto Polis, believes that

> the use of technology in cities does not need to be framed by the smart cities agenda; it needs to be implemented based on the notion of the right to the city and the radicalisation of democracy – questioning who are these technologies serving? And why?

Despite the current challenges triggered by the political turmoil and the unsettled convergence of social and economic issues in the country, there are still good lessons in terms of internet (and smart city) governance. The country has much to gain in the change of the federal government and in a broader, more inclusive

approach to the smart city agenda. We need to diversify the voices of those who are formulating and implementing smart city policies. The future of our cities cannot be left in the hands of technology corporations and dazzled mayors. Brazilians are leaders not only in internet governance but also in framing the right to the city movement worldwide. Our civil society and academia have been offering important analyses, studies, empirical data, and advocacy lessons that would greatly contribute to a better smart city governance for the country. It is fundamental to listen to them in the process.

Conclusion

The Brazilian case presented here is another step towards evidence-based research and advocacy on the implementation of the smart cities technopolitical agenda in the Global South. It addresses the urgency in converging agendas of urban planning and internet governance, while it points out the main challenges multistakeholderism is facing over the last years in Brazil. In this complex ecosystem, state and non-state actors navigate amid conflicting interests and an ever-changing regulatory framework. Once a leader in digital policy, Brazil is confronted with the consequences of Bolsonaro's election in 2018, in which parts of the Brazilian civil society saw their priorities shift from a positive agenda to continuous efforts to guarantee fundamental rights. This could, however, shift with a new administration in Brazil.

The country offers a rather attractive market for smart solutions, making the smart city agenda already a reality in many municipalities, with consulting firms and PPPs gaining a central role, and leaving few opportunities for broader social participation. Regulation tries to tackle many emergent issues; however, we often see that technology is usually implemented first, followed by conflicts, concerns, and then regulation. The asynchronous timing among innovation, policy, advocacy, and legislation leaves gaps that have been mostly filled out by the private sector. To make matters worse, the current authoritarian federal government threatens to emphasise disproportionately the private sector and transnational corporations, thus weakening multistakeholderism as well as citizens' wellbeing.

In Brazil, the current regulatory framework is still not sufficient to contain most of the problems that appeared with the implementation of the smart city agenda. It is necessary to discuss the consequences of transferring the management of our cities and the responsibility of data governance to the private sector – and important decisions should never be made without public consultations or behind closed doors. More than ever, internet governance and urban governance agendas should establish a dialogue and gather specialists, practitioners, and advocates to work together towards an idea of smartness/intelligence that is more aligned with the right to the city. Additionally, there is a crucial need for further research and advocacy around this topic, in order to ensure that the smart city agenda will not be used as another mechanism that reproduces exclusion and discrimination in the country.

Acknowledgments

This work was supported by the Open Society Foundations (OSF) and developed at the Center for Technology and Society at FGV Law School (CTS-FGV) in Rio de Janeiro, Brazil, under the name "Discrimination and Data Control in Brazilian Smart Cities." It was coordinated by Jhessica Reia and Luca Belli, and it had the generous contribution of other researchers: Tatiana Murta and Victor Caldas. We want to thank Pedro A.P. Francisco, Will Straw, and Filipa Pajević for their significant inputs to the final draft of this chapter.

Notes

1 The Internet Governance Forum had its firsts workshops addressing smart cities in 2016. There were three in 2016, two in 2017, one in 2018, and one in 2019.
2 See http://habitat3.org/the-new-urban-agenda/.
3 See HABITAT III. Comments from Brazil to the issue papers that will inform the discussions of the UN Habitat III Conference. Available at: http://habitat3.org/wp-content/uploads/BRASIL-Comments-on-Habitat-III-Issue-Papers.pdf.
4 See, for example, *Observatório da Privacidade* [*Privacy Observatory*] (https://observatorioprivacidade.com.br/memorias/) and the report published by InternetLab's team in 2016, available at: www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf.
5 While these three cities are particular cases that do not reflect the whole country in its entirety, they are significant examples of global cities that embraced a specific agenda on how "smartness" should operate and be intertwined in their infrastructures.
6 See, for example, discussions around "informational city" (Castells 1989); "ubicomp" (Weiser 1996); "media city" (McQuire 2008); Communicative City (Gumpert and Drucker 2008); among others.
7 See www.curitiba.pr.gov.br/noticias/prefeitos-assinam-compromisso-de-curitiba-com-intencoes-para-cidades-inteligentes/36488.
8 The Brazilian Agency for Industrial Development is a federal government agency whose mission is to promote the implementation of industrial policies.
9 Ato da Mesa n° 69, 2005, available at: https://www2.camara.leg.br/legin/int/atomes/2005/atodamesa-69-10-novembro-2005-539350-publicacaooriginal-37793-cd-mesa.html.
10 See www.diariodepetropolis.com.br/integra/petropolis-presente-no-smart-city-day-166775.
11 See https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdu/conheca-a-comissao/subcomissoes.
12 See https://polis.org.br/.
13 See www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm.
14 The Authority should have a consultative council formed by state and non-state actors, such as representatives of the Senate, Congress, Public Prosecutor's Office, Internet Steering Committee, civil society, academia, unions, and the private sector.
15 On October 15, 2020, President Bolsonaro nominated the five members of the ANPD. As feared by different stakeholders, three of the nominees are members of the Armed Forces. The militarisation of the ANPD is a problem, as it might not have the public interest, multistakeholder approach desired by civil society and the private sector.
16 For the complete material, see www.juazeiro.ce.gov.br/Imprensa/Diario-Oficial/Num4762-14062018/.
17 The document made available for public consultation can be found here: www.campinas.sp.gov.br/arquivos/desenvolvimento-economico/pecc-2019-2029.pdf.
18 For further information, see https://wifilivre.sp.gov.br/.

