INTERNATIONAL
POLITICAL ECONOMY SERIES
SERIES EDITOR: TIMOTHY M. SHAW

Information, Technology and Control in a Changing World

Understanding Power Structures in the 21st Century

Edited by Blayne Haggart · Kathryn Henne · Natasha Tusikov

palgrave
macmillan

International Political Economy Series

Series Editor
Timothy M. Shaw
Visiting Professor
University of Massachusetts Boston
Boston, MA, USA

Emeritus Professor
University of London, London, UK

The global political economy is in flux as a series of cumulative crises impacts its organization and governance. The IPE series has tracked its development in both analysis and structure over the last three decades. It has always had a concentration on the global South. Now the South increasingly challenges the North as the centre of development, also reflected in a growing number of submissions and publications on indebted Eurozone economies in Southern Europe. An indispensable resource for scholars and researchers, the series examines a variety of capitalisms and connections by focusing on emerging economies, companies and sectors, debates and policies. It informs diverse policy communities as the established trans-Atlantic North declines and 'the rest', especially the BRICS, rise.

More information about this series at
http://www.palgrave.com/gp/series/13996

Blayne Haggart • Kathryn Henne
Natasha Tusikov
Editors

Information, Technology and Control in a Changing World

Understanding Power Structures in the 21st Century

palgrave
macmillan

Editors
Blayne Haggart
Brock University
St. Catharines, ON, Canada

Kathryn Henne
University of Waterloo
Waterloo, ON, Canada

Natasha Tusikov
York University
Toronto, ON, Canada

ISSN 2662-2483 ISSN 2662-2491 (electronic)
International Political Economy Series
ISBN 978-3-030-14539-2 ISBN 978-3-030-14540-8 (eBook)
https://doi.org/10.1007/978-3-030-14540-8

Library of Congress Control Number: 2019934563

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgements: Let's Put on a Show!

Staging an academic workshop like the one upon which this edited volume is based is a lot like putting on a show. There's an initial inspiration: *Hey, wouldn't it be great if we brought together a bunch of super-talented people to talk about Susan Strange and knowledge governance?* Then you assemble your dream line-up, a mix of eminent scholars, mid-career faculty, and early-career researchers, followed by the thrill of people you've admired for years agreeing to take part in your long-dreamed-of event.

There's also, of course, the mind-deadening minutiae of processing expense forms and arranging hotel rooms, the anxiety over the usual last-minute drop-outs (*c'est la vie; no drama*) and any number of unforeseen crises, inevitable disagreements amongst the organisers, and annoying micro-managing to ensure everyone sticks to their allotted presentation times.

But these downers are more than offset by the sheer enjoyment that comes from watching and listening to immensely talented people do their thing, and from the serendipitous creative and intellectual connections that can only emerge in a live setting. Especially when you've selected your line-up well and avoided any self-important divas.

All this is to say that we could not have been happier that the people behind the words you will find in this volume agreed to participate in this project. It was a great privilege (and so much fun) to have so many expert voices discuss knowledge governance from so many angles over the workshop's two days. We are very thankful that they thought it would be a productive use of their time to write and present papers on Susan Strange and knowledge governance (said papers all being completed on time!), and then to revise their papers multiple times over several months in

response to persistent emails from us for *just one more round of revisions.* (Sorry about that: Next time you're in town, the first drink is on us.) We are also appreciative of our four discussants, who show up in these pages to offer their thoughts on how these chapters fit into the big picture, for so gamely diving into the subject material, even (for one of them) at an unavoidable 10,000-kilometre distance. Thanks to them, and also to Michael Jablonski and Mark Schwartz, who both enriched the workshops with their comments.

Of course, these events don't happen without a lot of logistical support. Our trio of PhD student transcribers—Jenna Harb, Jenniffer Olenewa, and Krystle Shore—provided exhaustive notes on the two-day workshop, which helped us all improve our initial papers. Thanks also are due to the Balsillie School of International Affairs in Waterloo, Canada, which hosted our two-day workshop, supported this book, and enabled us to provide brain-sustaining lunches and break food. As anyone who has ever been to a conference knows, the most stimulating discussions usually happen outside of working hours. To that end, we also want to thank the Solé Restaurant and Wine Bar and King Street Trio Uptown for hosting our working dinners. And a special thanks to Kent Weyand for the tasty mixed drinks he served us over the course of the two days (after hours, of course), and for letting Natasha and Blayne crash on their exceptionally comfortable basement sofa bed. Let's do a *GTA V/Red Dead Redemption 2* marathon in the near future.

Neither do such events come for free. In our case, funding was supplied by a grant from the Social Sciences and Humanities Research Council of Canada Insight Development Grant and the Canada Research Chair in Biogovernance, Law and Society. Blayne's share of the final editing on this project was completed while serving as a research fellow at the Käte Hamburger Kolleg/Centre for Global Cooperation Research at the University of Duisburg-Essen in Germany. He thanks the Centre for providing the time and space to complete this work.

Our plan was always to have a record of the workshop so that it could live on through more than just happy memories and word of mouth. The enthusiastic expressions of support as we were putting the workshop together from series editor Timothy Shaw and Palgrave Macmillan's Christina Brien were heartening affirmations in the value of what we were (are) doing. Thanks also to Clara Heathcock, Katelyn Zingg, and Ekambaram Ganesh at Palgrave Macmillan for their support.

In an important way, this workshop had its genesis in our time together at the Regulatory Institutions Network (RegNet), now the School of Regulation and Global Governance, at the Australian National University, Natasha as a doctoral candidate, Kathryn as a postdoctoral fellow, and Blayne as a visiting researcher. Peter Drahos, John Braithwaite, and Valerie Braithwaite, three of RegNet's founders (Peter also being Natasha's supervisor), and Susan Sell, a current member of RegNet, are all significant influences on our thinking. Beyond their specific academic influence is RegNet itself. RegNet's core principles involve an emphasis on the importance of regulation in all its forms, a concern about unjust expressions of power and domination, and a belief in the value of cross-disciplinary engagement. The workshop, this edited volume, and our general approach to scholarship represent our continued, if necessarily imperfect, attempts to practise a RegNet approach to academic citizenship. We therefore would like to dedicate this book to Peter, John, Val, and Susan, and RegNet.

Duisburg, Germany — Blayne Haggart
Waterloo, Canada — Kathryn Henne
Toronto, Canada — Natasha Tusikov

Contents

Notes on Contributors

Sara Bannerman Canada Research Chair in Communication Policy and Governance, is Associate Professor of Communication Studies at McMaster University in Canada. She researches and teaches on communication policy and governance, and directs McMaster's Communications Governance Observatory. She has published two books on international copyright—*International Copyright and Access to Knowledge* (2016) and *The Struggle for Canadian Copyright: Imperialism to Internationalism, 1842–1971* (2013)—as well as numerous peer-reviewed articles and book chapters on international copyright, privacy, and other topics in new media, traditional media, and communications theory. Bannerman is a Vice Chair of the Law Section of the International Association for Media and Communication Research.

Madeline Carr is Associate Professor of International Relations and Cyber Security at University College London. She is also the co-investigator of the Standards, Policy and Governance stream of the PETRAS research hub on the cybersecurity of the Internet of Things (IoT). Carr is the principal investigator on a project looking at international cooperation on the IoT cybersecurity of critical infrastructure and on the project ECSEPA (Evaluating Cyber Security Evidence for Policy Advice), which explores how UK cybersecurity policymakers evaluate evidence in short-term incident response and long-term planning scenarios.

Allison Fish is a Senior Lecturer in the TC Beirne School of Law at the University of Queensland where she directs the Law, Science, and Technology Program. Her research lies at the intersections of law,

socio-cultural anthropology, and science and technology studies. The three questions that have directed much of her recent work are as follows: what are the legal forms, technological infrastructures, and cultural logics that shape information/knowledge management practices? How do law and technology function together to mediate access to valuable knowledge? And how is accessibility increasingly framed as a fundamental human right and critical pathway to social enfranchisement? To date, the bulk of her work has addressed the application of intellectual property law to the regulation of various domains. Recently, however, she has initiated other projects examining other aspects of the law-and-technoscience interface.

Randall Germain is Professor of Political Science at Carleton University, Canada. His teaching and research focus on the political economy of global finance; issues and themes associated with economic and financial governance; and theoretical debates within the field of international political economy (IPE). His work has been published in journals such as *Review of International Political Economy*, *Review of International Studies*, *Global Governance*, and *European Journal of International Relations*. He is the author of *The International Organization of Credit* (1997) and *Global Politics and Financial Governance* (Palgrave Macmillan, 2010). He is working on a manuscript that explores the use of the idea of history in IPE.

Blayne Haggart is Associate Professor of Political Science at Brock University in St. Catharines, Ontario, Canada. His book, *Copyfight: The Global Politics of Digital Copyright Reform*, was published by University of Toronto Press in 2014. Prior to his academic career, he was a professional economist, working for several Canadian parliamentary committees, as well as a journalist. His research focuses on the implications of changing intellectual property rules and the rising importance of knowledge governance in the global economy.

Debora Halbert is a Professor of Political Science at the University of Hawai'i at Mānoa and the Associate Vice President for Academic Planning and Policy for the University of Hawai'i System. She has published three books on issues of intellectual property, *Intellectual Property in the Information Age: The Politics of Expanding Rights* (1999), *Resisting Intellectual Property* (2005), and *The State of Copyright* (2014), and co-edited the *Sage Handbook on Intellectual Property* (2015) with Professor Matthew David.

Jenna Harb is a PhD candidate in the Department of Sociology and Legal Studies at the University of Waterloo. She studies surveillance and

security, with emphases on intersections between technology, policy, regulation, and social inequality. Her research examines local and global influences underpinning the use of biometric technologies as a key apparatus of governing marginalised populations, particularly as it relates to the transnational management and control of refugees.

Kathryn Henne is the Canada Research Chair in Biogovernance, Law and Society at the University of Waterloo, Canada, where she is a fellow of Balsillie School of International Affairs and Assistant Professor of Sociology and Legal Studies. She is also Associate Professor at RegNet, the School of Regulation and Global Governance at Australian National University. Her research is concerned with how biogovernance—that is, the governance of populations and individual humans through science and technology—informs everyday life. It spans topics related to biometric surveillance and policing, regulatory science, sport and physical culture, and drug regulation.

Jennifer Musto is Assistant Professor of Women's and Gender Studies at Wellesley College. Her research focuses on the ways in which laws, technologies, and collaborative modes of governance are leveraged to address exploitation, intimacy, violence, and vulnerability, broadly defined. Her current research examines the role that third-party actors play in mitigating tech-facilitated harm and how data in general and data-driven interventions in particular are being leveraged to respond to it. She is the author of *Control and Protect: Collaboration, Carceral Protection, and Domestic Sex Trafficking in the United States* (University of California Press, 2016).

Angela Orasch is a PhD candidate in the Political Science programme at McMaster University. She has published work in the field of Canadian social policy and Canadian intergovernmental relations. Her research is situated within the field of urban/municipal policy and governance, examining the political economy of smart cities in North America. She is also a member of Evergreen's mid-sized cities research collaborative, where her research examines governance models of Canadian smart city initiatives.

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 Australian National University. 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 2016. Prior to her work in academia, she was a strategic criminal intelligence analyst with the Royal Canadian Mounted Police in Ottawa, Canada.

Dwayne Winseck is Professor at the School of Journalism and Communication, with a cross-appointment at the Institute of Political Economy, Carleton University. His main research interests include the political economy of telecommunications, the internet, and media as well as communication history and theory. He is also director of the Canadian Media Concentration Research Project (cmcrp.org) and has been the lead Canadian researcher in the International Media Concentration Research Project since 2009.

List of Figures

Introduction

Blayne Haggart, Kathryn Henne, and Natasha Tusikov

The control of knowledge is fast becoming the dominant means by which economic, political, and social control is exerted globally. We can observe these dynamics in countless and seemingly unconnected corners of society, ranging from the increasing dependence on intellectual property rights and other intangible forms of property to capture economic value to the ever-more invasive cataloguing of citizens and migrants alike by the state at the border. The embrace of digitisation, the expansion of ubiquitous commercial and state surveillance, and the interpenetration of online and "offline" activity are reshaping our societies and our everyday lives.

B. Haggart (✉)
Brock University, St. Catharines, ON, Canada
e-mail: bhaggart@brocku.ca

K. Henne
University of Waterloo and Balsillie School of International Affairs, Waterloo, ON, Canada

Australian National University, Canberra, ACT, Australia
e-mail: khenne@uwaterloo.ca

N. Tusikov
York University, Toronto, ON, Canada
e-mail: ntusikov@yorku.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_1

Scholars from various disciplines have recognised the significance of these changes. Interdisciplinary fields, such as Socio-Legal Studies, Science and Technology Studies (STS), Surveillance Studies, and Communication Studies, focus on discrete areas related to knowledge or specific issues, such as intellectual property, privacy rights, internet governance, or data governance. Unfortunately, International Political Economy (IPE) lags far behind these more specialised fields, still largely content to focus on production, trade, and finance as its primary concerns (Haggart 2017a). While much excellent work has emerged from the division of labour by discipline, much of it suffers from the same problem that afflicts modern academic knowledge production in general: the siloing of research and the stifling of dialogue across disciplinary borders. Even though phenomena such as the increasing economic reliance on intellectual property, ubiquitous surveillance, the preoccupation with data collection, the rise of online platforms, and the obsession with technological innovation describe different aspects of the same phenomenon—that is, the move of the control of knowledge to the centre of social life—they are almost always treated and studied discretely.

This edited volume makes the case that it is essential to study these phenomena as related and connected forms of knowledge governance. It came about because the three of us realised that although we are based in different disciplines—Haggart in IPE, Henne in Socio-Legal Studies and STS, and Tusikov in Criminology and Regulatory Theory—our specific research areas overlap significantly. This overlap was not so much in terms of our actual subjects: Henne has an abiding interest in the biometric tracking and regulation of bodies, Tusikov's work focuses on non-state internet governance, and Haggart focuses on copyright governance. Rather, we noticed that our three research agendas all shared a concern with technology-enabled surveillance, and the commodification of different aspects of the world for the purposes of exerting economic, political, and social control. Most significantly, it was abundantly clear that the rules governing all three areas were the result (and source) of great power. These rules create winners and losers, advancing certain values, norms, and policies at the expense of others. In short, we were all studying the control of knowledge as determinant of societal power and influence.

In order to test our assumption that these disparate issue areas can be productively linked, we convened a workshop in May 2018 at the Balsillie School of International Affairs in Waterloo, Ontario. The two-day work-

shop brought together leading and emerging scholars from across the social sciences with the goal of seeing whether a common dialogue and understanding would be possible. The chapters and reflections in this volume are the result of that workshop. Our authors and discussants represented the fields of Communication Studies, IPE, International Relations (IR), Criminology, Law, Political Science, Anthropology, STS, Socio-Legal Studies, and Women's and Gender Studies, a diverse group with positivist, interpretivist, and poststructuralist commitments.

In this introductory chapter, we set out the purposes of the workshop and this volume. We also outline our overall shared theoretical framework, which draws on the understudied (at least from a knowledge-governance perspective) work of the late IPE scholar Susan Strange. We then offer a critical analysis of her theory as it relates to knowledge governance, and conclude with an overview of the chapters in this volume.

1 Creating a Common Dialogue

For this project, we were interested in a few basic questions: what is the nature of a knowledge-based (or digital- or information-based) society? What are its effects? What sustains it? How just is this new form of society, and how can be it be made more just?

One of the biggest challenges to fostering truly multidisciplinary dialogue is agreeing on theoretical "ground rules." Every discipline has its own peculiarities, emphases, and jargon, as well as different conceptions about the purpose of social-scientific inquiry, namely whether research should primarily be to understand or to change society. In our case, the contributors to our volume did share two pre-existing general points of agreement:

First, a common understanding of knowledge as being socially constructed. In this volume, we do not share a single, fully realised, specific definition of what, exactly knowledge is. In fact, we argue that such a definition is likely a fool's errand. Our two lead-off chapters, by Haggart, and Bannerman and Orasch, employ somewhat different definitions of knowledge. Taken together, they suggest that different approaches to knowledge yield different insights, without one view being more absolutely correct than the other. While we might disagree, for example, about exactly what type of knowledge *technology* is, we all shared an understanding that *knowledge* represents a socially constructed interpretation of reality, and is distinct from the concept of information. Elsewhere, Haggart

(2017b), drawing on Berger and Luckmann (1966) and the sociology of knowledge, argues that if *information* is phenomena that exist regardless of human observation of it, knowledge is the necessarily partial, biased, and always-incomplete interpretation of information. Knowledge thus captures everything from data itself to intellectual property to privacy and surveillance regulations, all topics that are discussed throughout this volume. Categories like "data" and "intellectual property" may themselves resist easy definition, but acknowledging that they are socially constructed—as Gitelman (2013) remarks, "raw data is an oxymoron"—and thus have a certain flexibility to them allows us to engage in a productive debate over the consequences of defining these forms of knowledge in a particular way. This is why we as editors have not required that our contributors agree on all nuances of these and related definitions: our goal is to spur discussion, not to artificially close off debate. After all, if all knowledge is necessarily partial, so too will any single definition fail to fully describe the underlying "reality" to which it is applied.

Second, an emphasis on the importance of regulation in creating and framing knowledge, and in governing its social effects. As Haggart lays out in this volume, regulation governs the way that knowledge is legitimised, created, disseminated, and used. The study of regulation is therefore a gateway to understanding power dynamics in society, as well as how rules (both formal and informal) create and sustain power imbalances, creating (and perpetuating) winners and losers.

This focus on regulation also partly accounts for the fact that most of this volume's chapters share a strong emphasis on empirical research. While this volume might be focused on the big picture—understanding the nature of the knowledge society—the chapters are all interested in how these macro-level societal changes are working themselves out on the ground, on how they affect actual individuals and groups. More specifically, while the contributors may differ somewhat on whether all research should be designed to emancipate groups, all are concerned with issues of social justice, and are conscious of the existence of injustices and how they can be propagated by social norms and regulations. Halbert, for example, grapples with whether a more permissive copyright regime of the type that she would otherwise tend to favour is actually promoting hate speech that she (it should go without saying) finds abhorrent. Henne, meanwhile, provides us with a consideration of how India's unique-identity verification system, Aadhaar, has affected the most vulnerable members of Indian society.