19 See, for example, the reports from 2018 (www.smartcityexpocuritiba.com/Relatorio_SCECWB18.pdf) and 2019 (www.smartcityexpocuritiba.com/Report_SCECWB19.pdf).
20 More information can be found here: https://web.archive.org/web/20190108192233/http://smartcitybusiness.com.br/home/conselho/.

References

ABDI. 2018. *Cidades Inteligentes: Oportunidades e Desafios para o Estímulo ao Setor no Brasil* [*Smart Cities: Opportunities and Challenges to Foster the Sector in Brazil*]. http://inteligencia.abdi.com.br/wp-content/uploads/2017/08/2018-09-11_ABDI_relatorio_5_cidades-inteligentes-oportunidades-e-desafios-para-o-estimulo-ao-setor-no-brasil_WEB.pdf.

Agência Senado. 2019. "Congresso conclui análise de vetos sobre proteção de dados [Congress Concludes Analysis of Data Protection Vetoes]." *Senado Notícias*. 2 October. https://www12.senado.leg.br/noticias/materias/2019/10/02/congresso-conclui-analise-de-vetos-sobre-protecao-de-dados. Accessed 5 August 2020.

Alves, Fabricio M., and Gustavo A.S. Vieira. 2020. "Sem a ANPD, a LGPD é um problema, não uma solução [Without the ANPD, the LGPD Is a Problem, Not a Solution]." *Jota*. 6 January. https://perma.cc/EVZ3-RMLR. Accessed 5 August 2020.

Antunes, Vitor. 2017. *Parceiras Público-Privadas Para Smart Cities* [*Public-Private Partnerships for Smart Cities*]. 2nd ed. Rio de Janeiro: Lumen Juris.

Arnaudo, Daniel. 2017. "Brasil e o Marco Civil da Internet: O Estado da Governança Digital Brasileira [Brazil and the Civil Rights Framework for the Internet: The State of the Brazilian Digital Governance]." *Artigo Estratégico* 25. https://igarape.org.br/marcocivil/assets/downloads/igarape_o-brasil-e-o-marco-civil-da-internet.pdf.

Balbim, Renato. 2017. "A geopolítica das cidades e a Nova Agenda Urbana. [The Geopolitics of Cities and the New Urban Agenda]." *IPEA – Boletim Regional, Urbano e Ambiental*. http://repositorio.ipea.gov.br/bitstream/11058/8139/1/BRU_n17_Geopol%C3%ADtica.pdf.

Belli, Luca, Marina Barros, and Jhessica Reia. 2018. "Les enjeux de l'encadrement et de la gouvernance de l'ouverture des données publiques au Brésil." *Revue française d'administration publique* 167 (3): 585–600.

Boldrini, Angela. 2019. "Sem atuação efetiva, frentes parlamentares proliferam no Congresso [Without Effective Action, Parliamentary Fronts Proliferate in Congress]." *Folha de S. Paulo*. 29 April. https://www1.folha.uol.com.br/poder/2019/04/sem-atuacao-efetiva-frentes-parlamentares-proliferam-no-congresso.shtml.

Câmara dos Deputados. 2019. *Relatório da PEC n° 17/2019 – Proteção de dados pessoais* [*Report on the Proposed Amendment to the Constitution n. 17/2019 – Personal Data Protection*]. www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1786699&filename=PRL+1+CCJC+%3D%3E+PEC+17/2019.

Cardullo, Paolo, and Rob Kitchin. 2019. "Being a 'Citizen' in the Smart City: Up and Down the Scaffold of Smart Citizen Participation in Dublin, Ireland." *GeoJournal* 84 (1): 1–13. https://doi.org/10.1007/s10708-018-9845-8.

Castells, Manuel. 1989. *The Informational City*. Oxford and Cambridge: Blackwell.

Cetic.br. 2019. *Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros – TIC Domicílios 2019* [*ICT Households survey 2019*]. www.cetic.br/pesquisa/domicilios/indicadores.

Doneda, Danilo, and Laura Schertel Mendes. 2019. "Um perfil da nova Lei Geral de Proteção de Dados brasileira [A Profile of the New Brazilian General Data Protection Law]." In *Governança e regulações da Internet na América Latina* [*Internet Governance*

and Regulations in Latin America], edited by Luca Belli and Olga Cavalli. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas.

Evangelista, Rafael de A., Tiago C. Soares, Sarah C. Schmidt, and Felipe Lavignatti. 2018. "DIO: o mapeamento coletivo de câmeras de vigilância como visibilização da informatização do espaço urbano [Digital Infomation Operative: A Mobile Game to Map Surveillance câmeras]." *Tecnopolíticas da vigilância: perspectivas da margem*, edited by Fernanda Bruno, Bruno Cardoso, Marta Kanashiro, Luciana Guilhon, and Lucas Melgaço. São Paulo: Boitempo.

Felix, Paula. 2019. "Em SP, patinetes somem das ruas após novas regras de uso [In São Paulo, Electric Scooters Disappear from the Streets Following New Regulation]." *Terra*. 2 June. www.terra.com.br/noticias/brasil/cidades/em-sp-patinetes-somem-das-ruas-apos-novas-regras-de-uso,b41178b78d8fd70eef2c990cc2971a0erqvo1qsc.html. Accessed 5 August 2020.

Firmino, Rodrigo J., Marta Kanashiro, Fernanda Bruno, Rafael Evangelista, and Liliane da Costa Nascimento. 2013. "Fear, Security, and the Spread of CCTV in Brazilian Cities: Legislation, Debate, and the Market." *Journal of Urban Technology* 20 (3): 65–84. https://doi.org/10.1080/10630732.2013.809221.

Folha de S. Paulo. 2019a. "Entenda o uso do WhatsApp nas eleições e o que aconteceu desde que a Folha revelou o caso [Understand the Use of WhatsApp in the Elections and What Has Happened Since Folha Revealed the Case]." *Folha de S. Paulo*. 8 October. https://www1.folha.uol.com.br/poder/2019/10/entenda-o-uso-do-whatsapp-nas-eleicoes-e-o-que-aconteceu-desde-que-a-folha-revelou-o-caso.shtml. Accessed 5 August 2020.

Folha de S. Paulo. 2019b. "Brazilian Government's War Against 'Gender Ideology' Arrives in Foreign Policy." *Folha de S. Paulo*. 26 June. https://www1.folha.uol.com.br/internacional/en/world/2019/06/brazilian-governments-war-against-gender-ideology-arrives-in-foreign-policy.shtml. Accessed 5 August 2020.

Gaffney, Christopher, and Cerianne Robertson. 2018. "Smarter Than Smart: Rio de Janeiro's Flawed Emergence as a Smart City." *Journal of Urban Technology* 25 (3): 47–64. https://doi.org/10.1080/10630732.2015.1102423.

Gumpert, Gary, and Susan J. Drucker. 2008. "Communicative Cities." *The International Communication Gazette* 70 (3–4): 195–208. https://doi.org/10.1177/1748048508089947.

Kitchin, Rob. 2014. "The Real-Time City? Big Data and Smart Urbanism." *GeoJournal* 79: 1–14. https://doi.org/10.1007/s10708-013-9516-8.

Kitchin, Rob. 2015. "Making Sense of Smart Cities: Addressing Present Shortcomings." *Cambridge Journal of Regions, Economy and Society* 8 (1): 131–136. https://doi.org/10.1093/cjres/rsu027.

Kitchin, Rob, Tracey Lauriault, and Gavin Cardle, eds. 2018. *Data and the City*. Nova York and Oxon: Routledge.

Kurban, Can, Ismael Peña-López, and Maria Haberer. 2017. "What is Technopolitics? A Conceptual Scheme for Understanding Politics in the Digital Age." *IDP. Revista de Internet, Derecho y Ciencia Política* [*Internet, Law, and Political Science Review*] 24: 3–20. http://dx.doi.org/10.7238/idp.v0i23.3061.

Mari, Angelica. 2019a. "Brazilian Government to Create Single Citizen Database." *ZD Net*. 11 October. https://zd.net/2NklVkj. Accessed 5 August 2020.

Mari, Angelica. 2019b. "Brazilian Citizen Data under Threat with Sale of National Tech Firms." *ZD Net*. 31 August. https://zd.net/2BRJEDa. Accessed 5 August 2020.

Mattern, Shannon. 2015. "Mission Control: A History of the Urban Dashboard." *Places Journal*. March. https://doi.org/10.22269/150309.

Mattern, Shannon. 2017a. *Code and Clay, Data and Dirt: Five Thousand Years of Urban Media*. Minneapolis: University of Minnesota Press.

Mattern, Shannon. 2017b. "A City Is Not a Computer." *Places Journal*. February. https://doi.org/10.22269/170207.

McQuire, Scott. 2008. *The Media City*. London: Sage Publications.

Morozov, Evgeny, and Francesca Bria. 2018. "Rethink the Smart City: Democratizing Urban Technology." *Rosa Luxemburg Stiftung*. www.rosalux-nyc.org/wp-content/files_mf/morozovandbria_eng_final55.pdf.

Neiburg, Federico, and Omar R. Thomaz. 2020. "Ethnographic Views of Brazil's (New) Authoritarian Turn." *HAU: Journal of Ethnographic Theory* 10 (1): 7–11. https://doi.org/10.1086/708670.

Niaros, Vasilis. 2016. "Introducing a Taxonomy of the 'Smart City': Towards a Commons-Oriented Approach?" *Triple-C*. 14 (1): 51–61. https://doi.org/10.31269/triplec.v14i1.718.

Papp, Anna Carolina. 2014. *Em nome da internet: Os bastidores da construção coletiva do Marco Civil* [*In the name of the internet: Behind the scenes of the Civil Rights Framework's collective construction*]. Undergraduate thesis, Department of Communication Studies, University of Sao Paulo. https://issuu.com/annacarolinapapp/docs/em_nome_da_internet.

Pinheiro-Machado, Rosana, and Lucia M. Scalco. 2020. "From Hope to Hate: The Rise of Conservative Subjectivity in Brazil." *HAU: Journal of Ethnographic Theory* 10 (1): 21–31. https://doi.org/10.1086/708627.

Pires, Maria C.S. 2005. "O município no federalismo brasileiro: constrangimentos e perspectivas [The Municipality in the Brazilian Federalism: Constraints and Perspectives]." *Cadernos da Escola do Legislativo* 8 (13): 55–84.

Prefeitura Municipal de Campinas. 2019. *Plano Estratégico Campinas Cidade Inteligente 2019–2029*. [*Strategic Plan Campinas Smart City 2019–2029*]. www.campinas.sp.gov.br/arquivos/desenvolvimento-economico/pecc-2019-2029.pdf.

Privacy International. 2017. *Smart Cities: Utopian Vision, Dystopian Reality*. https://privacyinternational.org/report/638/smart-cities – utopian-vision-dystopian-reality.

Rede Brasil Atual. 2019. "'Governar por decretos é minar a democracia': entidades criticam 'postura autocrática' de Bolsonaro [To Govern by Decrees Is to Undermine Democracy: Entities Criticize Bolsonaro's 'Autocratic Stance']." *Rede Brasil Atual*. 31 May. www.redebrasilatual.com.br/politica/2019/05/decretos-presidenciais-democracia/. Accessed 5 August 2020.