As we note below, we still ran into misunderstandings and theoretical disagreements, particularly with respect to terminology and over the primary end purpose of theory. In the end, we felt these disagreements were generative: participants' open commitment to dialogue and to understanding these differences helped to clarify, not impede, our discussions. They were "productive problems," to use a phrase that was repeated several times during the workshop.

2 Enter the Strange

Theory, consciously or unconsciously, precedes analysis. Therefore, even with these shared commitments, we agreed on the need for a shared theoretical framework that would be flexible enough to incorporate potentially conflicting ontologies and epistemologies, one that would allow us to talk with, not past, each other, and to give us a common reference point, even it sparked disagreements.

Susan Strange's name is not found in the pantheon of those theorists who have been brought to bear on our understanding of knowledge governance—Foucault, Veblen, Haraway, Berger and Luckmann, and so on. A giant in IPE, she founded the British School of IPE thought, coming to academia in her 40s following a 20-year journalism career including with the *London Observer* newspaper. Strange, who passed away in 1998 at the age of 75, was an idiosyncratic thinker who strongly favoured empirical research, building her understanding of the world from the ground up. For her, IPE was defined by its subject matter, the politics and economics of the international order, and it invited a multitude of different theoretical approaches.[1] She was highly critical of American IPE and IR scholarship generally, seeing it primarily as a handmaiden to the U.S. state.

Despite her stature in IPE, Strange is virtually unknown outside of IPE and IR. Although (as we shall see) she placed the control of knowledge at the very heart of her theoretical framework, this lack of awareness holds true for those disciplines that study knowledge-related issues of the type covered in this volume: This lack of attention does make some sense, since her primary empirical contribution was to the study of global finance, not knowledge. With some exceptions (e.g., Mytelka 2000), those scholars

[1] That said, as Langley (2009) notes, her materialist commitments have led to a bias against poststructuralist theory in the British IPE School.

who have picked up Strange's mantle have also tended to focus on international financial governance (e.g., Germain 2010).

Her relative lack of profile outside of IPE represents something of a missed opportunity for knowledge-governance scholars. As we develop through this volume, she offers us a very compelling, if imperfect, way of synthesising and understanding not only disparate parts of the knowledge society, but of showing how knowledge-regulation connects to and affects the wider society.

Strange does not offer a grand theory to explain social relations. Unlike Marx, for example, she offers a minimalist theory of the global political economy derived from some basic first principles. This theory tells us what is in the world and how these elements are related. Because its claims are very broad and general, her approach can accommodate vastly different theoretical perspectives. This framework may frustrate those seeking a theory of everything, but it is perfect for those of us who eschew such theorising and want to talk across theoretical boundaries.

2.1 Key Concepts

Like all productive theories, Strange's framework is useful because it focuses our attention on key aspects of the world around us, and allows us to generate productive questions. Here, we highlight four in particular:

2.1.1 Structural Power

In her 1987 (2nd edition 1994) book *States and Markets*, Strange argues that societies of any size must provide the following: physical security, a sense of justice, material wealth, and individual freedom. Societies differ in how they order the relative importance of each of these, and how they are delivered.

These aspects are delivered through the creation of rules and norms that comprise social orders. This is done through the exercise of power. For Strange, the key form of power was not relational power, defined as the ability to compel someone to do something they would not otherwise do. Rather, she argued we should focus more on what she called structural power. Strange defines structural power as:

> the power to shape and determine the structures of the global political economy within which other states, their political institutions, their economic

> enterprises and (not least) their scientists and other professional people have to operate. This structural power … means rather more than the power to set the agenda of discussion or to design … the international regimes of rules and customs that are supposed to govern international economic relations. … Structural power, in short, confers the power to decide how things shall be done, the power to shape frameworks within which states relate to each other, relate to people, or relate to corporate enterprises. The relative power of each party in a relationship is more, or less, if one party is also determining the surrounding structure of the relationship. (Strange 1994, 24–25)

In short, Strange advocates focusing on the underlying game and the norms that structure interactions. Such an approach has an obvious utility to students of regulation and norm construction.

2.1.2 Four Key Structures; The Knowledge Structure

If Strange's conception of structural power has an innate appeal for those interested in studying how societies are structured and change, it is her observation of the key areas of power in the global political economy that should make anyone interested in anything related to knowledge governance pay attention. Different theorists have identified different ultimate sources of social power. For traditional realists in IR, it is the ability to provide security for one's society that is the ultimate precondition for the very existence of society. Marxists, famously, argue that in the end it is production that turns the motor of history. Poststructuralists, for their part, say that it is language that makes the world go round.

In contrast to these monocausal theories, Strange argues that power emanates from not one, but four, key sources:

- Security: the ability to provide or deny physical security;
- Production: the ability to determine what gets produced, by whom, and who can consume production;
- Finance: the ability to create money and to allow and deny access to credit; and
- Knowledge: the ability to determine what is considered to be legitimate knowledge, and to determine who can create, disseminate and use this knowledge.

Strange argues that none of these is necessarily a priori more important than the others. Instead, the question of which one is most important can only be answered by looking at history to determine which structure is

dominant at that moment. Historical context matters. Each source of structural power (which she refers to as "structures") is interrelated, meaning that what happens in one structure affects what happens in another. The dominance of a structure means that its logic will dominate the functioning of the other structures. For example, in an era dominated by production, as most of the twentieth century was, research and development was seen as an input into the production of new products. In the twenty-first century, with the knowledge structure dominant, technology itself is no longer just an input; it has become the product to be bought and sold (Breznitz 2007).

Of greatest importance to this volume is Strange's description of a knowledge structure. Her conception of structural power offers us a framework to understand the historical emergence of a knowledge-based society as being continuous with what had previously existed. It links the various forms of knowledge-regulation under a concept—the knowledge structure—in a way that allows us to overcome the artificial barriers created by academia. Focusing on the underlying rules and norms helps to render visible otherwise-hidden power dynamics. For example, the chapters by Tusikov and Winseck (complemented by Carr's reflections on their contributions) both examine what underlying structures—related to the Internet of Things (IoT) in Tusikov's case, and control over the internet's infrastructure in Winseck's—can tell us about the exercise of power in the internet age, rendering visible the "plumbing of power."[2] Strange, herself a materialist, would likely also have agreed with Carr's acknowledgement of the importance of the materiality of the internet to the exercise of power as elaborated by Tusikov and Winseck.

While her knowledge-structure framework poses some conceptual problems, discussed below and in the chapter by Haggart, it has the very distinct advantage of identifying where we should be focusing our attention: on the rules and norms governing the knowledge structure, and how changes in their relative importance compared with the other structures are affecting society, for better and worse.

2.1.3 State and Non-State Actors; Market and Authority

The power of private actors to set standards and enforce rules is one of the defining characteristics of the current digital world. The companies that dominate online activity—what Tusikov (2016) calls macro-intermediaries—often

[2] Thanks to Mark Schwartz for this turn of phrase.

have the global scope to structure the lives of billions of individuals via their privately set regulations. Examples range from a payments service like PayPal that, through its terms of service, can (and does) go beyond what is required by the law to decide who can and cannot use its services (Bridy 2015; Malcolm 2017), to online intermediaries from Google to GoDaddy engaging in "handshake agreements" to act as judge, jury, and executioner in the private enforcement of trademarks (Tusikov 2016).

Any understanding of the current global political-economic moment, therefore, must account for how private actors have state-like capabilities to regulate our lives. Despite the long history of private actors, especially companies, setting and enforcing rules online, often through self-regulatory efforts or in some form of cooperation with the state (e.g., Marsden 2011), it would be a mistake to write off the state as a dominant global player and form of governance. In fact, as many internet governance scholars have noted, the internet is highly amenable to regulation by both states and private actors (e.g., Wu and Goldsmith 2006; Zittrain 2006). At the end of the day, states are still seen as the primary legitimate authority for organising politics and society. It is also likely that tech companies' regulatory dominance is somewhat overstated. Tusikov (2016) reveals, for example, that supposedly voluntary agreements to enforce trademarks online between trademark rights holders and internet intermediaries like Google are actually actively crafted, very quietly, by states. State power is still important and must be accounted for in any analysis.

These political dynamics would be very familiar to Strange. For Strange, structural power is subject to political contestation and involves a contest between both state and non-state actors. She frames this contestation as a battle between what she calls market (non-state actors, often businesses) and authority (the state). At a given time, either one of these may be more or less important in determining the shape and content of structural power. In her formulation, the state is neither the handmaiden of capital nor the ultimate authority; rather, battles to dominate the various structures involve a contest between what she terms market and authority. In any given situation, structural power may lie with either or both types of actor, with political outcomes reflecting "where structural power lies in that relationship" (May 1996, 174).

This approach thus avoids the tendency, prevalent among American digital-rights activists, to treat concentrated private, corporate power as

less problematic than state power (Glaser 2018). In a Strangean framework, both state and non-state actors are taken seriously, with similar capabilities to structure our lives, for good or ill. Any analysis that downplays either state or non-state actors, or that fails to investigate their interplay, is necessarily incomplete.

2.1.4 Research Focus and Emphasis on Empirical Work

Strange's journalism training is nowhere more obvious than in the research question that motivated her academic work. Her guiding question, famously, was *cui bono?*, or Who benefits? Emphasising that political and regulatory decisions create winners and losers focuses the mind in a particular direction: on the rules, institutions, and mechanisms in, say, finance that drive outcomes; on the actors that set the rules in motion; and on the winners and losers from these policies.

Strange's research question also implies an empirical methodology. It necessarily requires that one get down into the weeds to understand how a particular part of the world actually works, and to analyse its eventual outcomes. Engaging in empirical research makes it difficult to abstract too far from the lived lives and politics of real people. In emphasising the importance of deep understandings through empirical research, it also provides a way for scholars from a multitude of disciplinary backgrounds to get together.

As the preceding reflection suggests, Strange's theoretical approach provides a flexible way for scholars to come together and engage in a dialogue based on a common approach. It has a simple and productive research question. It requires accepting only a few key points: that norms and rules are constitutive of society and worth focusing on; that there is a relationship between her identified structures[3]; that empirical research has value; that both state and non-state actors can be authoritative; and that the relationship between market and authority is historically contingent and must be investigated, not assumed.

[3] And even if one does not buy Strange's argument about these being *the* key structures/sources of structural power, or that none of these is necessarily a priori more important than the others, her formulation can still get us thinking about the relationships between these issue areas.

2.2 *Strange in Critical Focus*

For us and the other workshop participants, Susan Strange was a means to the end of facilitating cross-disciplinary dialogue. The workshop was explicitly designed not to be a workshop on Strange's approaches to knowledge governance but rather to be a workshop on knowledge governance that uses Strange to help us engage with the topic. Consequently, the direct Strangean footprint in some of the contributions is relatively light, confined to a focus on state and non-state interactions over knowledge-regulation, as in the chapter by Fish. That said, while the workshop participants all found Strange's theoretical framework a useful way to frame our discussions, we did not (and do not) apply her uncritically in this volume. Our discussions revealed several gaps in her approach. They are primarily related to her embrace of materialism over social construction, and the status quo, or stability, bias in her theory. We revisit these limitations throughout this volume, particularly in the reflections that end each section and in the conclusion.

2.2.1 *Underdeveloped Conception of the Knowledge Structure*

Of her four identified main sources of structural power, Christopher May (1996, 182) argues that the knowledge structure is both the "most suggestive (and problematic)." The other three structures are relatively well-developed. The production structure draws on Marxist analysis (May 1996, 178), while the security structure would be familiar to any realist IR scholar in terms of its relationship between the strong and the weak and the need to police borders against other states. The finance structure, meanwhile, was the subject of much of Strange's productive scholarly work (most notably Strange 1986, 1998).

There is a logic problem at the heart of her knowledge structure. The knowledge structure consists of two parts: the power to designate what is thought of as useful knowledge—in other words, what is considered to be "true" knowledge—and the power to determine what knowledge is produced, and how it is disseminated and used, and by whom. Moreover, Strange claims that the knowledge structure is interrelated and equivalent in importance to the other three structures. As May points out, however, the power to determine what constitutes legitimate knowledge would seem to also involve the power to determine whether we should value security, say, over prosperity. As a result, this power would necessarily have to stand above the other structures.

Strange does not make this move because her conception of power is strongly materialist. As a result, she never fully (or perhaps directly is a better word) engages with the notion of immaterial power and how this might construct material power. Instead, she leaves this problem unresolved. Strange's materialism also manifests itself in her failure to mark a difference between *information* and *knowledge*. For her, the two are effectively the same thing, with knowledge essentially being more-complex forms of information. That Strange does not buy into the notion of social construction explains the conflation of these two points and represents a key difference between our approach and hers.

As we discussed earlier, we take the position that knowledge is indeed socially constructed and that how it is constructed, and in whose favour, is a primary research question. That said, for reasons that we discuss below, we do not believe this is a fatal flaw in her theory. In his chapter, Haggart offers a possible way out by analytically separating these two parts of the knowledge structure, so that the study of what knowledge is legitimated, and by whom, is set aside to focus on the regulation of knowledge. This question of knowledge-legitimation is picked up by Harb and Henne's discussion on the power dynamics behind disinformation in the service of the state constructing the identities of marginalised groups. In his reflection, Haggart highlights the significance of the power to name marginalised groups as discussed by Harb and Henne, connecting it to Halbert's discussion of copyright as a censorship regime. In both cases, power expressed through the knowledge structure is used to legitimise a particular form of truth itself. Meanwhile, Bannerman and Orasch offer a finer-grained conceptualisation of the knowledge structure. Both of these chapters suggest that while Strange's knowledge structure is very provocative, there is a need for further discussions about the best ways to conceptualise it. In this light, the chapters by Haggart and by Bannerman and Orasch should be seen as the start of the conversation, not its conclusion.

2.2.2 Identity Construction and Definitions of Granularity

Another consequence of Strange's materialist commitments is that she ignores identity formation and how socially constructed dynamics, such as race or gender, influence the provision (or not) of security, finance, and production, or their relationship to the creation or legitimisation of knowledge. Not only is her work silent on these points, in her 1995 presidential address to the International Studies Association, she famously said of feminists—in comments that were deleted from the published

version of her address—that they should "stop the whining and just get on with it" (Whitworth 2006, 88) (reported elsewhere as telling the female members of the association to "…stop whining, have their babies sooner rather than later and get on with their careers" [Centre for the Study of Globalisation and Regionalisation 1998]) even as her own ascendance to the very heights of a male-dominated field, was the embodiment of what many would characterise as a feminist achievement (Sen 1998).

Our workshop discussions also uncovered other theoretical blind spots. While we and the workshop participants found her commitment to empirical research as a means of understanding the world to be one of her most appealing characteristics, it nonetheless emerged as a point of contention. The issue turns on the notion of "granularity." In IPE, granularity refers to the embrace of a fine level of detail about a subject: to understand the global financial system, study how exchange rates are determined, and by whom, for example. In other disciplines, such as feminist studies and anthropology, however, they favour the notion of knowledge being "situated." According to Donna Haraway, a prolific feminist scholar who is attentive to human and non-human relations and inequalities, situated knowledges rely on "partial, locatable accounts of the world," which "are both accurate and explicitly embedded within the contexts of its own production" (Haraway 1988, 575–599). In other words, we have to get close to the ground—as opposed to far away, which positivists tend to embrace—in order to generate robust knowledge. In this book, Harb and Henne, Fish, and Henne embrace a more situated approach by looking at individual persons, or actual bodies, and how they affect and/or are affected by their social locations. While Strange's research question, *cui bono?*, gives pride of place to the location of winners and losers in one's analysis, it does not necessarily translate into either a direct focus on people as the unit(s) of analysis, nor does it necessarily foreground issues of inequality, be it economic or social. Needless to say, the lack of specific attention to these issues is concerning to scholars interested in issues of subjectivity and representation against the backdrop of social difference. Here, Germain, an IPE scholar, and Musto, a Gender Studies scholar, use their reflections to work through these issues.

2.2.3 Status Quo Bias

"Theory," as Robert W. Cox reminds us, "is always for someone and for some purpose" (1981, 128). All theories contain inherent biases, and Strange's is no different. While her focus on winners and losers emerging

from the exercise of structural power reflects a concern with justice, her framework also exhibits a bias in favour of stability and the status quo. For example, her 1987 article on whether the United States should still be considered a dominant power—"The Persistent Myth of Lost Hegemony"—embraces the values of order and stability. Here, the main problem with the global financial system was not the fact of U.S. hegemony, but that the United States, the dominant global power, was acting irresponsibly, a consequence of its peculiar domestic politics. In her analysis, order and stability emerge as key values. While she elsewhere indicated that she was not wedded to the states system and hoped to see the emergence of a "global civil society" to challenge the hegemony of a transnational corporate class (Strange 1999), in this case she expressed the hope that the United States would exercise more far-sighted self-interest in its engagement with the world. She was not necessarily against hegemony; she was against unstable hegemony. The failure to provide good governance is what is problematic for Strange.

2.3 Productive Problems

And yet, we must also note that Strange has tended to be identified as a critical theorist. Her focus on how society's underlying structures are contested—indeed, her insistence that we cannot take them for granted—separates her from problem-solving theorists who take these underlying structures for granted. Highlighting how these rules and norms advantage or disadvantage particular groups, in fact, effectively grants the Critical Theory point that underlying rules and norms perpetuate advantages and disadvantages. Indeed, this is exactly what structural power is supposed to do. Her comfort with the exercise of hegemonic power may not sit well with many social activists, but as Germain notes in this volume, there is no reason why activists cannot use Strange's conceptions to pursue transformative change. In fact, if her understanding of structural power is correct, they would be wise to think long and hard on its implications for how they might achieve such change. If there is one point we can take away from Strange, it is that we cannot wish away the exercise of power in the world: rules will always be contested.

Turning to the role of ideas, identity, and social construction in Strange's theory, we can make a similar comment. One of the most interesting things about Strange is that, in acknowledging that the ability to determine what counts as legitimate knowledge is a key element of

structural power, she opens the door to engage with issues of social construction, of identity construction, and to distinguish between knowledge and information within her theory. Focusing on how the legitimation of knowledge occurs, and by whom, offers a front door through which we can consider the power dynamics involved in perpetuating ideas related to and categories of ideas such as gender and race. While Strange's materialist commitments meant that she was unable to follow her theory to its logical conclusion in this area (May 1996), there is no reason why we cannot.

Overall, Strange's theoretical framework as it relates to knowledge is underdeveloped (May 1996), a fact to which Haggart in this volume pays particular attention. Her conceptualisation of knowledge and information is highly unsatisfying and her stated categories of what comprises knowledge are not wholly convincing, but for all that, they do introduce the fundamental question of what is knowledge as a source of (immaterial) power into a discipline—IPE—that tends to shy away from such questions. Hers is a primarily materialist theory that explicitly includes social construction in her conceptualisation of the knowledge structure. It exhibits a strong bias towards stability and the status quo, but her primary research question, *cui bono?*, is an open invitation to social change for those who are not happy with how this question might be answered. Her (and IPE's) conceptualisation of granularity may not explicitly hold persons as the primary unit of analysis, but as Fish and Henne's chapters suggest, there is nothing in Strange that suggests that they cannot be.

One of the ways to judge a theory is by whether it produces useful research questions. From this perspective, Strange's approach has much to recommend, particularly as it relates to the study of knowledge governance from a multidisciplinary perspective. In fact, its messiness is one of her theory's most important advantages because it produces productive problems that spur further thought rather than close off areas of research. Setting material forces alongside the immaterial (however slight it might be in her original conceptualisation) allows us to use her theory as a playground: she identifies the two as important but leaves it up to the rest of us to have the discussion about their relative importance and how they might fit together. Similarly, asking who benefits from a particular configuration of structural power puts us on the road to solving an empirical question while leaving open whether the discovered state of affairs is desirable or not. It also leaves open the question of which "who's" from her research question that our own research should consider.

Beyond these contested points, her theorising about structural power and the balance between market and authority yields very fruitful pathways for future research. In the case of knowledge governance and its relationship with other facets of structural power, it renders visible the importance of knowledge governance, and invites us to consider how the rising dominance of the knowledge structure might affect our conceptualisations of security or how production is structured. It suggests that we should pay attention to both state and corporate power and their interaction. It places human agency front and centre: change does not happen because of some amorphous thing called "culture" or "the market": it happens because state and non-state actors—people—act purposefully to their own ends. Crucially, it emphasises the need to pay attention to how changing underlying rules and norms create winners and losers in society. Perhaps most importantly, if our workshop experience is anything to go by, it provides a framework to encourage discussion amongst people from disparate backgrounds. Given that our current understanding of what Strange calls the knowledge structure is currently the domain of many different disciplines, this is a very good thing.

3 Organisation of This Volume

As we have already stated, the purpose of this volume is to provide a fuller understanding of the knowledge structure as it is currently constituted, drawing on different interdisciplinary analyses and perspectives. However, we recognise that knowledge structures are historical constructs. Consequently, both the knowledge structure and our understanding of it change over time. One of the challenges in writing anything, be it a book, journal article, or edited volume, is that the act of writing something down tends to imply a degree of finality to the consideration of the topic. In real life, of course, debates are never settled fully. While all of the contributions in this volume are well-considered and thoughtful engagements with their subjects, we see all of our work as part of an ongoing discussion. We want them to inspire as many *yeah, but …* moments as *a-ha!* ones.

Furthermore, we are very conscious that although our individual names are at the top of each chapter, they are the product of numerous dialogues with other texts and colleagues. Of particular importance in this case were our four workshop discussants, who were selected according to their particular expertise and who each commented on two papers. While their work is reflected in the final versions of the chapters in this volume, we

wanted to make visible their perspectives, and to highlight the extent to which these papers are the product of an ongoing conversation that we hope continues far into the future. We have taken their comments and synthesised them with the themes that arose during the workshop's general discussion, presenting them here as "reflections" on the workshop.[4] We hope that they provide readers with an idea of the questions and issues these chapters have spurred in our minds as we worked through the puzzles they presented.

While the expansive nature of knowledge governance means that we are not able to cover all issues in an eight-chapter volume, we have organised the volume to highlight four themes. Each of the four parts includes two chapters, followed by a reflection from the discussant responsible for critiquing the papers.

The first section engages directly with Strange in an attempt to further develop her theoretical framework and to address some of the concerns raised in this introduction. Bannerman and Orasch's lead-off chapter begins by illustrating the relationship between what they identify as the three key parts of the knowledge structure—technology, ideas, and regulation—and the other three structures, including how these three structures (production, security, and finance) themselves feed back on and influence the knowledge structure. In doing so, they offer a template to other researchers who may wish to apply Strange's framework to their own issue area. What's more, they use Strange's framework to offer their answer to explain why some tech and information society writers were so much more optimistic than others. By considering four classic texts in terms of the extent to which their analyses engage with structures beyond the knowledge structure, Bannerman and Orasch conclude that analyses that more deeply engaged with all four of Strange's structures were more likely to register the potential for power inequities emerging from the interactions among the knowledge, production, security, and financial structures.

While Bannerman and Orasch point to the utility of Strange's multi-structural framework of analysis as applied to the political economy of communication literature, Haggart proposes a reformulation of Strange's knowledge structure that renders it more amenable to empirical analysis

[4] Brad Sherman served as the discussant on Debora Halbert's paper. However, as Jenna Harb and Kathryn Henne's paper was not presented at the workshop, the reflection on these two papers is credited to Haggart and incorporates Sherman's comments.

and addresses the problematic material/ideational highlighted in this introduction. He proposes an analytical distinction between the two, which he calls the *knowledge-legitimation* and *knowledge-regulation* aspects of the knowledge structure. This separation allows us to consider the interplay between the material and the ideational as it relates to the legitimation of knowledge, while focusing on knowledge's regulatory aspects highlights the power dynamics that shape the knowledge structure, as well as the forms of legitimate knowledge it supports. He uses this framework to analyse the negotiation of the Trans-Pacific Partnership (now the Comprehensive and Progressive Agreement for Trans-Pacific Partnership).

The second section is directly concerned with the exercise of structural power as it relates to knowledge governance and the internet. In a departure from the theoretical explorations from Bannerman and Orasch, and Haggart, Tusikov and Winseck offer highly empirical accounts that examine the power relations inherent within the IoT and the internet's material infrastructure. Tusikov argues that knowledge governance is a core feature of the IoT devices, which are embedded within copyright law and manufacturers' licensing agreements that govern the devices' all-important software. Control over software, Tusikov contends, enables control over hardware, meaning that consumers have a limited, even precarious ownership over their purchased goods. Drawing from critical data studies, her chapter invites a consideration of the changed nature of ownership of software-enabled physical goods and, more broadly, the ways in which manufacturers' control over data, in this case from IoT devices, is an increasingly important source of regulatory power and central feature of the global political economy.

Winseck, meanwhile, tackles the conventional wisdom regarding American dominance of the internet. The full picture regarding American power requires looking not just at the content layer of the internet, but also at who controls the physical machinery of the internet—a pure expression of structural power. From this perspective, he argues, the issue of control is much more complex. The rise of non-American control over and involvement in key internet-infrastructure projects around the world suggests that American dominance is already on the wane. In its place, he argues we are likely to see the emergence of what Eli Noam calls a "federated internet."

The third section focuses on what Haggart calls the *knowledge-legitimation* aspect of the knowledge structure: the determination of truth. Halbert's contribution considers copyright—a central form of

regulation in a market-based, knowledge-driven economy—as a tool of censorship. While we are used to thinking of copyright as a law regulating the market in creative works, it functions primarily by determining what can and cannot be expressed, that is, as a form of censorship. Copyright's censorship function has long been targeted by activists in the name of freedom of expression and creativity. Complicating this easy narrative, Halbert profiles two cases in which copyright has been "weaponised" as a tool to fight racism and white supremacy. Given the toxic effects of racism and white supremacy, does this make copyright-as-censorship a good thing? Is tolerating neo-Nazi screeds the price of free speech? Halbert, in the end, rejects this simple framing and invites us to consider not the unrealistic question of whether rules should govern speech, but *what rules* we should adopt. Because there are always rules.

If Halbert's chapter focuses on the use of copyright to delegitimise forms of knowledge (be it culturally enriching or racist and socially destabilising) through its suppression, Harb and Henne's chapter focuses on another form of knowledge power: the delegitimisation of individuals and peoples through the creation of misinformation and disinformation. The ability to determine what counts as legitimate knowledge is a fundamental source of structural power within the knowledge structure, and they show how the U.S. and Canadian governments have used this power against Indigenous populations. If nothing else, as they state, it is a reminder of the continued (structural) power of the settler colonial state to, in a sense, define reality.

Following on Harb and Henne's analysis on state use of misinformation to define and delegitimise vulnerable peoples, the chapters in the final section engage with how knowledge-regulation is used to control people.

Surveillance features prominently in both chapters, in two different contexts. Henne's chapter examines the increasingly relevant practice of jurisdictions using biometric technologies to collect data and verify of social assistance recipients. While usually promoted as a way to save money and prevent fraud, they also represent mechanisms of control over the most vulnerable people in society. Henne considers the Aadhaar system in India, which has issued over one billion unique identification numbers since being launched in 2010, examining the way that such surveillance works as a means to regulate its subjects.

Fish centres her analysis on the history of surveillance at the Mariposa Port of Entry in Ambos Nogales (Nogales, Sonora, in Mexico and Nogales, Arizona, in the United States). Surveillance, she argues, does not exist on its own, nor are its effects solely determined by its technological form (having

changed from face-to-face and paper-based monitoring to more complex digital and visual surveillance). Instead, it must be understood in its particular social and legal context. Ambos Nogales, as a meeting point between two nation-states, intersecting with social, political, and economic interests, is therefore an ideal place to examine how particular technological and social intersections work to define legitimate cross-border practices, including how "trust" is constructed in determining who and what is considered to be legitimate travellers and trade.

In our conclusion, we offer our answers to our primary questions—what is the nature of the knowledge structure as it is currently constituted? In whose interest is it operating? Drawing on the previous eight chapters, we assess the utility of Strange for understanding knowledge structure-related developments, arguing that this collection points to the many ways power structures are shifting. In the interests of continuing this important discussion we make an argument for treating knowledge governance as a single, albeit interdisciplinary, field of inquiry, defined by subject and open to diverse perspectives, similar to Strange's conception of IPE, and lay out a Strange-inspired research agenda. It is our hope that this agenda and the research presented in this volume will inspire others to approach knowledge governance as an integrated field of study, with this Strangean framework as a potential meeting point for future inter- and multidisciplinary research.

References

Berger, Peter L., and Thomas Luckmann. 1966. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. London: Penguin.

Breznitz, Dan. 2007. *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland*. New Haven: Yale University Press.

Bridy, Annemarie. 2015. Internet Payment Blockades. *Florida Law Review* 67 (5): 1523–1568.

Centre for the Study of Globalisation and Regionalisation. 1998. Susan Strange Obituary. *Newsletter* Issue 2. Accessed November 9, 2018. https://warwick.ac.uk/fac/soc/pais/research/researchcentres/csgr/newsletters/nl2.pdf.

Cox, Robert W. 1981. Social Forces, States and World Orders: Beyond International Relations Theory. *Millennium: Journal of International Studies* 10 (2): 126–155.

Germain, Randall, ed. 2010. *Global Politics & Financial Governance*. London: Macmillan.

Gitelman, Lisa, ed. 2013. *Raw Data Is an Oxymoron*. Cambridge, MA: MIT Press.

Glaser, April. 2018. The Watchdogs That Didn't Bark. *Slate*, April 19. Accessed November 9, 2018. https://slate.com/technology/2018/04/why-arent-privacy-groups-fighting-to-regulate-facebook.html.

Haggart, Blayne. 2017a. Introduction to the Special Issue: Rise of the 'Knowledge Structure': Implications for the Exercise of Power in the Global Political Economy. *Journal of Information Policy* 7: 164–175. https://doi.org/10.5325/jinfopoli.7.2017.0164.

———. 2017b. Incorporating the Study of Knowledge into the IPE Mainstream, or, When Does a Trade Agreement Stop Being a Trade Agreement? *Journal of Information Policy* 7: 176–203. https://doi.org/10.5325/jinfopoli.7.2017.0176.

Haraway, Donna. 1988. Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. *Feminist Studies* 14 (3): 575–599.

Langley, Paul. 2009. Power-Knowledge Estranged: From Susan Strange to Poststructuralism in British IPE. In *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*, ed. Mark Blyth, 126–139. New York: Routledge.

Malcolm, Jeremy. 2017. Payment Processors Are Profiling Heavy Metal Fans as Terrorists. *Electronic Frontier Foundation*, July 14. https://www.eff.org/deeplinks/2017/07/payment-processors-are-profiling-heavy-metal-fans-terrorists.

Marsden, Christopher. 2011. *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*. Cambridge: Cambridge University Press.

May, Christopher. 1996. Strange Fruit: Susan Strange's Theory of Structural Power in the International Political Economy. *Global Society: Journal of Interdisciplinary International Relations* 10 (2): 167–189.

Mytelka, Lynn K. 2000. Knowledge and Structural Power in the International Political Economy. In *Strange Power: Shaping the Parameters of International Relations and International Political Economy*, ed. Thomas C. Lawton, James N. Rosenau, and Amy C. Verdun, 39–56. Aldershot: Ashgate.

Sen, Gautam. 1998. Obituary: Professor Susan Strange. *The Independent*, December 9. https://www.independent.co.uk/arts-entertainment/obituary-professor-susan-strange-1190179.html.

Strange, Susan. 1986. *Casino Capitalism*. Oxford: Basil Blackwell.

———. 1987. The Persistent Myth of Lost Hegemony. *International Organization* 41 (4): 551–574.

———. 1994. *States and Markets*. 2nd ed. New York: Continuum.

———. 1998. *Mad Money*. Manchester: Manchester University Press.

———. 1999. The Westfailure System. *Review of International Studies* 25 (3): 345–354. https://www.jstor.org/stable/20097604.

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

Whitworth, Sandra. 2006. Theory and Exclusion: Gender, Masculinity, and International Political Economy. In *Political Economy and the Changing World Order*, ed. Richard Stubbs and Geoffrey Underhill, 3rd ed., 88–99. Don Mills: Oxford University Press.

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

Zittrain, Jonathan. 2006. A History of Online Gatekeeping. *Harvard Journal of Law & Technology* 19 (2): 253–298.

PART I

Susan Strange and the Twenty-First Century Knowledge Structure

Taking Knowledge Seriously: Towards an International Political Economy Theory of Knowledge Governance

Blayne Haggart

International Political Economy (IPE) scholarship has traditionally focused its attention on issues of production, trade, and finance. The treatment of knowledge—particularly commodified knowledge—as a source and vector of power equal to or greater than that of finance or production is a key blind spot in our understanding of the global political economy. This chapter offers a framework, based on the work of Susan Strange, for considering the relationship between what she called the "knowledge structure" and the other key sources of political and economic power—security, production, and finance. Because Strange's structural framework is explicitly

This chapter is a modified and updated version of an article that originally appeared as "*Incorporating the Study of Knowledge into the IPE Mainstream, or, When Does a Trade Agreement Stop Being a Trade Agreement?*" *Journal of Information Policy 7 (2017): 176–203.*

B. Haggart (✉)
Brock University, St. Catharines, ON, Canada
e-mail: bhaggart@brocku.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_2

concerned with the relationship among these four factors, it offers a useful way for scholars to treat knowledge governance—including intellectual property (IP), internet governance, and data governance—as a significant influence on economic prosperity and societal well-being.

This chapter also proposes an articulation of Strange's knowledge structure that attempts to address her assertion that the effects of the knowledge structure were "unquantifiable" (1994, 119). It does so by disaggregating Strange's framework into two interrelated but analytically separable aspects—its *regulatory* aspect (the rules governing the creation, dissemination, and use of knowledge) and its *knowledge-legitimation* aspect (the processes by which certain knowledge is deemed legitimate or not). A focus on the regulatory aspect of the knowledge structure both reveals what knowledge is considered to be legitimate and allows us to investigate directly the key question of who benefits from particular expressions of knowledge-regulation, subjects that motivate the research discussed throughout this book. It also highlights the extent to which we are seeing the emergence of a newly dominant form of economic conflict, one centred not around free trade versus protectionism, but between what I call knowledge feudalism and digital statism.

This chapter is structured as follows. The first section defines what this chapter means by knowledge governance, emphasising its distinction between *information* and *knowledge*. This point is illustrated primarily with respect to IP and data. The second section presents the chapter's Strangean-derived theory of the knowledge structure. The third section uses an examination of the negotiations over the Trans-Pacific Partnership (TPP, now the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP) and the United States-Mexico-Canada Agreement (USMCA) concluded in September 2018, to underscore the utility of a knowledge structure-based analysis, particularly to highlight aspects of such agreements that are often missed when knowledge governance issues are not emphasised. It also defines the key dimension of the debate over knowledge governance, namely between knowledge feudalism and digital statism. The final section offers some thoughts about how scholars can use this approach to study the rising importance of knowledge governance in other areas of the global political economy.