Reia, Jhessica. 2019. "O direito à cidade (inteligente): Tecnologias, regulação e a Nova Agenda Urbana [The Right to the (Smart) City: Technologies, Regulation, and the New Urban Agenda]." In *Horizonte Presente: Tecnologia e Sociedade em debate* [*Current Horizons: Debates on Technology and Society*], edited by Jhessica Reia, Pedro Augusto P. Francisco, Marina Barros, and Eduardo Magrani. Rio de Janeiro: Editora Letramento. https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27448/Horizonte%20presente%20-%20tecnologia%20e%20sociedade%20em%20debate.pdf?sequence=1&isAllowed=y. Accessed 11 August 2020.

Reia, Jhessica, and Pedro Mizukami. 2015. "Reformando a lei de direitos autorais: desafios para o novo governo na área da cultura [Reforming the Copyright Law: Culture Related Challenges for the New Government]." *RECIIS – Revista Eletrônica de Comunicação, Informação e Inovação em Saúde* 9 (1). https://doi.org/10.29397/reciis.v9i1.923.

Sadowski, Jathan, and Roy Bendor. 2019. "Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary." *Science, Technology, & Human Values* 44 (3): 540–563. https://doi.org/10.1177/0162243918806061.

Scruggs, Gregory. 2019. "Ministry of Cities RIP: The Sad Story of Brazil's Great Urban Experiment." *The Guardian*. 18 July. www.theguardian.com/cities/2019/jul/18/ministry-of-cities-rip-the-sad-story-of-brazils-great-urban-experiment. Accessed 5 August 2020.

Simão, Valdir. 2019. "Frente fria: por uma lei das frentes parlamentares [Cold Front: A Law for the Parliamentary Fronts]." *Folha de S. Paulo*. 3 April. https://www1.folha.uol.com.br/opiniao/2019/04/frente-fria-por-uma-lei-das-frentes-parlamentares.shtml. Accessed 5 August 2020.

Söderström, Ola, Till Paasche, and Francisco Klauser. 2014. "Smart Cities as Corporate Storytelling." *City* 18 (3): 307–320. https://doi.org/10.1080/13604813.2014.906716.

Souza, Carlos A.P., Marília Maciel, and Pedro A. Francisco. 2010. "Marco Civil da Internet: uma questão de princípio [Brazilian Civil Rights Framework for the Internet: A Matter of Principle]." *PoliTICs* 7. https://politics.org.br/edicoes/marco-civil-da-internet-uma-quest%C3%A3o-de-princ%C3%ADpio.

Townsend, Andrew. 2013 *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia*. New York: W.W. Norton.

United Nations. 2015. *HABITAT III Issue Paper 21 – Smart Cities*. http://habitat3.org/wp-content/uploads/Habitat-III-Issue-Paper-21_Smart-Cities-2.0.pdf.

United Nations. 2018. *World Urbanization Prospects: The 2018 Revision*. Department of Economic and Social Affairs, Population Division. Online Edition. https://esa.un.org/unpd/wup/Publications/Files/WUP2018-KeyFacts.pdf.

Urupá, Marcos. 2019. "ANPD poderá ter Conselho Diretor nomeado até o final do ano [National Data Protection Authority May Have Its Board Appointed by the End of the Year]." *Teletime*. 6 August. https://teletime.com.br/06/08/2019/anpd-podera-ter-conselho-diretor-nomeado-ate-o-final-do-ano/. Accessed 5 August 2020.

Waldron, Travis. 2019. "Brazil is about to Show the World How a Modern Democracy Collapses." *Huffington Post*. 1 January. www.huffingtonpost.ca/entry/brazil-jair-bolsonaro-democracy-threat_n_5c2a30c5e4b08aaf7a929cbb?ri18n=true&guccounter=1. Accessed 5 August 2020.

Weiser, Mark. 1996. Ubiquitous Computing. Last modified 17 March. http://web.archive.org/web/20070202035810/www.ubiq.com/hypertext/weiser/UbiHome.html. Accessed 5 August 2020.

Winner, Langdon. 1980. "Do Artifacts Have Politics?" *Daedalus* 109 (1): 121–136.

Conclusion

State power (and its limits) in internet governance

Natasha Tusikov, Blayne Haggart and Jan Aart Scholte

As set out in our introductory chapter, this volume has asked (a) in what ways and to what extent do (and might) we see increased state involvement in contemporary internet governance and (b) under what conditions can that greater government role in the internet be a good or a bad thing? As seen throughout the book, the question of what role the state is playing (and should play) in internet governance holds particular salience today. Neoliberal ideas of the minimalist state, so in vogue at the dawn of the global internet, are now in decline, and great-power competition is on the rise in digital arenas and generally. Some even see a real possibility that the internet splinters along territorial-state borders.

The ten preceding chapters have explored these questions from various disciplinary and theoretical perspectives, covering concrete circumstances in diverse world regions and addressing different aspects of the internet, including infrastructure, data and content. Recurrent major themes have involved debates between multilateralism and multistakeholderism, differences and similarities between authoritarian and democratic states, and the relationship between the state and (global) digital capitalism.

It is now time, in closing the book, to bring together insights from the various chapters to offer some overall conclusions about the role of the state in internet governance today and into the future. We highlight five main points. First, current trends show widespread state attempts to exert greater control in internet governance, and these government initiatives often conflict with the private regimes that have previously dominated in areas such as internet infrastructure. Second, business plays significant constraining and enabling roles in shaping state power vis-à-vis the internet. Third, both authoritarian and democratic states (in different ways and to different degrees) face technical, social and economic limitations when they seek to exert "sovereignty" in internet governance. Fourth, multistakeholder internet governance in practice often puts both state and civil society actors in a secondary role behind business and technical interests. Fifth, the US government continues to have a consequential role in the overall regime complex for internet governance. We end with thoughts on future lines of research concerning the role of the state in internet governance.