1 Structural Power, Knowledge, and the Knowledge Structure

"Knowledge is power" is not a new saying. The control of knowledge has been central to human activity, whether it is religious knowledge in terms of how to get to heaven (Strange 1994, 123), scientific knowledge of how a steam engine works, or purloined knowledge used to compromise a rival country's president. The first step in understanding the role that knowledge plays in human society involves recognising the difference between knowledge and information. In their foundational work, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (1966), Berger and Luckmann define knowledge as "the certainty that phenomena are real and that they possess specific characteristics" (1966, 14). Knowledge is an approximation of an underlying reality—of phenomena—that we can think of as information. Knowledge is created through social processes; it is socially constructed. Consequently, knowledge creation involves human agency and interpretation: it is always and necessarily a partial, intersubjective representation of information/phenomena. It need not be an accurate representation of information/"reality"—as in the case of "fake news"—but it can be. For example, data, while often thought of as pure information, is a form of knowledge. It is a partial representation of underlying phenomena whose collection (through the decision to make an observation) and definition are the product of human decisions. As the title of Gitelman's 2013 volume put it succinctly, "Raw data is an oxymoron": it is knowledge, not information.

While knowledge has always been politically, socially, and economically central to society, its relative importance has arguably changed over the past several decades. The case of IP is instructive. IP is the legal framework regulating the creation, use, and dissemination of commodified knowledge, be it creative works (copyrights), industrial processes (patents), or identifying marks (trademarks).[1] It is a form of knowledge, not information, because it represents a commodified, partial apprehension of an underlying phenomenon. Copyright, for example, attributes the creation of a text to an individual author. In reality, of course, every text builds on

[1] These are the three primary types of intellectual property (IP); others include trade secrets and "neighbouring rights," which protect copyright-adjacent rights such as broadcasting.

and incorporates already-existing texts, as the citations in this chapter attest. As Jessica Litman notes, the notion of the individual author is merely a useful "conceit" that allows us to give some order to the creation of knowledge (1990, 42).

For most of the past several hundred years, IP has been a relatively obscure backwater, of interest primarily to those industries and practitioners directly affected by it, such as publishers and pharmaceutical manufacturers. This is no longer the case. That the 2015 National Security Strategy of the United States elevated the protection and enforcement of IP law to a national security concern (Halbert 2016; Haggart and Jablonski 2017) demonstrates the extent to which IP is no longer a niche issue. IP, as well as data and internet governance, now lie at the very heart of the global order.

More specifically, "intangible assets" such as IP, but also "brand names, research and development, patents and other forms of abstract capital such as digital platforms and data flows" have overtaken "so-called fixed or tangible assets in the profitability and valuation of many leading corporations" (Bryan et al. 2017, 56), accounting for anywhere from 50 per cent to 84 per cent of the market value of the Standard and Poor's 500 index (Monga 2016; Ocean Tomo 2015). This change signals the importance of the control of data and IP, and the means by which these are created and disseminated, which very much includes the internet, as well as the arrival of a transformative moment in the global political economy (Bryan et al. 2017, 57).

Understanding how knowledge operates in the global political economy requires unpacking the links between knowledge and society. The framework developed by Strange offers a compelling and coherent theory of how knowledge fits within the wider political economy. Strange argued that the exercise of relational power—the ability to get someone to do something they would not otherwise do—was much less consequential than the exercise of structural power. She defined structural power as

> the power to shape and determine the structures of the global political economy within which other states, their political institutions, their economic enterprises and (not least) their scientists and other professional people have to operate. This structural power … means rather more than the power to set the agenda of discussion or to design … the international regimes of rules and customs that are supposed to govern international economic relations. … Structural power, in short, confers the power to decide how things

> shall be done, the power to shape frameworks within which states relate to each other, relate to people, or relate to corporate enterprises. (1994, 24–25)

Some forms of structural power are more important than others. Strange identifies four in particular, which she argues are most necessary to the survival of human communities. They are as follows:

- security—"the provision of security by one group for another. They may in the process acquire advantages in the production or consumption of wealth and special rights or privileges in that society" (May 1996, 178);
- production—"what is produced, by whom and for whom, and on what terms" (May 1996, 179);
- finance—the ability to control and deny access to credit, and thus to production and markets; and
- knowledge, which this chapter will discuss below.

In contrast to a Marxist approach, which prioritises production as the foundation of power, or realist International Relations, which emphasises physical security, Strange does not accord a priori importance to any single structure. Rather, each can be relatively more important in a given era or situation (May 1996, 178; see also Cox 1996). For example, Strange's empirical work on global finance (e.g., Strange 1986, 1998) argues that finance has been the key structure in the global economy since the 1980s (May 1996, 180–181). By not prioritising one structure over another, her structural-power framework is more sensitive to various fundamental changes in the global political economy than production- or security-focused theories. Furthermore, she acknowledges that each structure is distinct yet interrelated. For example, in providing security, actors "may in the process acquire advantages in the production or consumption of wealth and special rights or privileges in that society" (May 1996, 178). The result is a framework that is historically based and alert to a multitude of areas from which substantial change might emerge.

It is also important to note that although Strange uses the language of "structures," human agency is a key component of her theory. Strange's framework focuses on the exercise of power and authority in the political economy, power being the ability to set (or have authority over) these structures. This authority is always exercised by actors, which can be both state and non-state actors.

2 Unpacking the Knowledge Structure

Although Strange placed knowledge at the heart of her analysis of the sources of power in the global economy (alongside production, finance, and security), her elaboration of the knowledge structure itself is both the "most suggestive (and problematic)" of Strange's four structures (May 1996, 182). Strange herself argues, "Power derived from the knowledge structure is … unquantifiable" (1994, 119), which would certainly seem to pose some small challenge to social scientists wishing to understand its effects. Thankfully, as this section will illustrate, this is not exactly the case: the knowledge structure is, in fact, capable of being analysed.

Strange defined the knowledge structure as determining "what knowledge is discovered, how it is stored, and who communicates it, by what means to whom and on what terms" (Strange 1994, 121). The key actors in the knowledge structure are "those who are acknowledged by society to be possessed of the 'right', desirable knowledge and engaged in the acquisition of more of it, and those entrusted with its storage, and on those controlling in any way the channels by which knowledge, or information, is communicated" (1994, 121).

In this definition, Strange identifies but conflates two related but distinct processes. The legitimation of knowledge involves deciding what is considered to be legitimate knowledge, and who is to be recognised as the purveyors or sources of this knowledge. This issue is separate from control over the communication (and, we could add, creation, dissemination, and use) of knowledge. Understanding what maintains and challenges ideologies—what is considered to be "the 'right', desirable knowledge"—is fundamentally a different task than understanding how knowledge (whatever form it may take) is created, disseminated, and used. Rendering Strange's knowledge structure concept useful as an analytical tool, therefore, requires disaggregating these two aspects.

2.1 Knowledge-Legitimation

Thankfully, these two categories are easily disaggregated, into what this chapter will refer to as the *knowledge-legitimation* and *knowledge-regulation* aspects of the knowledge structure. The first category, *knowledge-legitimation*, to use Strange's words, "comprehends what is believed (and the moral conclusions and principles derived from those beliefs)" and what is known (Strange 1994, 31–32). This is akin to the Berger and

Luckmann definition of knowledge mentioned earlier, which sees it as a partial apprehension of underlying phenomena.

It is this knowledge-legitimation part of the knowledge structure that Strange seems to argue is "unquantifiable." While it is possible to see that epistemologies and ontologies have changed over time, identifying the source of power to create beliefs (Langley 2009, 130) would seem to present some serious, if not impossible,[2] challenges, not least because of the socially constructed nature of knowledge itself. The knowledge-legitimation aspect of the knowledge structure also raises the question of its relationship to the rest of the global political economy. Strange argued that no structure, including the knowledge structure (specifically, its knowledge-legitimation aspect) has a fundamental primacy over any other. However, as Langley notes from a poststructuralist perspective, if socially constructed knowledge shapes how we approach the world, it must be given ontological primacy (Langley 2009). Tooze, like Langley, notes that while Strange recognises that power is constructed and maintained by belief systems and systems of meaning (e.g., language) and not simply by material means alone, her realist/positivist commitments prevented her from following this insight to its logical conclusion (Tooze 2000, 188–189). In short, she failed to place language and knowledge as necessarily prior to the other structures.

Scholars recognised this problematic aspect of Strange's knowledge structure early on. In grappling with this issue, May argues for a research agenda that focuses not only on

> questions regarding what is known by whom, but [also] as importantly *why certain truths are accepted as known, while others are not, and how this agenda of truth is set and contested within the knowledge structure*. When we start to address these sorts of issues, we can start to fully recognise the interaction between the knowledge structure and the security, production, and finance structures. (emphasis in original) (1996, 185; see also Langley 2009, 132)

While Strange's commitments may have prevented her from giving "ontological primacy to knowledge" (Langley 2009, 131), it is possible to incorporate Langley's, May's, and Berger and Luckmann's insights on the social construction of reality into Strange's model without sacrificing its utility in empirically analysing the effects of the knowledge structure. Acknowledging that the social construction of reality and knowledge

[2] For a classic example of how paradigm/belief shifts have been studied in political science, see Hall (1993).

necessarily requires recognising the knowledge-legitimation structure's (or *knowledge-as-belief*) primacy over the other structures, since knowledge shapes the terms on which we engage with the world. At the same time, Strange's posited connections between the knowledge structure and the other structures suggest that power related to knowledge-legitimation can be influenced by events in the other structures.

2.2 Knowledge-Regulation

The second part of the knowledge structure, the *knowledge-regulation* category, is more amenable to direct analysis. Knowledge must be communicated to others in order to be useful.[3] This happens via "channels by which beliefs, ideas, and knowledge are communicated—including some people [and ideas, one might add] and excluding others" (Strange 1994, 119). These are subject to political contestation and regulation. Thus, what form they take and who they favour can tell us a great deal about power in the knowledge structure.

This part of the knowledge structure consists of the formal and informal rules governing the creation, dissemination, and use of knowledge, and the networks—human, institutional, technological—involved in knowledge creation, dissemination, and use. Examples of this form of structural power include IP laws, data governance (decisions related to its collection and use), and internet governance. Many other examples could be added to this list. This regulatory part of the knowledge structure continues to be under-examined by International Relations and IPE scholars, even though we live in a time of "unprecedented structural change" within the global capitalist economy, facilitated, and stimulated by "unprecedented transnational communication capacities" (Comor 1994, 1).

Understanding this second part of the knowledge structure is crucial for three reasons. First, the fact that knowledge must be communicated to exist in any real form as knowledge means that studying the communication of knowledge—what is communicated, by whom, and how—can render visible dominant or conflicting ontologies and epistemologies: the supposedly "unquantifiable" becomes quantifiable. If we assume that which is deemed to be socially valuable is communicated, examining the regulatory characteristics of the knowledge structure can reveal

[3] This formulation ignores knowledge of the world that, in Berger and Luckmann's (1966) sense of the word, individuals share with no one.

what society believes to be valuable knowledge, and the key players in this area. For example, the distinction made by copyright law between otherwise identical digital copies of "legitimate" and "pirated" movies suggests that the arbiter of legitimacy in the cultural sphere are market-based actors, namely those movie studios that control economically valuable copyrights.

We can make a similar argument about data. Data (personal or otherwise) is what political economist Karl Polanyi would call a "fictitious commodity" (Polanyi 2001), a partial representation of human activity or naturally existing phenomena collected for some purpose. For example, a doctor might record your heartbeat to assess your health, while a fitness device might collect yours and others' heartbeats as data to be sold, perhaps to an insurance company. Failure to recognise that data is a form of partial, commodified knowledge governed by rules and norms can lead to perverse policy outcomes, perpetuating existing societal injustices and inequalities (Haggart 2018).

The analytical separation between the knowledge-legitimation and knowledge-regulation categories proposed here does not imply a functional separation; it merely allows for a wider variety of questions to be asked and investigated in a more analytically precise manner. Communication technologies and knowledge-regulation generally are co-constitutive with the knowledge-legitimation side of the knowledge structure. For instance, Comor (2001) argues that the increasingly commercial nature of the internet—shaped by regulation driven by key U.S. economic and political interests (knowledge-regulation)—would make it more likely to produce a global commercial society than the global civil society dreamed of by internet optimists (knowledge-legitimation). More recently, Powers and Jablonski (2015) argue that U.S. political ideology and commercial interests shape the U.S. Administration's "Internet Freedom" agenda. The effect in both cases is to promote regulations, laws, treaties, and technological standards that reflect and reinforce a specific view of what information should flow freely (political) and what should be restricted (commercialised), as well as ubiquitous electronic surveillance that represents a sharp departure from the privacy standards of the international postal (snail mail) regime. In short, regulation reflects ideology, and vice versa. Understand one and you are on your way to understanding the other.

Second, as has already been noted, access to and control over knowledge is increasingly becoming a direct vector for the exercise of power. The ris-

ing use of IP laws to capture value within global production chains—which implies a relatively less important role for labour and physical production—offers a clear example of this new reality (Dedrick et al. 2010). The increasingly ubiquitous state and commercial use of surveillance technologies and the datafication of everything demonstrates the same point (Gitelman 2013; Mayer-Schönberger and Cukier 2013; West 2017; Zuboff 2015).

Third, the question of whether the digital revolution is ushering in a fundamental change in our basic conceptions of knowledge and social organisation remains open. Strange, who died in 1998, argued that the digital revolution was not that revolutionary, because we have not seen a switch in what is considered authoritative knowledge (i.e., belief systems) as dramatic of that from religious to scientific authority during the Enlightenment (Strange 1994, 127–129). The continued propertisation of knowledge via IP and data has the potential to move us into a world of secular, corporatised knowledge, in which the legitimacy of a specific piece of information (i.e., whether it is "right" to use it) is determined not by an appeal to scientific truth, but to whether the knowledge has the appropriate ownership pedigree. Access to life-saving medicines governed/restricted by patents is an obvious example of this tendency.

Even if we are not witnessing an epochal change in the knowledge-legitimation part of the knowledge structure, it still makes sense to focus more on the knowledge structure, as even regulatory changes can have significant effects on everyday life.

3 Operationalising Strange: The Knowledge Structure in the Global Political Economy

The Strangean structural-power framework discussed above necessarily involves historical analysis. Highly protectionist IP rights, for example, did not just become important within trade agreements because of some law of nature or as the result of some inevitable feature of capitalism. Neither is there anything "natural" about the internet's decentralised structure, or its bias towards a particular conception of "internet freedom." Rather, knowledge structures emerge through historically contingent actions of state and non-state actors. By tracing how knowledge-governance regulations (*knowledge-regulation*) have changed over time, we can not only discern the key players exerting structural power, and whose interests

have been served by these changes, but we can also better understand changes in what forms of knowledge are considered to be legitimate (*knowledge-legitimation*).

For Strange, as has already been noted, power and authority "are conferred on those occupying key decision-making positions in the knowledge structure" (1994, 121). This approach suggests three questions that we can use to guide a substantive research agenda in the knowledge structure:

1. On the knowledge-legitimation side, quoting and paraphrasing May (1996, 185): why are certain "truths" accepted as known, while others are not, and how is this agenda of "truth" set and contested within the knowledge structure?
2. On the regulatory side, from Strange, how, to whom, and on what terms is knowledge created, communicated, and used?
3. How do changes in the knowledge structure affect the exercise of power and outcomes in other parts of the political economy?

To illustrate the importance of these questions, the following section uses the negotiation of the (CP)TPP to explore why IP and cross-border data flows are included in free trade agreements; who the dominant actors are exerting structural power in this area; and the implications of this exertion of structural power on the wider society.

This analysis highlights how the emergence of highly protectionist IP rights and an embrace of the free flow of (commodified) data across borders has come to be seen as a natural part of the international trade regime, even though the economics of intangibles such as IP and data is not the same as the economics of tangible goods. Specifically, these IP and data provisions reflect the exercise of structural power by key state and non-state actors promoting their conception of their own self-interest. The result has been the transformation of the global political economy from one based on production and finance to one dominated by knowledge.

3.1 The Curious Cases of Intellectual Property and Data in International Trade Agreements

Since the 1990s, IP rights have been a central feature of almost every major international trade agreement, to the extent that they are now normally thought of as being part of the international trade agenda. More

recently, cross-border data flows have also been accepted unquestioningly into these agreements. If one takes a small step back, however, the issues raised by their inclusion—in other words, their legitimation as a commodified form of "tradeable goods"—becomes readily apparent. Following the establishment of the Bretton Woods system, specifically the General Agreement on Tariffs and Trade (GATT) after World War II, countries have used international trade agreements to liberalise trade. This pursuit of "free trade" was legitimised through appeals to David Ricardo's famous 1817 theory of comparative advantage, which holds that—under certain circumstances—even countries that are absolutely worse at producing goods than their partners can gain from trade. It is not too much to say that the modern economic argument in favour of trade agreements rests almost exclusively on the shoulders of, and draws political and social legitimacy from, the theory of comparative advantage.

The major problem for including data flows and IP in trade agreements is that the theory of comparative advantage does not apply to intangibles such as IP and data. While the lower tariff and non-tariff barriers—the nominal goal of most liberal trade agreements—are supposed to encourage trade, stronger IP effectively acts as a barrier to the exchange and use of knowledge and the goods (such as books, journals, and digital files) that store this knowledge. While free trade can potentially result in win-win situations, stronger IP benefits IP owners and states that host these owners (primarily the United States), while disadvantaging non-IP owners, who must pay to access innovation-creating knowledge and hope that the terms are not too stringent. However, because these economic agreements tend to be seen through a trade lens, protectionist tendencies of IP are often ignored or downplayed. IP's inclusion in trade agreements (the "free" in front of trade is sometimes silent but always implicit) means that strong IP protection has been effectively legitimised by the doctrine of comparative advantage, despite comparative advantage having no relevance whatsoever to it. In this sense, IP can be thought of as a "free trade free-rider."

Data functions in a similar way. As with IP, the proprietary control of data allows for the establishment of network effects, potentially leading to anti-competitive effects (Haggart 2018; Srnicek 2017). The concern of control then becomes a key issue, affecting everything from individual property rights to the ability to deliver public services. On property rights, always-connected Internet of Things devices not only deliver data (to be analysed and quantified) back to the home company, they allow the company to treat the purchased object as a service that only works if it remains

connected, and the company can effectively brick it at any moment (see Tusikov in this volume). In much the same way, as private data companies increasingly establish themselves in markets such as rental housing, they appropriate and make proprietary data essential to the planning and delivery of government services; as Scassa notes in the case of Airbnb, this effectively creates a dependency relationship between city governments and Airbnb (Scassa 2017). Placed in a global context, with markets in areas of search and social networks dominated by U.S.-based monopolies, calls for free cross-border data flows can be seen as a problematic push to maintain U.S. dominance over data-based businesses. This dominance emerges because already-established U.S. giants can use free cross-border data provisions in international trade agreements to expand into other countries without facing any restrictions on their activities and dominate any local players. Such provisions can be problematic because they mean that individuals' data can be transferred to countries where they may face, for example, different privacy rules.[4]

3.1.1 Knowledge Feudalism

Such provisions enact a form of what, following Drahos and Braithwaite (2002), we can call knowledge feudalism, since the combination of proprietary knowledge and free cross-border knowledge flows lock IP- and data-poor countries into dependent relationships with IP- and data-rich countries and companies. In contrast, smaller countries and emerging companies will (or should) tend to pursue policies that enable balanced (user-friendly) IP provisions, greater cooperation related to data sharing and an openness to data-localisation provisions in trade agreements. Taken together, such policies would work to negate the advantages enjoyed by dominant, often-monopolistic knowledge-based companies.

Commodified knowledge in the form of IP and data emerged from historical processes deeply rooted in capitalism, Enlightenment individualism, and the emergence of the nation-state, which serves as the enforcer of IP rights and historically has pursued data collection as a means of self-identity and security.[5] In terms of our immediate questions related to the introduction of IP and data-flow regulations into trade agreements and

[4] This assertion actually understates the significance of this situation, since data is an increasingly central component of all business activities.

[5] On the historical emergence of IP, see Sherman and Bently (1999); on the state's relationship with data and statistics, see Scott (1998).

their benefits, we can begin our account in the 1960s for data flows and the 1970s for IP.

With respect to IP rights, both the presence of IP in trade agreements and their highly protectionist/knowledge-feudalist orientation emerged out of the domestic politics of the United States. In the 1970s, pharmaceutical companies, manufacturers whose business model was based on exploiting and protecting their patents, lobbied the U.S. government to pursue ever-stronger international IP protection (Drahos and Braithwaite 2002; Sell 2003). As Sell (2003) and Drahos and Braithwaite (2002) document extensively, they were resoundingly successful in convincing a government preoccupied with the potential loss of its economic hegemony to the rising "Asian Tigers," particularly Japan, to pursue stronger IP rights. Over the subsequent two decades, IP-based industries and the U.S. government, particularly the Office of the United States Trade Representative, worked together—with one side sometimes pulling or pushing the other—to make strong, protectionist IP rights an essential part of the U.S. trade agenda.

A similar story can be told for the inclusion of protection for free cross-border data flows in trade agreements. In this case, we can look to the famous roots of the internet itself in the 1960s as a U.S. military project designed to keep the country's command-and-control structure functioning in a decentralised manner in the event of a nuclear war. As Powers and Jablonski (2015) document, the decision in the 1990s to commercialise this nascent "information superhighway" led to the emergence of a vibrant commercial internet sector, whose economic lifeblood quickly became the data produced by its customers and captured through increasingly ubiquitous surveillance. As the birthplace of the internet and with a head start on the rest of the world, the United States produced the world's (with the primary exception of China) leading, and monopolistic, internet companies: Google and Facebook as the new kids on the block, joined by the previous generation's duopolists, Microsoft and Apple. Srnicek (2017) tells an alternate but complementary story, arguing that the push towards the increasing commodification of data was largely the result of the 2008 Global Financial Crisis, as companies increasingly turned to the use of data in order to maintain the economic returns to which they had become accustomed. This policy, while seemingly in keeping with the ideals of free trade, has the effect of allowing U.S.-based data companies such as Google and Facebook to use network effects to stifle potential competition in other countries (Haggart and Jablonski 2017; Powers and Jablonski 2015).

3.1.2 Digital Statism

Although knowledge feudalism is ascendant, it is not an inevitability set in stone. Rather, it is the socially constructed outcome of a confluence of social, political, and economic factors, largely centred on the United States. In response to this knowledge-feudalist strategy, we are witnessing in many corners the emergence of state-centred economic strategies emphasising national competitiveness and varying degrees of openness to less-restrictive IP rules, as well as an openness to considering limits on unfettered cross-border data flows. This chapter refers to this constellation of policies as digital statism, and can also perhaps be thought of as a form of digital economic nationalism. For example, in the area of machine learning (or "artificial intelligence"), states are being encouraged to pick winners in an attempt to create their own national champions to counter the U.S. giants. Sovereign patent funds, in which the state controls and licenses strategic patents to its favoured (domestic) industries, are attracting interest, as are public data trusts, which would control data generated by the public and put to socially approved uses (Fitzgerald 2017; Srnicek 2017). Cries for substantial regulatory reform of the giant internet platforms are becoming more common, particularly in regards to the need for governmental regulation (see, e.g., Srnicek 2017; Noble 2018; Schneier 2015). Many governments have embraced or are considering rules requiring that data generated in their territories remain in their territories, although they remain controversial (World Trade Organisation 2018, 143–144).

Such policies, rather than being traditional forms of protectionism, are at least partly a reaction to the particular nature of an economy based on the control of knowledge, and the monopolistic-style returns that can accrue to the company or country that controls economically valuable knowledge and the means of communication.

The global scale of the internet means that these issues, and the importance of telecommunications policy, assume a global importance. At the heart of this system currently sits the United States, which claims a special place as the guarantor of the internet. Just as the 2015 U.S. National Security Strategy sets out a national-interest position on IP, so too does it for internet governance: "As the birthplace of the Internet, the United States has a special responsibility to lead a networked world" (White House 2015). This leadership, the report continues, involves upholding "the long-standing norms of international behavior." The report lists these as including "protection of intellectual property, online freedom, and respect for civilian infrastructure" (White House 2015), suggesting that these

issues—internet governance, IP and data governance—should be seen as a unified form of knowledge governance, and the U.S. approach as a form of knowledge feudalism. As currently configured, global internet governance largely reflects U.S. commercial and social priorities, privileging political speech and protecting the interests of U.S.-based IP owners and internet data companies like Google (Powers and Jablonski 2015). These views are also reflected in the trade agreements to which this chapter now turns.

3.2 Trade and the (CP)TPP: When Is a Trade Agreement Not a Trade Agreement?

The TPP was negotiated largely in secret among the United States, Japan, and ten other Asia-Pacific countries beginning in 2008.[6] The agreement was signed in February 2016. Following the withdrawal of the United States in January 2017, the 11 remaining members negotiated a modified version of the TPP, the CPTPP, which was signed on March 8, 2018. Both the negotiation of the TPP and its quasi-successor agreement, the CPTPP, hold significant lessons for our understanding of global economic governance, especially as it relates to IP and knowledge governance. Most significantly for our purposes, in the absence of U.S. pressure the TPP's IP provisions were significantly watered down in the CPTPP, even as its data-governance provisions remained.

The negotiations for the "original" TPP, for many reasons, faced considerable and virulent opposition. In terms of motivations, proponents have focused on the TPP's role as a geopolitical move to counter China in the Asia-Pacific (e.g., Solis 2015) and the benefits that would accrue to members in a "free trade" area encompassing "12 nations on four continents" (e.g., Daley 2015). Its 30 chapters cover trade in goods and services, as well as investment dispute settlement, electronic commerce (i.e., internet governance), and IP rights (Office of the United States Trade Representative 2015). The dominant framing of the agreement was as a "free trade" agreement (e.g., Curry 2016).

The problems with the framing of the TPP as a "free trade" or even as a "trade" agreement are nicely illustrated by Nobel Prize-winning economist Paul Krugman's intellectual journey with respect to the TPP. On December 12, 2013, Krugman, the most prominent economist of his

[6] By 2016, TPP membership consisted of Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam, and the United States.

generation, remarked on his *New York Times* blog that he was "having a hard time figuring out why this deal is especially important." Krugman, an international trade economist by training, argued that the TPP was unlikely to have any significant effect because "most conventional barriers to trade—tariffs, import quotas, and so on—are already quite low" (Krugman 2013a). After over 60 years of continuous multilateral trade negotiations, the "battle" to liberalise the global trading regime "has been decisively won," with "import tariffs and other restrictions … reduced to the lowest levels the world has ever seen" (Rodrik 2011, 252). According to the World Bank, the average all-country most-favoured-nation applied tariff rate in 2010 was 8.1 per cent. This was down from 26.3 per cent in 1986. In high-income Organisation for Economic Co-operation and Development countries, the rate was even lower: 2.8 per cent in 2010 (Rodrik 2011, 252). Rodrik cites research arguing that eliminating all remaining tariffs everywhere would raise world economic activity by only one-third of 1 per cent (2011, 252).

However, as Krugman (2013b) realised only two days later and has since continued to remark (Krugman 2015a, b, c), the current generation of "trade" agreements are no longer focused mainly, or even primarily, on traditional trade issues and should not be analysed as if they do. Rather, IP and investor-state dispute settlement have emerged as the key areas of concern with the agreement, alongside the negotiations' all-enveloping secrecy. To this, we could add the TPP's e-commerce chapter, which guarantees cross-border data flows and prohibits the requirement of local data storage as a condition of doing business in a TPP country (Geist 2017). This guarantee fits with U.S. objectives to ensure that the internet's "pipes" remain open to the free flow of data, including U.S. IP, while potentially allowing U.S. security agencies legal access to data coming into or going out of the United States.

The withdrawal of the United States from the TPP led the remaining 11 states to renegotiate the agreement. As one would expect from IP-importing states, and in line with a digital statist framework, in the move from the TPP to the CPTPP, states, led by Canada (Geist 2017), agreed to suspend the original TPP obligations as they related to a number of IP factors:

- Obligations related to patent-term adjustment and patent-term restoration, data protection for small-molecule drugs and biologics, and certain provisions on patentable subject matter;

- An extension to the term of copyright and related rights, a provision on national treatment related to payments on copyright and related rights, and provisions related to digital locks and rights-management information, two key areas of digital-copyright law; and
- New obligations related to the liability of Internet Service Providers for the actions of their users, and related to enforcement in respect of encrypted program-carrying satellite and cable signals (Government of Canada 2018).

The provisions related to the free flow of data (especially CPTPP Article 14.4), however, remained, which is inconsistent with an anti-knowledge feudalist, digital statist approach and requires explanation.

3.3 A Strangean Analysis of the TPP and CPTPP

That non-trade issues are increasingly important in such agreements presents problems for our understanding of the meaning of such agreements and highlights the extent to which production is increasingly intertwined with knowledge governance. First, it calls into question the agreements' legitimacy, since they are not based on Ricardo's theory of comparative advantage. Second, and related, approaching these agreements as if they are primarily about trade obscures their potentially more-important longer-term role in setting global (non-trade) standards for IP and data.

As stated above, a knowledge-structure analysis of agreements like the TPP or CPTPP focuses one's attention on three key questions:

1. What type of knowledge is defined as important, and how this definition is set and contested within the knowledge structure—in this case, the TPP?
2. How do regulatory measures define and shape the creation, communication, and use of knowledge?
3. Who benefits from these rules and definitions?

The first two questions are intertwined, since regulations constitute particular definitions of knowledge. The IP chapter of the TPP can be seen as a continuation of the United States' decades-long push for ever-more-protectionist IP laws, bilateral trade agreements with countries such as Australia and Jordan, as well as the plurilateral and ill-fated Anti-Counterfeiting Trade Agreement (Flynn et al. 2012).

The TPP looks quite different if one starts from the perspective of the knowledge structure, taking seriously its knowledge-regulation components, rather than starting from the assumption that this "trade" agreement must primarily be about production and trade. Seen from this perspective, it appears as an attempt to lock the TPP members into a knowledge-feudalist framework. As Weatherall (2016, 2) notes, the TPP's IP chapter would have actually "facilitate[d] the erection of barriers to [the] free movement of goods and the provision of services across borders." For example, Weatherall argues that "the IP chapter is perhaps the only chapter in the TPP which [would have made] it *easier* to stop goods at the border because the border measures … which [would have] allow[ed] for detention of alleged infringements at the border, are broadly written" (2016, 3). While this finding should not come as a surprise, as it is in keeping with the reality, noted above, that protectionist IP almost necessarily acts as a barrier to exchange, it is obscured in discourses that focus on tariffs and treat IP in trade agreements as an issue that does not require extensive economic evaluation.

The protectionist, knowledge-feudalist aspects of the TPP's IP chapter could also be observed in its requirement that member countries extend the term of copyright protection to life of the author plus 70 years (Canada's, for example, was life plus 50 before the TPP talks; the 2018 USMCA that as of this writing is slated to replace the North American Free Trade Agreement would raise it to life plus 70). This change is an example of unabashed protectionism. Copyright is supposed to encourage the creation of creative works by providing creators with the exclusive right, subject to some exceptions, to exploit their work. This protection comes at the cost of restricting future creativity: all new knowledge builds upon existing knowledge, so placing restrictions on who is allowed to access a work necessarily affects future creativity and the flow of knowledge. Extending the term of protection by 20 more years after the creator's death, in Canada's case, moreover, will not incentivise the creation of any more works: most people can barely plan out their lives five years in advance, let alone 70 years after their death. Beyond this change, the chapter also included a ban on the circumvention of digital rights management tools, criminal enforcement of copyright laws, and a de facto notice-and-takedown regime for Internet Service Providers wishing to avoid liability for their customers' actions (Malcolm 2015; Geist 2015a, b), policies that would have served to strengthen member countries' IP regimes.

The TPP's e-commerce chapter's bias, meanwhile, was towards facilitating unfettered cross-border data flows. For example, paragraph 3 of Article 14.11 is a general prohibition on data localisation, and is worded in such a way to make it difficult for governments to require that data be stored locally, and not moved to another country where it would be covered by different data-protection frameworks (Kilic and Israel 2015, 3–4). This restriction raises issues around governments' ability to regulate on behalf of the privacy needs of its citizens, as citizens' data may be transferred to jurisdictions with lower privacy requirements. However, far from being contradictory, the two chapters are in fact complementary, in that the TPP's knowledge-related chapters privilege open networks over which well-protected (U.S.) IP can flow into other countries, with cross-border data flows subject to few local rules.

As this brief analysis suggests, the TPP privileged those actors that control economically valuable data and IP, and the means of distributing knowledge. The United States and U.S.-based industries were able to influence the rules towards knowledge-feudalist ends. While standard free-trade orthodoxy suggests that there is at least the possibility that "free trade" agreements (i.e., ones that lower tariff and non-tariff barriers) can lead to benefits for all parties, the knowledge-protectionist nature of the TPP would have made such a happy ending unlikely. Because it takes knowledge to create knowledge, knowledge-protectionist agreements almost necessarily benefit those who currently control existing commodified knowledge. Following this logic, the TPP can be seen as an agreement that was designed to create a global, knowledge-feudalist economic regime centred on the control and regulation of knowledge, in which current IP owners are well positioned to exact tribute from knowledge users (Balsillie 2016; see also Drahos and Braithwaite 2002). It would have reinforced global value chains in which production can be outsourced from the Global North to the Global South with the head companies in the Global North (such as Apple) able to maintain control over a large share of the value created through its control of IP. Strong IP protection in trade agreements effectively acts as rent-seeking, extracting revenue from foreign markets on behalf of Global North-based (primarily U.S.) IP owners. Including the free flow of data in these agreements is similarly designed to maintain the advantage of the global (U.S.) data giants. In terms of who would have benefitted, then, the United States, copyright and patent-based industries, and online technology and telecommunications companies like Google would have been the primary beneficiaries of agreements like the TPP.

The TPP represented a concerted effort by the United States to exert structural power, not only in the sense of setting the regulations of global market for knowledge, but also with respect to the knowledge structure's *knowledge-legitimation* aspect, to convince other countries that the U.S. position favouring protection over dissemination is morally superior to those that emphasise the need and right to share and access knowledge and culture (Haggart and Jablonski 2017). If this analysis is correct, treating trade agreements as being primarily about the cross-border movement of physical goods is missing the extent to, and the means by, which the knowledge structure is becoming increasingly dominant as a means to power in the global political economy.

One puzzle remains. If the CPTPP's IP provisions rejected the knowledge-feudalist approach to IP, why did the CPTPP member states not change the TPP's provisions in favour of free cross-border data flows? The answer, in this case, comes back to the agency of the actors involved. As already noted, Canada led the charge to strike the TPP's IP provisions from the CPTPP. This move was largely the result of a concerted lobbying campaign by the Canadian tech community, particularly former BlackBerry CEO Jim Balsillie and his associated Council of Canadian Innovators. They, as well as the Waterloo-based think tank, Centre for International Governance Innovation (CIGI), laid the intellectual and political groundwork to convince the Canadian government to give IP a higher priority in the negotiations and to pursue a less-protectionist, less knowledge-feudalist IP policy.[7] When it comes to data flows, however, governments remain, as of November 2018, behind the learning curve. The March 2018 Facebook-Cambridge Analytica revelations have led to a renewed appreciation of how Facebook had been engaging in ethically and legally questionable behaviour with its users' data in ways that may have contributed to the 2016 election of U.S. President Donald Trump and the Brexit vote in the United Kingdom. More generally, these events have served as a wake-up call as to the political and economic importance of data. They came, however, too late to influence the CPTPP. That said, it would be surprising if the next round of data-related trade talks were not affected by these revelations.

The changes in the CPTPP suggest an evolving but still limited understanding by the remaining countries of what it means to be in a knowledge-based economy, as the CPTPP countries dialled back the IP requirements while keeping the prohibition on data localisation. In other words, they were not yet acting fully as digital statists. This limited understanding

[7] Disclosure: The author has written several papers for CIGI.

was confirmed by the September 30, 2018, conclusion of talks between Canada and the United States to replace the North American Free Trade Agreement with a USMCA whose IP and data provisions largely replicate those of the TPP that the United States had rejected (Geist 2018a), including the 20-year copyright term extension and an even stricter data-localisation prohibition (Geist 2018b). Canadian willingness to give in on these issues demonstrates the United States' strong relational power over Canada (the ability to get one actor to do something they would not otherwise do), as well as the Canadian calculation that these "new economy" issues were not worth going to the mat to defend.