DOI: 10.4324/9781003008309-15

Increased state intervention

The first part of this volume focused on the role of the state writ large in internet governance, while later parts looked at country- and region-specific case studies. The desire, even need, of states to exert their influence over the internet in the pursuit of a wide range of policy objects is a recurring theme throughout the book. As chapters by Chenou and ten Oever particularly remind us, state involvement in internet governance is not necessarily authoritarian or anti-democratic, although that is sometimes the case. As ten Oever notes, state involvement in internet governance generally arises when governments prioritise policy objectives other than interoperability and connectivity, as have predominated in private internet governance.

These broader policy objectives can include regime stability (e.g., in China and Russia), collection of domestic data and content governance (e.g., in China, Russia and Latin America), and policing of societally harmful disinformation (e.g., in the European Union, EU). In addition, as chapters by Chenou and Ciurak and Ptashkina especially indicate, state concerns with economic prosperity increasingly drive government interventions in the digital economy, including (as seen in chapters on China and Russia) to cultivate a domestic technology industry. From another angle, as the chapter by ten Oever particularly underlines, state involvement can pursue human rights concerns that private regimes of internet governance have often been slow to address. Thus, increased state involvement has considerably widened the scope of internet governance beyond narrow technical matters to a full range of economic and social matters.

Whereas the pursuit of "digital sovereignty", however that notion may be defined, is more commonly associated with authoritarian states, the chapters by Rone, Chenou, and Reia and Fergus Cruz show that democratic states also have political and economic motivations to control flows of information and data within their jurisdictions. Similar to the authoritarian states discussed in the volume, the democratic states under analysis also operate within distinct socio-economic and political contexts that shape their interests in and capacity to govern the internet (see, e.g., Glasius and Michaelsen 2018). While not all of the objectives pursued by states may be positive or considered legitimate – suppression of political speech is still suppression of political speech – states are uniquely positioned in global society to reconcile diverse and often-conflicting values and policy goals.

States and/versus markets

As various chapters across our volume have also shown, the assumption of a hard and fast line between authoritarian and democratic states buckles somewhat when one scrutinises their relationship to markets and digital capitalism. We have repeatedly seen that companies substantially construct and constrain state power in internet governance. Of particular significance are internet firms that provide vital digital hardware and software. The influence that the state can exert in internet governance depends in good part on the degree to which it controls key corporate actors operating on its territory.

In both democratic and authoritarian countries, state and market actors have a symbiotic relationship regarding the internet. Consider the issue of surveillance and content regulation. Governments, whether democratic or authoritarian, require some degree of cooperation from technology companies that supply the software and hardware that underpins content filtering, cloud storage and data analytics systems that compose state surveillance programmes.

State-corporate configurations are evident in democratic countries (Lyon 2014). The Snowden files expose deep interdependent relationships between major US-based internet firms and the US government, along with key American allies like the United Kingdom. Some scholars have referred in this regard to an "information-industrial complex" (Powers and Jablonski 2015, 47; Greenwald 2014). In the US, this complex involves mutual benefits: The government obtains surveillance technologies for national security programmes from the companies; and the companies obtain lucrative contracts as well as support from US policies on international trade and investment (Powers and Jablonski 2015). In Brazil, Reia and Fergus Cruz find that industry—particularly in the form of foreign multinationals—plays a dominant role with government policymakers in shaping policies towards market-friendly "smart cities".

State-corporate alliances to facilitate government surveillance programs are also evident in authoritarian countries. China's extensive systems of domestic surveillance, social control and online censorship fundamentally rely upon its technology companies who provide and operate the hardware and software that compose these systems. Given China's long-term protectionist measures and prohibitions on many foreign technology platforms and applications, along with incentive programs for domestic firms (see, e.g., Plantin and de Seta 2019), the country has a stable of domestic technology champions that the Chinese government can enroll to facilitate its policies. Yet this relationship involves more than direct state control over industry: It is a symbiotic partnership between the Chinese government and its commercial internet firms (Jiang and Fu 2018; Shen 2016). As our contributions from Jia and Luo and Lv highlight, the Chinese state depends on its for-profit platforms to deliver not just security, but also economic prosperity, which provides these platforms with notable room to manoeuvre with respect to the government.

Our chapters have revealed contrasting experiences between China and Russia when it comes to relations with foreign (specifically US-based) internet companies. In China, the state's overriding power is evident. The government has long restricted or entirely blocked access to platforms and applications like Facebook, Twitter, Instagram and Snapchat (Plantin and de Seta 2019). In contrast, the Russian case illustrates the difficulty that states can face when trying to regulate large multinational internet firms in respect of content and data. Stadnik's chapter describes the Russian government's raft of legislation and policies that aim at extending government control over internet infrastructure and industry operators. Yet while these measures have forced compliance from domestic firms, foreign companies (particularly large US-based firms) have refused to yield, so highlighting a major shortfall in the government's power.

Dynamics of cooperation and conflict between the state and companies also mark efforts to regulate internet content in democratic countries. Companies may have various motivations for participating in state-led regulation. Firms may also create their own rules or processes to preempt possible government regulation or to water down existing rules (Black 2008; Büthe 2010; Cutler, Haufler and Porter 1999). As Rone's chapter finds, one cannot assume that technology companies always cooperate with democratic governments in addressing online disinformation. Facebook, in particular, has posed particular challenges for EU efforts to regulate in this area (Schmidt and Dupont-Nivet 2019). Rone notes that, with "preemptive cooperation," market actors participate in the lawmaking process in order to make regulation as weak and flexible as possible. Corporate actors might also adopt private rules to repair or safeguard their reputations. For example, following the Cambridge Analytica scandal and the United Nations finding that Facebook contributed to the genocide in Myanmar (Human Rights Council 2018), the company may be motivated, at least in part, to attempt to restore its damaged image. Platforms also engage in what Rone terms "conflictual cooperation", where companies decline to join with regulators or attempt actively to defy or subvert regulations. Rone's account of the EU disinformation campaign underlines the difficulty of involving corporate actors whose interests conflict with the regulation. For example, Google and Facebook fundamentally oppose independent assessment, let alone reform, of their algorithm-powered business models.