Nonetheless, states are becoming ever-more aware of the importance of IP rights to their economic prosperity, and how stronger IP rights tend to disadvantage IP importers (i.e., most non-U.S. and non-European countries). In contrast to IP, the effects of data commodification remain relatively understudied and poorly understood by policymakers. Given the monopoly position of U.S. data-driven corporations, such as Google, in the non-Chinese part of the global economy, these rules will contribute to the continued structural and relational power of the U.S. state and its data-driven firms.

4 Conclusion

Back when control over production was seen as a key determinant of state strength, it was often asserted that "What's good for General Motors is good for America." Now, in terms of the relative importance of the four sites of structural power, it is control over knowledge, not production, that has taken centre stage, a finding that is easily missed when one, for example, sees agreements like the (CP)TPP through a trade lens and not a knowledge lens. The choice of lenses can be consequential. As this chapter's analysis of the TPP and USMCA strongly suggests, adopting a trade lens as opposed to a knowledge lens leads governments to underestimate the far-reaching importance of knowledge-governance rules to the underlying structure of the entire economy.

A Strangean analysis has much to offer scholars who are already active on knowledge-governance issues. Its focus on foundational power structures allows us to highlight the inherently political, contestable nature of seemingly "natural" and "fixed" systems like copyright and the internet itself, while placing these issues within a wider political and social context.[8]

[8] In this, IPE overlaps with Critical Communication Studies, a relatively small subfield within Communication Studies.

By focusing our attention on knowledge as a vector of power, on the interplay of state and non-state actors, and the connections amongst key structures in the global political economy, Strange's conceptualisation of structural power offers us a coherent way to understand these changes and their implications.

As scholars, we would not consider our students to have received a complete education if they graduated without at least some understanding of international security, global finance, and global production. As the examples of the TPP and CPTPP suggest, the time has come to add the global regulation of knowledge to this list. Clarifying Strange's conception of the knowledge structure offers a necessary first step towards setting a twenty-first-century pedagogical and research agenda that will allow a more complete answer to the fundamental questions of the global political economy: Who governs? And who benefits?

References

Balsillie, Jim. 2016. For Canadian Innovators, Will TPP Mean Protection—Or Colonialism? *Globe and Mail*, January 30. http://www.theglobeandmail.com/report-on-business/rob-commentary/for-canadian-innovators-will-tpp-mean-protection-or-colonialism/article28462854/.

Berger, Peter L., and Thomas Luckmann. 1966. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. London: Penguin.

Bryan, Dick, Michael Rafferty, and Duncan Wiggin. 2017. Capital Unchained: Finance, Intangible Assets and the Double Life of Capital in the Offshore World. *Review of International Political Economy* 24 (1): 56–86. https://doi.org/10.1080/09692290.2016.1262446.

Comor, Edward A. 1994. Introduction: The Global Political Economy of Communication and IPE. In *The Global Political Economy of Communication*, ed. Edward A. Comor, 1–18. London: St. Martin's Press.

———. 2001. The Role of Communication in Global Civil Society. *International Studies Quarterly* 45 (3): 389–408. http://www.jstor.org/stable/3096084.

Cox, Robert W. 1996. 'Take Six Eggs': Theory, Finance, and the Real Economy in the Work of Susan Strange. In *Approaches to World Order*, ed. Robert W. Cox and Timothy J. Sinclair, 174–188. Cambridge: Cambridge University Press.

Curry, Bill. 2016. The ABCs of TPP. *Globe and Mail*, January 25. http://www.theglobeandmail.com/report-on-business/international-business/what-is-tpp-understanding-the-new-pacific-tradedeal/article26648948/.

Daley, William M. 2015. Free Trade Is Not the Enemy. *New York Times*, May 19. Accessed September 3, 2018. http://www.nytimes.com/2015/05/19/opinion/free-trade-is-not-the-enemy.html.

Dedrick, Jason, Kenneth L. Kraemer, and Greg Linden. 2010. Who Profits from Innovation in Global Value Chains? A Study of the iPod and Notebook PCs. *Industrial and Corporate Change* 19 (1): 81–116. https://doi.org/10.1093/icc/dtp032.

Drahos, Peter, and John Braithwaite. 2002. *Information Feudalism: Who Owns the Knowledge Economy?* London: Earthscan Publications Ltd.

Fitzgerald, Oonagh. 2017. *Understanding the Promise and Peril of Sovereign Patent Funds.* Centre for International Governance Innovation Policy Brief No. 102 (April). https://www.cigionline.org/sites/default/files/documents/Policy%20Brief%20No.102web_0.pdf.

Flynn, Sean M., Brook Baker, Margot Kaminski, and Jimmy Koo. 2012. The US Proposal for an Intellectual Property Chapter in the Trans-Pacific Partnership Agreement. *American University Law Review* 28 (1): 105–205. http://digitalcommons.wcl.american.edu/auilr/vol28/iss1/5/.

Geist, Michael. 2015a. Why the TPP Creates a Backdoor Copyright Takedown System in Canada. *Michaelgeist.ca*. Accessed October 13, 2015. http://www.michaelgeist.ca/2015/10/why-the-tpp-creates-a-backdoor-copyright-take-down-system-in-canada/.

———. 2015b. Canada Caves on Copyright in TPP: Commits to Longer Term, Urge ISPs to Block Content. *Michaelgeist.ca*. Accessed October 9, 2015. http://www.michaelgeist.ca/2015/10/canada-caves-on-copyright-in-tpp-commits-to-longer-term-urge-isps-to-block-content/.

———. 2017. Canada Successfully Stands Up for Balanced IP and Canadian Culture in TPP Deal. *Michaelgeist.ca*. Accessed January 23, 2017. http://www.michaelgeist.ca/2018/01/canada-successfully-stands-balanced-ip-canadian-culture-tpp-deal/.

———. 2018a. From Copyright Term to Super Bowl Commercials: Breaking Down the Digital NAFTA Deal. *Michaelgeist.ca*. Accessed October 1, 2018. http://www.michaelgeist.ca/2018/10/from-copyright-term-to-super-bowl-commercials-breaking-down-the-digital-nafta-deal/.

———. 2018b. How Canada Surrendered Policy Flexibility for Data Localisation Rules in the USMCA. *Michaelgeist.ca*. Accessed October 10, 2018. http://www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/.

Gitelman, Lisa, ed. 2013. *Raw Data Is an Oxymoron*. Cambridge, MA: MIT Press.

Government of Canada, Global Affairs Canada. 2018. What Does the CPTPP Mean for Intellectual Property? Accessed January 30, 2018. http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/sectors-secteurs/ip-pi.aspx?lang=eng.

Haggart, Blayne. 2018. *The Government's Role in Constructing the Data-Driven Economy.* Centre for International Governance Innovation, March 5. https://www.cigionline.org/articles/governments-role-constructing-data-driven-economy.

Haggart, Blayne, and Michael Jablonski. 2017. Contradictory Hypocrisy or Complementary Policies? The Internet Freedom Initiative, US Copyright Maximalism and the Exercise of US Structural Power in the Digital Age. *The Information Society* 33 (3): 103–118. https://doi.org/10.1080/01972243.2017.1294128.

Halbert, Debora. 2016. Intellectual Property Theft and National Security: Agendas and Assumptions. *The Information Society* 32 (4): 256–268. https://doi.org/10.1080/01972243.2016.1177762.

Hall, Peter. 1993. Policy Paradigms, Social Learning and the State. *Comparative Politics* 25 (2): 275–296. https://doi.org/10.2307/422246.

Kilic, Burcu, and Tamir Israel. 2015. *The Highlights of the Trans-Pacific Partnership E-commerce Chapter*. Public Citizen and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, November 5. http://www.citizen.org/documents/tpp-ecommerce-chapter-analysis.pdf.

Krugman, Paul. 2013a. TPP and IP, a Brief Note. *New York Times* (blog), December 14. http://krugman.blogs.nytimes.com/2013/12/14/tpp-and-ip-a-brief-note/.

———. 2013b. TPP. *New York Times* (blog), December 12. http://krugman.blogs.nytimes.com/2013/12/12/tpp/.

———. 2015a. The Mis-Selling of the TPP. *New York Times* (blog), May 19. http://krugman.blogs.nytimes.com/2015/05/19/the-mis-selling-of-tpp/.

———. 2015b. This Is Not a Trade Agreement. *New York Times* (blog), April 26. http://krugman.blogs.nytimes.com/2015/04/26/this-is-not-a-trade-agreement/.

———. 2015c. TPP at the NABE. *New York Times* (blog), March 11. http://krugman.blogs.nytimes.com/2015/03/11/tpp-at-the-nabe/.

Langley, Paul. 2009. Power-Knowledge Estranged: From Susan Strange to Poststructuralism in British IPE. In *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*, ed. Mark Blyth, 126–139. New York: Routledge.

Litman, Jessica. 1990. The Public Domain. *Emory Law Journal* 39: 965–1023. https://www.law.duke.edu/pd/papers/litman_background.pdf.

Malcolm, Jeremy. 2015. The Final Leaked 'Secret' TPP Text Is All That We Feared: Top Down Control of the Internet. *Global Research*, October 12. http://www.globalresearch.ca/the-final-leaked-secret-tpp-text-is-all-that-we-feared-top-down-control-of-the-internet/5481702.

May, Christopher. 1996. Strange Fruit: Susan Strange's Theory of Structural Power in the International Political Economy. *Global Society* 10: 167–189. https://doi.org/10.1080/13600829608443105.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

Monga, Vipal. 2016. Accounting's 21st Century Challenge: How to Value Intangible Assets. *Wall Street Journal*, March 21. https://www.wsj.com/articles/accountings-21st-century-challenge-how-to-value-intangible-assets-1458605126.

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

Ocean Tomo. 2015. Annual Study of Intangible Asset Market Value. March 5. www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study.

Office of the United States Trade Representative. 2015. Summary of the Trans-Pacific Partnership. Accessed November 16, 2016. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership.

Polanyi, Karl. 2001. *The Great Transformation: The Political and Economic Origins of Our Time*. Boston: Beacon Press.

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

Rodrik, Dani. 2011. *The Globalisation Paradox: Democracy and the Future of the World Economy*. New York: W.W. Norton & Company.

Scassa, Teresa. 2017. Sharing Data in the Platform Economy: A Public Interest Argument for Access to Platform Data. *UBC Law Review* 50 (4): 1017–1071. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3077996.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company.

Scott, James. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

Sell, Susan K. 2003. *Private Power, Public Law: The Globalisation of Intellectual Property Rights*. Cambridge: Cambridge University Press.

Sherman, Brad, and Lionel Bently. 1999. *The Making of Modern Intellectual Property Law*. Cambridge: Cambridge University Press.

Solis, Mireya. 2015. *The Geopolitical Importance of the Trans-Pacific Partnership: At Stake, a Liberal Economic Order*. Order from Chaos blog, Brookings Institution, March 13. http://www.brookings.edu/blogs/order-from-chaos/posts/2015/03/13-geopolitical-importance-transpacific-partnership.

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

Strange, Susan. 1986. *Casino Capitalism*. Oxford: Basil Blackwell.

———. 1994. *States and Markets*. 2nd ed. New York: Continuum.

———. 1998. *Mad Money*. Manchester: Manchester University Press.

Tooze, Roger. 2000. Susan Strange, Academic International Relations and the Study of International Political Economy. *New Political Economy* 5 (2): 280–289. https://doi.org/10.1080/713687770.

Weatherall, Kimberlee. 2016. Intellectual Property in the TPP: Is Chapter 18 the New TRIPS? http://law.unimelb.edu.au/__data/assets/pdf_file/0009/1954152/Weatherall,-IP-in-the-TPP-The-New-TRIPS.pdf.

West, Sarah Myers. 2017. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society* 58: 1–22. https://doi.org/10.1177/0007650317718185.

White House. 2015. *National Security Strategy of the United States of America*. Accessed September 3, 2018. http://nssarchive.us/national-security-strategy-2015/.

World Trade Organisation. 2018. *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce*. Accessed November 8, 2018. https://www.wto.org/english/res_e/publications_e/wtr18_e.htm.

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89. https://doi.org/10.1057/jit.2015.5.

A Strange Approach to Information, Network, Sharing, and Platform Societies

Sara Bannerman and Angela Orasch

Susan Strange's framework for international political economic analysis emphasises the importance of the interrelationships between what she saw as four interlinked structures and sources of power in the global economy: security, production, finance, and knowledge (Strange 1994, 26). As change occurs in one structure, it is important to systematically consider the implications of such changes in the other four structures. For example, contest and change in the knowledge structure, such as the rising size and importance of online platforms like Facebook and Amazon, have implications for production, security, and finance; such changes can shift loci of power in the global political economy, both geographically and in the state-capital-civil society nexus, in ways that have important social and economic implications.

Although Strange's work has often been overlooked in literature on the political economy of communication,[1] Strange provided a powerful lens

[1] Castells cited Strange in *The Network Society*, in discussing multinational corporations (2009, 121). Hassan's *The Information Society: Cyber Dreams and Digital Nightmares* (2008, 30) makes a passing mention of Strange's concept of "casino capitalism" (Strange 1986), and Comor mentions Strange in the context of a broader discussion engaging Robert

S. Bannerman (✉) • A. Orasch
McMaster University, Hamilton, ON, Canada
e-mail: banners@mcmmaster.ca; orascha@mcmaster.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_3

for examining this field, through which it is useful to consider existing scholarship on concepts of the information, network, sharing, and platform society. This chapter has two objectives. First, it provides an overview of how the knowledge structure interacts with the other three structures of power, emphasising the reciprocal nature of the influence of the knowledge structure on the other three structures. Second, it assesses the extent to which four major works related to transformations in the knowledge structure—Daniel Bell's *The Coming of the Post-Industrial Society* (1976), Manuel Castells' trilogy *The Network Society* (first published 1996–1998), Yochai Benkler's *The Wealth of Networks* (2006), and Nick Srnicek's *Platform Capitalism* (2017)—examine the interrelationships between Strange's four structures and their effects on the exercise of structural power, and the consequences for their overall conclusions.

Each of these classic (or soon-to-be-classic) works of information, network, sharing, and platform societies addresses the interactions between Strange's four key structures to different degrees. Daniel Bell's *The Coming of the Post-Industrial Society* (1976), published before Strange's key works as they relate to structural power, presented one of the first, and most salient, theorisations of the "information society." Bell examined the effects of information technologies (the knowledge structure) on production, thus focusing primarily on the knowledge structure and the production structure, predicting that computerisation would lead to a society of white-collar professional work, personal relationships, and scientific planning (1976; Webster 2006, 42). Manuel Castells' more complex account, in his trilogy first published in 1996 through 1998, theorised a set of changes attendant in the rise of what he calls the "network society" that took on board many of the interactions between knowledge, production, finance, and security. In 2006, Yochai Benkler published *The Wealth of Networks*, a rosy theorisation of the implications of internet-enabled commons-based peer production, focusing mainly on the knowledge and production structures. Benkler's picture of the sharing society was blind to many of the

Cox in the introduction to the edited volume *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy* (1996, 9). Jin, in *Digital Platforms, Imperialism and Political Culture* (2015, Chap. 4), discusses Strange's arguments about the decline of the state. Strange has recently been drawn on more prominently in Horten's *The Closing of the Net* (2016), and in several articles in a special issue of the *Journal of Information Policy* Vol. 7 (2017). See also Haggart and Jablonski (2017), 103–118.

elements of Strange's framework and to some of the inequities carried forward by information technologies. In 2017, a darker picture emerged in Nick Srnicek's *Platform Capitalism* and his conceptualisation of the platform society more broadly. Srnicek's work analysed the interactions between the knowledge, production, and financial structures, producing a nuanced picture of the ongoing inequalities that the interactions between these structures produce.

The extent to which each author engaged with the relationships among the four structures influenced their overall orientation. In particular, those theorists (Bell 1976; Benkler 2006) who neglected to address all four structures also failed to register ways in which power inequities can be sustained through the interactions between the knowledge, production, security, and finance structures. Bell (1976) and Benkler (2006) focused their analyses primarily on the knowledge and production structures but did not fully encompass the security and financial structures in their analyses. This helped lead, we argue, to rosy pictures of the information and sharing society, and to an inadequate account of the unequal power relations attendant in those societies. In contrast, Castells (1997) and Srnicek (2017) more fully accounted for all four of the structures that Strange's framework suggests are important, including the security and financial structures. These accounts bring on board a fuller account of the unequal power relations at play in information and sharing societies, emphasising the utility of Strange's approach.

Our chapter proceeds as follows. We begin by describing our conceptualisation of the knowledge structure as comprised of three aspects: technology, ideas, and regulation. In parts two, three, and four, we describe the interactions between each of the three aspects of the knowledge structure and the security, production, and financial structures, respectively. We also note the "feedback" of each structure into the knowledge structure, showing how changes in, for example, the production structure influence the knowledge structure. Throughout, we return to our four key texts to note the extent to which each addresses these key structures, and how their attention or relative neglect of the non-knowledge structures affect their analysis. We conclude that it is important for communications theorists to take into account all four structures of power and ask what the implications of changes in the knowledge structure are for civil society and progressive change today.