Limits to sovereignty

Another important overall finding in this volume is that state control over the internet confronts limitations. In addition to the inability always to compel transnational firms to comply with government rules, state power also faces technical constraints and competing priorities for economic growth. Both democratic and authoritarian states encounter significant, although differing, challenges in asserting their would-be sovereignty vis-à-vis the internet.

Technical limitations of state power are nicely captured in Santaniello's assessment of French President Emmanuel Macron's speech to the Internet Governance Forum (IGF). As Santaniello points out, Macron's examples focused more on content, rather than the engineering infrastructure of the internet, where it is difficult to envision private regulation giving way to sovereign state control. Technical limitations to state power also figure in Stadnik's description of the Russian government's desires to enact a form of autarkic "information sovereignty". Here, the authoritarian spirit may be willing, but the state lacks the capacity to achieve the aim. Similarly, Rone in her chapter on the EU explains that governments often lack the resources and technical expertise to compel platforms to comply with state rules.

Another major limitation on the involvement of democratic states in internet governance involves the issue of legitimacy. As Rone shows, legitimacy problems emerge from limited democratic participation in EU rule-making around internet content. These processes tend to sideline elected officials and to lack a broad

public consensus on how to regulate the issue. This absence of perceived legitimacy hampered efforts by the French government to introduce legislation to counter disinformation and the UK government's white paper to address online harms: Both cases aroused charges of censorship. Public perception of legitimacy, Rone contends, is paramount, requiring governments to ensure democratic participation and popular acceptance. Private actors' involvement in internet governance – and associated concerns about a conflict of interest – can also hamper legitimacy. After all, the EU relies on the platforms themselves to address disinformation, which raises questions of transparency, accountability and anti-competitive practices.

In contrast, authoritarian states can often skirt questions of democratic legitimacy in internet governance, so long as they have the coercive power necessary to implement rules and compel compliance. As Luo and Lv point out, even seemingly apolitical issues around the internet can fall under the heavy hand of the authoritarian Chinese government if these matters are seen to challenge the security of the state and the Communist Party (which are usually treated as one and the same). In practice there is no limit to the scope of what the government can define as a "security" concern.

Yet perhaps the most significant limitation on state sovereignty vis-à-vis the internet lies with economic factors. As set out in the book's introduction and detailed in several subsequent chapters, both democratic and authoritarian states are embedded in larger forces of global capitalism, which deeply affects how governments perceive their role in regulating the internet. Both Chenou and Ciuriak and Ptashkina firmly embed questions internet governance – in particular data governance – within the larger structure of global capitalism. As Chenou points out, Latin American countries are responding to the nature of the global digital capitalist system according to their particular historical and institutional context. This dynamic also plays out in Reia and Fergus Cruz's discussion of Brazilian data governance in the context of the smart city.

The pervasiveness of global capitalism also figures in the case studies of China and Russia. The chapters by Stadnik, Jia, and Luo and Lv demonstrate that the power of the corporate sector is not limited to democratic countries. Even in China, the paradigmatic example of state domination over the internet, government does not control all elements of the network. More importantly, the Chinese state does not seek such absolute power, opting instead for lighter-touch regulation in areas of technological innovation and commercial development in order to maintain economic growth. Jia argues that internet governance in China is more dynamic and less monolithic than is typically portrayed. The Chinese government, Jia explains, is deliberately inactive in some areas, knowingly enabling internet companies to exploit regulatory grey areas. In particular, the Chinese government allows domestic internet companies to take advantage of a particular corporate governance structure – becoming "variable interest entities" – in order to circumvent restrictions on foreign ownership and enable the companies to acquire foreign capital that is essential for their growth and overseas expansion. Simply put, the Chinese government officially allows internet companies to circumvent its rules on foreign ownership in order to facilitate long-term economic goals.

Luo and Lv draw similar conclusions, arguing that the Chinese government pursues "fragmented authoritarianism" in internet governance. China's coercive interventions principally focus on issues perceived to be vital to the stability of the regime, such as pro-democracy protests in Hong Kong or criticism of the Chinese government's response to Covid-19. In contrast, non-sensitive issues (such as the example of online health information cited by Luo and Lv) are subject to fragmented oversight, often among competing governmental agencies. So the Chinese government follows the dual purpose of ensuring political stability while promoting technological innovation and economic growth.

An important part of China's balancing act to serve economic growth is that it needs access to global capital markets in order to maintain and expand its internet sector. The dependence on foreign markets and foreign capital also opens these companies to external influence, particularly from US regulators. China's efforts to strengthen its own domestic capital market, as detailed by Jia, is an attempt to address this limitation.

Russia's embeddedness within the structures of global capital place it in a similar situation. The government faces steep hurdles in getting foreign internet firms to comply with its laws on content filtering and data localisation, in part because the country relies upon the services of foreign firms. Google, for example, at first failed to comply with the Russian law requiring the removal of specific search results and was fined for non-compliance in 2018. Only Russian search engines such as Yandex, Sputnik, Mail.ru and Rambler comply with the laws. Stadnik also notes that the Russian regulator, Roskomnadzor, has limited ability to compel foreign internet firms to comply with its content filtering or data localisation laws, except by "issuing fines and threatening exclusion from Russian territory". Taken altogether, these chapters highlight the extent to which a full understanding of internet governance requires close attention to the global capitalist system within which it is embedded.

Multistakeholderism: sidelining the state and civil society?

The themes noted so far – increased state assertiveness, state-market interplay, and constraints on state power – all play out in the multistakeholder venues that figure especially prominently in governance of internet infrastructure. As Santaniello notes, multistakeholderism holds out the promise of inclusiveness, also including the state. Governments are typically considered stakeholders that define and protect the public interest through legitimate representation of the general population (in respect of democracies, at least), arbitrating among competing societal objectives. However, Cavalli and Scholte underline that states have struggled with little success to increase their place in multistakeholder internet governance, as seen in both the Internet Assigned Numbers Authority (IANA) transition and arguments around ".amazon". Meanwhile, Reia and Fergus Cruz show that, in the case of smart city policies in Brazil, the federal government can sideline state and municipal levels of government in multistakeholder discussions.

A common finding across the chapters is that corporate actors play a weighty and arguably disproportionate role in multistakeholder governance of the internet,

whether in collaboration with or challenging state actors (see also Carr 2016). While multistakeholderism has a normative bias towards inclusivity, this volume adds to a growing body of research that concludes that "multiple" stakeholders are not equal stakeholders. In their chapter on the IANA transition, Cavalli and Scholte contend that the multistakeholder process effectively reduced the role of governments. While the IANA transition talks often discussed a feared state dominance, the problem of industry dominance was relatively neglected.

That said, not all corporate actors play equal roles. Cavalli and Scholte indicate that while large internet companies from the Global North tended to be highly active and influential participants in the IANA transition deliberations, small- and medium-sized enterprises – and companies of all sizes from the Global South – generally had less influence. Similarly, Rone points to the prominent role played by US-based social media platforms, particularly Facebook and Twitter, in the EU campaign against disinformation.

Along with sidelining the state, several of our chapters have suggested risks that multistakeholder processes can marginalise civil society in internet governance (Carr 2016; Hintz and Milan 2009). As might be expected, our studies of China and Russia confirm little role for civil society in internet governance in those countries. In addition, however, Reia and Fergus Cruz show that civil society can be squeezed out of policymaking in Brazil around smart cities. This near-absence of civil society groups is striking, given their previously prominent role in creating Brazil's groundbreaking internet bill of rights in 2014, the *Marco Civil da Internet*, as well as in making Brazil a world leader in free software(Hoskins 2018; Souza, Steibel and Lemos 2017). In addition, Rone's chapter shows that civil society representation has been sidelined in EU policymaking on disinformation.

The structural power of the United States

This book has intentionally privileged voices from outside the US-dominated mainstream of internet governance to see how this policy field looks from a decentred perspective. Nevertheless, the role of the US government has been an omnipresent background consideration. In particular, our chapters on China, Latin America, Russia and Europe have often examined the role of US official and commercial actors in setting the agenda, shaping the discourse and influencing particular policy measures. From the earliest days of the internet, the US has embedded standards that advance its economic, political and national security interests: for example, in relation to the commodification and free flow of data as well as the protection of intellectual property rights (Powers and Jablonski 2015; Carr 2016; Haggart 2019; Ciuriak and Ptaskina this volume; Chenou this volume).

Chapters in this volume often highlight the extent to which the United States continues to exert structural power in internet governance as well as digital economic policies more broadly. Following Susan Strange, structural power refers here to the capacity to "shape and determine the structures of the global political economy" (1994, 24–25). Chenou and ten Oever address this situation most directly with their attention to US influence on digital capitalism and multistakeholder

institutions, respectively. Both moves serve US interests to have an uninhibited global flow of data and knowledge (Powers and Jablonski 2015). Likewise, US structural power defines the global financial system that bankrolls digital capitalism. As noted earlier, even China-based firms depend in part on access to US financial markets for their continued growth domestically and internationally (Fuchs 2016; Jia and Winseck 2018).

US structural power is also evident when many of our chapters find that US-based companies continue to play a dominant role in supplying operating systems, applications, search engines and e-commerce. For example, Rone concludes that US-based corporations endeavoured to influence and even manipulate EU efforts to regulate online disinformation. In Russia, Stadnik finds that US-based companies at best only partially comply with national laws on data localisation and content regulation. The market dominance of US internet actors in most countries (notably excluding China) means that it can be challenging for any state regulator to compel these firms to comply with local legislation. Often the US firms invoke an ideological commitment to "free speech" to justify their defiance. Thus, any consideration of the role of the state in current internet governance is not incomplete without particular attention to the US government, most particularly with respect to the privatised areas of regulation.

While US structural power in internet governance is often underappreciated, it is also important to highlight that hegemony in internet governance is not static, nor does a single country exert hegemony over the entire internet ecosystem. As Winseck (2019) argues, while the US may dominate the internet's platforms,

> ownership and control of core elements of the global internet infrastructure such as the fibre optic submarine cables, autonomous systems numbers (ASNs) and the Internet Exchange Points (IXPs) that constitute the guts of the internet, is steadily tilting towards the rest of the world, especially Europe and Brazil Russia, India, China, and South Africa (BRICS).
>
> (Winseck 2019, 94)

Similarly, Scholte has found that the early days of US supremacy have largely given way to a "complex hegemony" in which the US role as a legitimising state is conditioned on the interplay of other forces and actors, including an important role for the "multistakeholder community" of academic, business, civil society, government and technical elites (Scholte 2020).