1 The Knowledge Structure

Knowledge, according to Strange, is one of four primary structures, or sources of structural power, in the global political economy. She noted that "structural power can […] be exercised by those who possess knowledge, who can wholly or partially limit or decide the terms of access to it" (1994, 28).[2] Strange argued that knowledge is a "special" kind of power:

> [K]nowledge is power and whoever is able to develop or acquire and to deny the access of others to a kind of knowledge respected and sought by others; and whoever can control the channels by which it is communicated to those given access to it, will exercise a very special kind of structural power. (1994, 30)

Information, defined as "meaningful data," contributes to knowledge, defined as "the summation of information into independent concepts and rules that can explain relationships or predict outcomes" (Zins 2006, 486). Bell, Castells, Benkler, and Srnicek emphasised the importance of information and knowledge as a source of relational and structural power; all of them, like Strange, accorded great importance to the structural importance of knowledge, and of how knowledge is transmitted and mediated vis-à-vis ICTs.[3]

Strange divided the knowledge structure into three parts: beliefs (value-based thought), knowledge ("what is known and perceived as understood"), and the channels of communication (1994, 119). For the purposes of our analysis, we find it useful to divide the knowledge structure, instead, into three parts: *technology, ideas and beliefs, and regulation*,

[2] For Strange, structural power is distinct from relational power, which is the power to cause someone to do something they would not normally do (1994, 24). In contrast, structural power is "the power to shape and determine the structures of the global political economy within which other states […] have to operate" (24–25). The latter, she notes, is increasingly what counts (24).

[3] While Bell saw the various sectors of society as separate, and de-emphasised the interlinkages between them (Webster 2006), Castells sees the network social structure as interrelated with other structures, production structures in particular. Castells sees the new network structure as transforming the labour structure (Castells 2009, xxiii), and even as reflexively transforming itself (Castells 2009, 78). Benkler, for his part, saw the rise of networks and commons-based peer production as decentralising both knowledge structures and production structures ("the capital structure of production and distribution of knowledge") (Benkler 2006, 30).

treating *ideas* and *beliefs* together as one part of the knowledge structure; discussing *technologies* rather than "channels" to broaden and update the scope of the technological change under analysis; and adding *regulation* as a key component of the knowledge structure, acknowledging the importance of knowledge and communications regulation as a key part of the knowledge structure.

1.1 Knowledge Structure: Technology

Technologies, and the infrastructures of knowledge and communication, play an important role in acquiring relational power. As Strange noted, "Today the knowledge most sought after for the acquisition of relational power and to reinforce other kinds of structural power (i.e. in security matters, in production and in finance) is technology" (1994, 31). Technological change implicates change in the production, security, and financial structures. It is also, in turn, affected by those structures and by ideational and regulatory changes within the knowledge structure itself.

Technology's role in driving economic and social change has been theorised in a number of different ways. Some such theories fall prey to charges of technological determinism, especially where they do not account for technological change as a complex process of interaction with all four structures of power. Because Bell pointed to computerisation as the main driver of the changes he anticipated in production, he was sometimes accused of technological determinism (Webster 2006, 44–45).[4] Somewhat similarly, Benkler saw technologies that enabled collaboration and sharing as primary drivers of changes in production, although he attempted to avoid charges of technological determinism by pointing to the important role of regulation and political battles in shaping the future of the networked information economy. He was nevertheless criticised as a technological determinist due to the overriding emphasis he placed on the affordances and power of information technologies to produce economic and political change, and the under-emphasis he placed on dialectic of competing interest groups attempting to control technological development (see Benkler 2006, 16–18; Vaidhyanathan 2006).

Castells and Srnicek, for their part, produced more complex accounts. Castells avoided charges of technological determinism by noting that networks of production, politics, and finance created feedback loops that fed

[4] Daniel Bell denied such charges (Webster 2006, 44–45).

into processes of technological change (2009, 5–6). Srnicek did so by understanding platform technology both as the driver, and an outcome, of changes in production (in the conditions of labour and the rise of information industries and platforms as major players), finance (rising financial volatility), and security (in the context of new forms of platform imperialism) (2017). These observations suggest that Strange's framework, in emphasising multiple structures of power and processes of interaction, provides a good antidote to technological determinism.

1.2 Knowledge Structure: Ideas

Changes in the knowledge structure also take the form of changing ideas and beliefs (Germain 2016). The rise of ICTs has been tied to changing concepts or perceptions of time and space. Bell and Castells have, in particular, focused on "the break-up of space and time" (Bell 1976, lxxix) and the "transformation of time" (Castells 2009, 460), and the rise of virtual reality as the elimination of spatial boundaries (Bell 1976, lxxviii; Castells 2009, 491–494). This ideational reshaping of time and space has had important implications in production, security, and finance, which we will explore in the sections to come.

Ideas associated with information and digital technologies often become hegemonic models for production and politics. Castells emphasised the power that the concept of a "network" has had in organising and transforming production, politics, and identity. Such ideational effects are noticed by Srnicek as well, theorised as an imperative to act within certain ideological parameters: "cities are to become smart, businesses must be disruptive, workers are to become flexible, and governments must be lean and intelligent" (2017, 13). Srnicek detailed the ways in which platforms produce a set of ideas and models that influence other structures of power. The very concept or idea of a "platform" is constructed as if it were a neutral apolitical ground—a platform upon which *others* speak—in part to duck responsibility and regulatory obligations for the activities that take place on platforms (Gillespie 2010; Srnicek 2017, 21). In these ways, ideas and beliefs have a powerful role to play in ordering, or reordering, knowledge, production, security, and finance structures.

1.3 Knowledge Structure: Regulation

Strange pointed to the importance of regulatory systems within the knowledge structure as key sources of structural power (1994, 128, 135). Whether it is public funding of research and development in science and education agencies (Bell 1976, 250–262), the impacts of financial deregulation and the resultant rise of multinational corporations on the network society, the regulation of intellectual property (Benkler 2006; Srnicek 2017, 114), or the importance of net neutrality regulations as a way to curb the power of transnational platforms (Srnicek 2017, 93), knowledge and communications regulation is an important element of the knowledge structure.

At the national level, regulatory structural power has shifted from national monopolies and state-owned media to arms-length regulators and private media and telecommunications companies. Susan Strange emphasised that the shifting of power from states to markets and corporations did not imply the decline in dominance of American power; rather, American dominance could be maintained and extended through such shifts (Strange 1989). Recent thinkers have echoed this point (Farrell and Newman 2018; Jin 2015). At the same time, regulatory power (the power to shape laws, regulations, rules, or technical standards) shifted from the national level to plurilateral regimes such as the North American Free Trade Agreement, to multilateral organisations such as the International Telecommunications Union and the World Intellectual Property Organisation; to private organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) (Mueller 1999); to private contracts and agreements governing the relationships between telecommunications, media, and internet services (Winseck 2017); and to technologies that determine what can and can't be done with digital platforms and technologies (Lessig 1999). At all of these levels, state power and inequality between states continue to play a role (Farrell and Newman 2018; Jin 2015).

Bell, Castells, Benkler, and Srnicek engaged with the technological, ideational, and regulatory changes attendant in the rising adoption of digital and network technologies. All four, as well, engaged with the importance of these changes in the production structure.

2 The Production Structure

Beyond the knowledge structure, Strange emphasised the importance of finance, security, and production in the exercise of structural power. Strange broadly defined the production structure as "…the sum of all the arrangements determining what is produced, by whom and for whom, by what method and on what terms" (Strange 1994, 64). The production structure represents the ways in which economic value is created, exchanged, and distributed. Strange understood the production structure as a fundamental force in shaping societal relations since, above all, societies are dependent upon labour relations and systems of production to feed, clothe, and shelter themselves (Strange 1994, 64).

Strange aligned with Robert Cox in understanding the production structure as a "system of accumulation"—a Marxian term which latently references the rather exploitative dimensions of the production structure and its relationship to other aspects of the "world order" (Strange 1996, 24). Such a system of accumulation is "the foundation, the base" (Strange 1994, 64), but is also dependent upon the information and network flows of the knowledge structure; the knowledge and production structures are in this way reciprocally connected.

2.1 Interactions Between the Production Structure and the Knowledge Structure

2.1.1 Technology

Similar to Bell (1976), Strange noted the ways in which technological change in the knowledge structure led to a rise in information work, causing companies to diversify into information sectors and centralise power in corporations headquartered within the United States (1994, 132–133). New technologies have enabled shifts in the product of labour, moving from an economy of goods (manufacturing) towards an economy driven by theoretical knowledge, technology, and information.

Castells echoed and expanded the insights of Bell and Strange, noting that the rise of network technologies, "were absolutely critical in ensuring the speed and efficiency of restructuring" of production (1997, 19). "Without new information technology," he argued, "global capitalism would have been a much-limited reality" (1997, 19). The networked economy, Castells emphasised, goes hand-in-hand with "downsizing,

subcontracting, and the networking of labour" (Castells 1997, 9), resulting in temporary, individualised labour, as well as declining trade unions and full-time salaried work (1997, 9–10).

Benkler, meanwhile, was dramatically more optimistic in what he saw as the likely impacts of technological change in the sharing society on labour and production. Focusing on technologies that enabled collaboration and sharing and the availability of tools of knowledge and cultural production, he predicted not centralisation, but the decentralisation of capital and production (2006, 30). This would lead, he suggested, to rising non-market forms of production, especially in the realm of culture. "New and important cooperative and coordinate [sic] action carried out through radically distributed, nonmarket mechanisms that do not depend on proprietary strategies" would result (2006, 3). In sum, Benkler expected what he termed "a new mode of production emerging in the middle of the most advanced economies in the world," driven by computer networks, for which information goods and services would "come to occupy the highest-valued roles" (6).

Srnicek, for his part, argued that the emerging platform society has centralising tendencies; instead of decentralising production, it has redrawn production and labour relations around access to digital infrastructure (Srnicek 2017; see also Fuchs 2014; Huws 2014). Online communications technologies have provided the infrastructure for the easy and efficient exchange of goods and services (Srnicek 2017; Drahokoupil and Fabo 2016) and companies such as Google, Amazon, Facebook, Uber, and Airbnb have developed and monopolised the technologies that link users to these platforms, gaining key monopolies in their respective platform-based industries. This has limited the public's ability to influence the direction of the digital marketplace, even as they are immersed within it (Kenney and Zysman 2016).

These technological shifts, and their attachment to monopoly platforms, have profoundly impacted employment and labour relations (see Fuchs 2014; Srnicek 2017). Corporations holding platform ownership, looking to their own profit margins, can create an environment that encourages the proliferation of part-time, precarious work, pushing the cost of labour down.

Srnicek (2017) noted the range of platforms that have transformed production. Advertising platforms have helped to make data mining an important part of the economy; cloud platforms are centralising cloud applications and services used by industry; industrial platforms have altered

production processes, streamlining them as part of an "industrial Internet of Things"; product platforms have transformed how goods and service are sold; and "lean" platforms like Uber and Airbnb have come to epitomise part-time precarious labour and hyper-outsourcing (35–53).

Platforms are increasingly important to the economic competitiveness of states because they confer structural economic power in the processes of production. Jin (2015) demonstrated the effect of platform technologies in the global political economy, highlighting the ways in which "non-Western countries have not, and likely cannot, construct a balanced global order because Google (including its Android operating system), Facebook, Twitter, and Apple's iPhones (and iOS), as well as YouTube, are indices of the dominance of the U.S. in the digital economy and political culture" (2017, 6).

Changes in the technological layer of the knowledge structure are significant in that they come to (re)draw the capabilities and processes of production both nationally and internationally. The impact of ideational change has pushed these impacts even further.

2.1.2 Ideas

Changing concepts of time and space have particular importance in restructuring production, impacting the perceived value of workers, labour, and privacy. Strange noted: "…the information revolution is rapidly devaluing the wealth and power of industrial workers—unless of course they also happen to be producers or processors of information" (1994, 132). Changing ideas about efficiency, precarious work, declining privacy, and the inevitability of such changes have, in many cases, given greater structural power to employers to extract greater profits while reducing social and employment obligations to workers (Castells 2009, Chap. 7; Srnicek 2017).

The ideas and beliefs that are part of the knowledge structure, as Strange emphasised, can also be important in processes of change in the production structure. Bell (1976), for example, noted the ways in which the structure of production would be altered by the rising importance given to information and theoretical knowledge; theoretical knowledge, he predicted, would be used in defining economic value, and would lead to a movement away from manual labour into professions and knowledge work—at least in the United States and other post-industrial economies. Castells focused on the ways in which the concept of the network would act as a model, restructuring production on a flexible, global, and

networked basis. He also emphasised the ways in which neoliberal market ideals of speed, efficiency, and productivity were buttressed by innovations in productive technologies; innovations in information and communications technologies (ICTs), he noted, have enabled the streamlining and organising information into readily accessible and manipulable units.

Benkler focused on the ways in which a decreased emphasis on intellectual property, and an expanded emphasis on commons, would, in the network society, shift production towards commons-based peer production. When determining how one defines an *idea* of "value," or of "the commons," this line of argument fixes that definition away from the material products of older economies and towards an ideational regime of some kind, thus shifting the epistemologies of previous knowledge structures towards a novel rendering. These ideas then shape the ways in which agents come to engage within the production structure of the sharing economy.

2.1.3 Regulation

Changes in the regulatory framework of the knowledge structure have also had impacts in relations of production. Deregulation of media and telecommunications have led to tremendous innovation in ICTs, which have transformed many areas of production. Free trade agreements in ICTs and telecommunications have facilitated an international production and consumption chain and propelled the rise of multinational corporations. Trade liberalisation in telecom has globalised ICT production, moving production to areas where labour costs are lower and contributing to the loss of living-wage, steady employment. Power has shifted from state-controlled innovation in ICTs to private sector-led innovation, affecting nearly every area of production. This is a shift away from older models of state-owned telecommunications and a general rise of relatively precarious labour in IT and telecommunications companies.

Free trade agreements have also raised levels of intellectual property protection around the world, protecting global markets in intellectual property for multinational corporations and changing the response of the state. For example, states are pursuing stronger copyright laws in order to reap the financial rewards from intellectual property and secure this revenue domestically (Haggart and Jablonski 2017, 103; Bannerman 2016). However, at the same time, free trade in intellectual property and ICTs has shifted economic and political power over production to multinational corporations, who continue to be the hegemonic players in telecommunications.

2.2 Feedback to the Knowledge Structure

The changes in the production structure addressed above come to further solidify a kind of neoliberal political economy where speed and efficiency are rewarded, even when their pursuit comes at a cost. The distribution of political and social power becomes concentrated in the hands of a few largely American (Jin 2015) monopoly corporations, while at the same time, to some extent, states lose agency over the control and regulation of the information produced and collected by corporations. Strange explains that "…when the production structure changes…big changes are apt to follow in the distribution of social and political power" (Strange 1994, 64), and this changed production structure then feeds back into the other structures. Inequality, a weakened voice for labour and precarious employment, coupled with corporate control and ownership over communication and information exchange, affects each structure in distinct ways. The finance structure is changed since the control over capital exchange and investment is shaped by information asymmetries, the security structure is changed, as it is increasingly automated and outsourced. As Strange noted, "Change in the production structure changes the very nature of the state. Its capabilities are changed and so are its responsibilities" (1994, 89). Such dynamics can be observed only through an examination of all four sources of power, and their interactions.

3 The Security Structure

While Bell, Castells, Benkler, and Srnicek all took account of the implications of a changed knowledge structure in production, not all noted the implications of such changes in the security structure. Strange defined the security structure as "the framework of power created by the provision of security by some human beings for others" (1994, 46). Those who provide security "acquire a certain kind of power which lets them determine, and perhaps limit, the range of choices, or options available to others" (1994, 46). While the state is, in modern times, a primary source of security, Strange points to other types of security also: the provision of security or protection from individuals (such as criminals), organisations (such as criminal or terrorist organisations), civil war or revolution, and environmental disaster (Strange 1994, 47). The definition of security has expanded to include information security alongside physical security; Horten (2016, 24), for example, drawing on Strange, points to internet

privacy, and control over the storage and/or dissemination of data as part of the security structure.

The knowledge and security structures are intensely interconnected; for example, that the roots of the internet lie in the American military has been well-noted (Bell 1976, lv; Benkler 2006, 40; Castells 2009, 68). However, the security structure has been a less integral part of many information, network, sharing, and platform society theories.

3.1 Interactions Between the Security Structure and the Knowledge Structure

3.1.1 Technology

ICTs, as Susan Strange noted, have a particular importance in the context of state security (Strange 1994, 126, 133–134), but also in the context of the security of non-state actors and groups, such as individuals, communities, and organisations. Private companies have benefited from a security-structure infrastructure that permits surveillance of employees and publics, and that affords digital locks and enforcement to protect intellectual property from appropriation through file sharing and the like. States have also benefited from a security-structure infrastructure that affords greater structural power to states—particularly core and authoritarian states—to undertake mass surveillance, and makes possible remote warfare using global positioning systems and drone technologies.

Major theorists of the information, network, sharing, and platform society have placed relatively little emphasis on the implications of technological change in ICTs for the security structure, and vice versa. Strange's framework suggests that these vectors are as important as those between the knowledge and production structures. More recent theorists, including Monica Horten (2016), have moved to fill the gap.

This is not to say that the security structure has been neglected entirely in the four accounts we examine. Some account was taken of the implications of ICTs for states, individuals, and civil society in the security structure under theories of the information, network, and sharing societies. These accounts were, however, not as full as are the accounts of implications in the production structure. Bell made note of the rise of early-warning networks, electronic

sensing, and computer-controlled weaponry (1976, 22, 357). Castells noted the changes that network technologies brought to the state security apparatus; they afforded "instant wars" that could be fought surgically and quickly (2015, 491).

Individuals and civil-society groups have also gained structural power through shifts in the knowledge structure. Benkler pointed to the ways in which networked communications can be used by members of civil society to circumvent authoritarian rule. He remarks, in particular, on the distributed architecture of the internet, which he suggested made it less susceptible to authoritarian control than mass media (2006, 266–271).

Individuals, for their part, have also gained some measures of security through the use of information technologies such as encryption, biometric security, and Internet of Things surveillance and monitoring devices that permit remote monitoring of the home for invasions, temperature drops, or leaks and floods. Individuals may gain some degree of structural power through the ability to personally create new software programmes and devices to meet personal security needs. For example, it is possible to create or utilise personal security and surveillance systems that would limit the options or range of choices for children, family members, or would-be invaders. However, the structural power afforded to individuals through new information technologies is highly limited, and may be countered by the power afforded to individuals to harass and control others online (Dragiewicz et al. 2018).