Towards future research

We noted in the book's introduction that our volume was far from the first on the role of the state in internet governance. Nor have we aspired to have the last word on the subject. Instead, the studies in our chapters invite further investigations, inter alia, into the five broad themes highlighted in this conclusion. How far can efforts to expand state involvement in internet governance go? How

do state-market interconnections play out, including in settings beyond those explored here? Do the technology and economics of the digital society present inherent limits to state sovereignty in internet governance, or can governments devise new ways to assert their primacy? What kinds of adjustments to multistakeholderism might better accommodate states and the public interest concerns that they can bring to the table? Or is enhancement of state-centred multilateralism still the better way to secure these ends? How deeply embedded is US power in internet governance; or is "hegemony" shifting to another state, or group of states, or indeed to non-state actors (Scholte 2020)? For example, as noted earlier, ownership and control of critical internet infrastructure are already diversifying to other regions (Winseck 2019, 94).

A particular contribution of this volume that invites further development is a more nuanced account of authoritarian states in internet governance. Our chapters have suggested three general conclusions: (a) that authoritarian governments, like other states, lack full control over the internet; (b) that the internet policies of authoritarian states are not all the same; and (c) that authoritarian and democratic governments hold similar as well as different positions in the internet realm. These points want further exploration in relation to China and Russia, as well as other authoritarian states not covered in our volume, including in Africa, the Middle East, and much of Asia (see, e.g., Freyburg and Garbe 2018).

Finally, we remain with a core more normative question of competing priorities. What does and should internet governance try to accomplish? When the aim is interconnectivity and interoperability, then private regulation through technically and commercially oriented actors might broadly suffice. Yet as soon as one broadens the policy agenda – to consumer protection, economic development, human rights, intellectual property, security and more – important public interest issues arise and the (democratic) state arguably has vital contributions to make. A carefully crafted return of the state in internet governance can be most welcome.

References

Black, Julia. 2008. "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes." *Regulation & Governance* 2 (2): 137–164. https://doi.org/10.1111/j.1748-5991.2008.00034.x.

Büthe, Tim. 2010. "Private Regulation in the Global Economy: A (P)Review." *Business and Politics* 12 (3): 1–38. https://doi.org/10.2202/1469-3569.1328.

Carr, Madeline. 2016. *US Power and the Internet in International Relations: The Irony of the Information Age*. New York: Palgrave Macmillan.

Cutler, A. Claire, Virginia Haufler, and Tony Porter, eds. 1999. *Private Authority and International Affairs*. Albany: SUNY Press.

Freyburg, Tina, and Tina Garbe. 2018. "Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa." *International Journal of Communication* 12: 3896–3916.

Fuchs, Christian. 2016. "Baidu, Weibo and Renren: The Global Political Economy of Social Media in China." *Asian Journal of Communication* 26 (1): 14–41. https://doi.org/10.1080/01292986.2015.1041537.

Glasius, Marlies, and Marcus Michaelsen. 2018. "Illiberal and Authoritarian Practices in the Digital Sphere." *International Journal of Communication* 12: 3795–3813.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State*. New York: Metropolitan Books.

Haggart, Blayne. 2019. "Taking Knowledge Seriously: Toward an International Political Economy Theory of Knowledge Governance." In *Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 25–52. New York: Palgrave Macmillan.

Hintz, Arne, and Stefania Milan. 2009. "At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy." *International Journal of Media & Cultural Politics* 5 (1–2): 23–38. https://doi.org/10.1386/macp.5.1-2.23_1.

Hoskins, Guy T. 2018. "Draft Once; Deploy Everywhere? Contextualizing Digital Law and Brazil's Marco Civil Da Internet." *Television & New Media* 19 (5): 431–447. https://doi.org/10.1177/1527476417738568.

Human Rights Council. 2018. "Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar." *Agenda Item* 4. United Nations. www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf.

Jia, Lianrui, and Dwayne Winseck. 2018. "The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization." *International Communication Gazette* 80 (1): 30–59. https://doi.org/10.1177/1748048517742783.

Jiang, Min, and King-Wa Fu. 2018. "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?" *Policy & Internet* 10 (4): 372–392. https://doi.org/10.1002/poi3.187.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1 (2): 205395171454186. https://doi.org/10.1177/2053951714541861.

Plantin, Jean-Christophe, and Gabriele de Seta. 2019. "WeChat as Infrastructure: The Techno-Nationalist Shaping of Chinese Digital Platforms." *Chinese Journal of Communication*, February, 1–17. https://doi.org/10.1080/17544750.2019.1572633.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: University of Illinois Press.

Schmidt, Nico, and Daphné Dupont-Nivet. 2019. "Facebook and Google Pressured EU Experts to Soften Fake News Regulations, Say Insiders." *OpenDemocracy (blog)*. 21 May. www.opendemocracy.net/en/facebook-and-google-pressured-eu-experts-soften-fake-news-regulations-say-insiders/.

Scholte, Jan Aart. 2020. "Rethinking Hegemony as Complexity." In *Hegemony and World Order: Reimagining Power in Global Politics*, edited by Piotr Dutkiewicz, Tom Casier, and Jan Aart Scholte, 78–97. Abingdon: Routledge.

Shen, Hong. 2016. "China and Global Internet Governance: Toward an Alternative Analytical Framework." *Chinese Journal of Communication* 9 (3): 304–324. https://doi.org/10.1080/17544750.2016.1206028.

Souza, Carlos Affonso, Fabro Steibel, and Ronaldo Lemos. 2017. "Notes on the Creation and Impacts of Brazil's Internet Bill of Rights." *The Theory and Practice of Legislation* 5 (1): 73–94. https://doi.org/10.1080/20508840.2016.1264677.

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

Winseck, Dwayne. 2019. "Internet Infrastructure and the Persistent Myth of U.S. Hegemony." In *Taking Knowledge Seriously: Toward an International Political Economy Theory of Knowledge Governance*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov. New York: Palgrave Macmillan.

Index

Page numbers in **bold** refer to tables; page numbers in *italics* refer to figures.