Horten (2016), drawing on Strange's framework, noted a deepening cooperation between corporations and the state in control of knowledge and security structures, and the tremendous losses in personal security, including privacy, suffered by individuals. She notes that the reduction in personal security and privacy imposed on individuals via user data profiling confers "a form of structural power in shaping access to knowledge because of its ability to shape the delivery of content to the user, and by limiting the preferences of the user it can also deny access to the content because the user simply never knows it is there" (2016, 24). Castells, meanwhile, emphasised the rise of global networks of organised crime and trafficking as a threat to state and individual security. Again, the benefits of security are unequally distributed; in some cases, technological underdevelopment made it difficult to prevent such happenings (1997, 188).

The emergence of platforms also has implications, not just for individual security but for state security as well. Backdoors to platforms like Google and Facebook, Yahoo, Skype, and YouTube are used in national

security programmes, such as the National Security Agency's PRISM programme, to conduct mass surveillance operations through bulk data collection (Horten 2016, Chap. 3). Platforms are enrolled, and access to them sometimes blocked, by states in the interest of national security (Jin 2015, 95; Morozov 2012).

Industrial security is also at stake, as industry processes, centralised in cloud and industrial platforms, increasingly tend towards monopoly (Srnicek 2017, Chap. 2). Industrial platforms can situate themselves as having insider knowledge of manufacturing security, further justifying their monopoly position (Srnicek 2017, 45).

Environmental security, food security, and security in terms of physical health are also all implicated by technological changes in the knowledge structure. ICTs themselves can pose environmental hazards, producing CO_2 and hazardous garbage, but can be used to monitor for environmental threats, or by activists and governments to raise awareness about environmental threats and risks through activist campaigns, early-warning systems, and emergency messaging systems. Furthermore, food security and health security are placed, more and more, in the hands of private producers of food and pharmaceutical products, who control the technologies and information that confer structural power over human security.

3.1.2 Ideas

Ideas and beliefs tied to changes in the knowledge structure have also shifted structural power in security. While this vector has not been well-emphasised in theorisations of the information and network society, Bell made mention of the rising importance of scientific knowledge in the development of military technologies such as hydrogen bombs, early-warning networks, intercontinental ballistic missiles, electronic sensing, computer-controlled weaponry, military logistics, and "automated" battlefields (1976, 22, 357). The concept of the network, which, Castells noted, works as a model for social organisation, has been transposed onto ideas about conflict and war. The use of network models and schemas of networked cyber action have been adapted into conceptualisations of cyberwarfare, and to increasing militarisation of the internet (Arquilla and Ronfeldt 2001).

Castells highlighted the ways in which changing concepts and perceptions of time, tied to new technologies, have altered the security structure by producing "instant wars" that are short and surgical. These shifts, he

emphasised, affect societies unequally; "instant wars," he said, "are an attribute of informational societies, but, as with other dimensions of the new temporality, they characterise the forms of domination of the new system, to the exclusion of countries and events that are not central to the emerging, dominant logic" (2009, 491).

3.1.3 Regulation

Regulatory changes in the knowledge structure, including laws against computer fraud and abuse, or hacking; privacy laws; network neutrality and regulation through internet filtering; the privatisation of telecommunications; intellectual property laws; and the globalisation of knowledge structure regulation, all have important implications in the security structure. In some senses, as Haggart explained, "national security policy and internet policy have been fused" (2017b, 164). Laws against computer fraud and abuse, or hacking; exceptions to privacy laws, especially on matters of law enforcement and national security; and intellectual property laws all confer structural power over the provision of security to states and private companies. Privacy laws have conferred structural power over personal information security to private corporations and, through exceptions, to law enforcement and national security agencies (Horten 2016, Chap. 2). Intellectual property laws have transferred structural power over the possible uses of knowledge structure infrastructures to states and to private corporations who benefit from global intellectual property laws. As Benkler noted, food and health security are implicated by intellectual property policies in ways that threaten to lock up innovation as well as place health and food security in private hands (2006, 328–353).

3.2 Feedback to the Knowledge Structure

Changes in the security structure feed back to the knowledge structure. "Instant wars" and cyberwars create winners and losers, fuelling and shaping growth in war- and cyberwar-related ICT industries. Workplace surveillance affects labour conditions, production, and profits within ICT industries. Cybersecurity regulation, intellectual property, antitrust regulation, and privacy loopholes help to shape ICT production and design, bolstering dominant players, and permitting widespread disclosure and transfer of personal information among ICT companies and services as a foundation for growth.

Just as they failed to account fully for the implications of changes in the knowledge structure in the security structure, so did Bell and Benkler fail to fully take on board the implications of these changes in the financial structure. Castells and Srnicek, for their part, better highlighted the implications of technological, ideational, and regulatory change in the knowledge structure on the financial structure.

4 The Financial Structure

Strange defined the financial structure as "the sum of all the arrangements governing the availability of credit plus all the factors determining the terms on which currencies are exchanged for one another" (Strange 1994, 90). For Strange, the financial structure consists of two fundamental components, the power to create and administer credit, as well as the power found within the monetary system itself, determining the relative value(s) of different currencies (1994, 90).

It is particularly important to examine the effects of technological change in the finance sector because technological changes in the knowledge structure interact with the finance structure in ways that have extended existing inequities. The financial structure, for its part, has had a significant effect on the knowledge structure, especially in financing its infrastructural development, and, in particular, the development of platforms—a discussion to which we shall return at the end of this section.

4.1 Interactions Between the Financial Structure and the Knowledge Structure

4.1.1 Technology

Strange pointed to the ways in which changes in the knowledge structure have had significant impacts on the financial structure. The rise of information technologies, she noted, permitted the growth and international expansion of currency, bond, and securities markets; banks and financial companies; and inter-banking systems. ICTs accelerated and expanded the availability of information about market trends and trading, enabling changes in the speed and exchange rate of monetary goods (1994, 133–134).

Other thinkers have built on these observations. Castells similarly noted that global computer networks have transformed global financial markets

(2009, xx). The global financial market, he suggested, is built on "a multidimensional infrastructure of connectivity: on air, land, and sea multimodal transportation; on telecommunication networks; on computer networks; on advanced information systems; and on the whole infrastructure of ancillary services (from accounting and security to hotels and entertainment)" connecting financial centres of New York, London, and Tokyo (2009, xxxv–xxxvi; see also 96). The networking of financial markets, Castells argued, had completely altered the conditions of the global financial order, through

> the integration of global financial markets that took place in the early 1980s using new information technologies. Under conditions of global financial integration, autonomous, national monetary policies became literally unfeasible, thus equalizing basic economic parameters of restructuring processes throughout the planet. (2009, 20)

The liberalisation and deregulation of telecommunications in the 1980s and its consequent growth, "prepared the ground for the global integration of financial markets and the segmented articulation of production and trade throughout the world" (2009, 60; see also 97). New information and networking technologies also

> made possible the invention of numerous exotic financial products, as derivatives, futures, options, and securitized insurance (such as credit default swaps) became increasingly complex and intertwined, ultimately virtualizing capital and eliminating any semblance of transparency in the markets so that accounting procedures became meaningless. (Castells 2009, xx)

New technologies have increased the availability and speed of financial data relevant to capital investment, impacting older structures and institutions around which money and credit were exchanged. The introduction of new ICTs has produced a globally accelerated financial system, defined through the quick and efficient movement of information and capital (Drummer, Feuerriegel and Neumann 2017, 221). ICTs working through algorithms and using "big data" have ushered in a new mode of exchange defined by greater "speed" and "efficiency" between discrete market agents across geographic points. Floor traders and traditional investors are being replaced by supercomputers and complex algorithms, allowing microsecond trading based on a collection of data from the news media, online analytics,

as well as corporate information regarding stock, price, and volume movements (McGowan 2010). This process is known as high-frequency trading (HFT) or low-latency trading, a reference to the speed and efficiency at which these exchanges occur.

Beyond speeding up trading instruments, the increased ubiquity of ICTs has influenced the methods by which credit is valued and granted, creating the infrastructure for novel types of crediting systems and new forms of currency (e.g., bitcoin). ICTs have opened up pathways for new types of crediting and exchange practices, both within and outside the traditional banking sector. These financial technologies, or "fintech," refer to a variety of activities that exist within the interplay of finance and communications technology (Dapp et al. 2014; McGowan 2010). This includes money management technologies such as bitcoin, a digital currency that is not directly tied to gold or commodity exchange but that relies on peer-to-peer networks and cryptography (blockchain) to solidify its value (Bonneau et al. 2015). Fintech also includes new financial payment and lending systems found in practices like microfinancing (Bruton et al. 2015; Mills and McCarthy 2014).

These changes in the financial structure produce winners and losers, which are sometimes geographically delineated, and the changing knowledge structure affects stratified financial systems in different ways. Castells argued that the global economy only reaches rich nations, while those in the Global South do not benefit from global capital in the same way (Castells 1997, 7; Castells 2009, 102). Even "financial inclusion" measures (Gabor and Brooks 2017) aimed at bringing individuals (specifically in the Global South) into "fintech–philanthropy–development" programmes that rely on people's use of mobile technology, gathering data from behaviour to assess risk and investment opportunities, facilitate a redefined and powerful role for financial institutions and the owners of capital. Fintech introduces a kind of market intervention that has the capacity to "decentralise" banking and facilitate disintermediation, whilst potentially posing threats to privacy and fairness of entry (Philippon 2016; Treleaven 2015).

4.1.2 Ideas

The transformative effect of certain ideas on the financial structure has been well-noted. While Bell took some note of the importance of new forms of knowledge facilitated by technology, focusing on rosy concepts of a managed global economy and a planned or managed "world society" (Bell 1976, 24–26, 348, 393; see also Castells 2009, xx), others went

further. Castells understood the rising complexity of computer-managed information as eliminating transparency and the possibility of management, thus exposing markets to the kinds of risks that led to the 2008 financial crisis (2009, xx). This made financial markets a kind of "global automaton" that imposed "its logic over the economy and society at large" (Castells 2009, xxi).

The financial structure, like the production structure, is affected by the rise of ideological notions of speed and efficiency. There is a set of theory and research which looks at the concept of speed, its manifestation in novel technologies and its relation to financial capitalism (Agger 2015; Glezos 2013; Virilio 1986, 2006). Perhaps more than in any other structure, the compression of space-time through technology is integral to the reinvention of the finance structure since it drives the pace of financial interaction. These ideas are similar to those which drove Strange's reading of "casino capitalism" (1986)—a financial world where the number and speed of financial transactions continue to grow, churning out increasing volatility in the marketplace.

One can also draw on theories of performativity in market economics (MacKenzie 2006) to understand the interconnections between the knowledge and finance structures. In examining this performative aspect of markets, Mackenzie theorised how "an economic theory or model posits a world" (2006, 45). In other words, the machinations of the market are contingent on the accepted viability and structured knowledge of how specific investments are pursued, devoid of an objective market assessment and merely reliant on the accepted collective knowledge of the investment community. These types of actions speak to the ways in which the knowledge structure permeates the actions of market investors in so far as they build an ideological basis within which they intervene and enact a market for themselves. In these moments, the knowledge structure builds the basis on which financial structures intervene and locate financial agency.

4.1.3 Regulation

Just as the privatisation, liberalisation, and deregulation of telecommunications have contributed to globalisation and innovation in the financial structure, so have intellectual property and privacy laws. For one, intellectual property laws have been exploited in the financial industry. HFT firms are protective of their algorithms as trade secrets; their "ownership" is pursued intently, making it difficult to "buy in" to the system or destabilise existing monopolies. The U.S. government has continued to

strengthen intellectual property rights with regard to HFT through the *Defend Trade Secrets Acts* of 2012, 2014, and 2016, firming the rights of ownership over trading algorithms and making it easier to litigate against perceived "thefts."

Privacy laws and regulation have largely worked to permit the use and exploitation of private data for the assessment of credit risk, or have failed to prevent and enforce privacy law against such uses. This lack of privacy control over an individual's data currently extends into the data derived from social media and various types of online behaviour (see Kshetri 2014). Due to the increased prominence and ubiquitous use of communication platforms such as Facebook, Instagram, and Twitter, as well as online shopping platforms such as Amazon, the crediting systems in the financial structure can now more easily gain access to data of individuals in the marketplace, creating expanded levels of economic surveillance.

4.2 Feedback to the Knowledge Structure

The novel methods employed in the accumulation and dispersion of capital produce new rules of the game. The effects of these changes feed back into the knowledge structure; financial actors, including banks and venture capitalists, have played significant roles in transforming the knowledge structure. Banks were a driving influence in liberalising the telecommunications industry, and the creation of venture capital has been essential to innovation in network and information technologies (Strange 1994, 92; Winseck 1998, 232; Castells 2009, 65). Regulators also played a role; Srnicek emphasised the role that eased monetary policy played in spurring investment in high tech, and specifically in large platforms like Amazon, Apple, Facebook, Google, and Microsoft following the financial crisis of 2008. That crisis led governments to take on debt and to engage in quantitative easing, closing the avenues of fiscal stimulus and investment in bonds by private actors, thus shifting investment to technology (Srnicek 2017, Chap. 1).

5 A Strangean Approach to Information, Network, Sharing, and Platform Societies

While existing theorisations of the information, network, sharing, and platform societies have taken into account reciprocal relationships between the knowledge and production structures, the reciprocal relationships

between the knowledge and security, and knowledge and financial, structures are, to date, somewhat under-theorised. Horten has, to some extent, filled the gap in her examination of the relationship between the knowledge and security structures, focusing on the importance of the regulatory aspect of the knowledge structure for security.

As our discussion in the previous section suggests, while all of our four key authors—Bell (1976), Castells (2009), Benkler (2006) and Srnicek (2017)—were primarily focused on developments in the knowledge structure, they differed to the extent that they engaged with the interrelationships between the knowledge structure and the other primary structures. Their degree of engagement had a significant effect on their overall orientation. For its part, Bell's (1976) account of the information society was weakened by its portrayal of a fairly unidirectional relationship between the technological aspect of the knowledge structure and production. His account of the rise of an information society freed, to some extent, from manual labour, and making use of computerisation and theoretical knowledge to manage economic planning and uncertainty de-emphasised, to some extent, the inequities that would play an important part in the information society. His vision was somewhat corrected by Castells' (2009) multidirectional account of the relationship between the ideational and technological aspects of the knowledge structure and production and finance. Castells, his theoretical model tempered by a more critical understanding of the ways in which globalisation and networking affected global production and finance (and by twenty years' hindsight) and the ways in which these developments feed back to the knowledge structure, presented a more nuanced account of the network society.

Benkler's (2006) theorisation, suggesting the rise of a new sharing society, suffered, like Bell's, from an under-theorised account of the power of finance in driving and promoting technological change in the knowledge structure, and in shaping the conditions of production. Despite his efforts to theorise the implications of commons-based peer production on food and health security, his account did not sufficiently take on board state interests in securing intellectual property and controlling or surveilling network communication infrastructures, and the regulatory and technological pressures that this entails. Such pressures serve to repress regulatory enablers of the sharing society. In contrast, Horten (2016), drawing on Strange's framework, offered an account of such pressures.

Srnicek's (2017) theorisation of platform capitalism presented a more robust account of the interrelationships between the knowledge, produc-

tion, and financial structures. He described the ways in which the financial structure, following the 2008 financial crisis, enabled the rise of platform capitalism, and the pressures that platforms and labour place on each other. He also noted the security structure's impact, through platforms' use of surveillance technologies, on labour conditions. Horten and Srnicek's theorisations thus presented a fuller account of the effects of a changing knowledge structure on other kinds of structuring forces.

Changes in the knowledge structure create effects and feedback loops that can shift power at the state-capital-civil society nexus. As Srnicek's work emphasised, the changes we describe in this chapter using Strange's framework have given significant structural power to the owners of ICT companies, as well as to more powerful states. Such companies—and platforms like Google, YouTube, Facebook, and Netflix in particular—have gained structural control over the menu of communication channels that individuals can access, through algorithms and machine learning, and over the architecture of the networks and devices upon which communications and communications platforms are built. While this control was, in large part, wrested from state monopolies in telecommunications and, in some cases, state-owned media, the state remains important in many respects, as having enabled the regulatory environment of technological change, globalisation, and, most recently, platform capitalism (Jin 2015, 109). As well, insofar as many platform companies are American, this affords significant power to extend American hegemony (Strange 1989; Farrell and Newman 2018; Jin 2015). Changes in the knowledge structure have also shifted power in the production structure to platform owners, to states and ICT owners in the security structure, and to those positioned to benefit from market volatility in the finance structure. Such shifts have counter-balanced, or outpaced, the empowerment of civil society and workers that Bell and Benkler had envisioned.

6 Conclusion

Many theorisations of changes in the knowledge structure fail to examine the full range of interrelationships between the knowledge, production, security, and finance structures. Some salient theorisations about what changes in the knowledge structure mean for civil society and production—access to the means of communication, the rise of commons-based production, more rewarding work, and continued economic prosperity—may

be blind to rising inequalities in the finance, production, and security structures, and to the impacts of dominant production, financial, and security interests on ICTs, ideologies, and regulation.

Susan Strange's theoretical framework, emphasising the interrelationships between the knowledge, production, security, and finance structures, has two main implications for those seeking to bring about change in the global political economy. First, it suggests that intervening in only one structure is probably insufficient. Interventions in the knowledge structure alone that do not contend with dominant interests in production, security, and finance may only produce limited, and short-lasting, effects. Her framework serves as a helpful tool for avoiding the fallacy of technological determinism; it suggests that technological change in the knowledge structure alone cannot be a driver of change; rather, changes in one structure affect, and are affected by, changes in the others.

Second, Strange's theory suggests that intervention might be necessary on all (intersecting) parts of the knowledge structure. The technological layer is a key battleground that affords structural power to those who control the technologies and channels of communication to permit or deny access to the means of knowledge and communication. The ideational layer is a second key battleground on which key ideas and ideals, such as the ideal of speed, the concept of "commons-based peer production" or the idea of a "platform" can be crucial to structural efforts to shape the visions of civil society, industry, and regulators. The third key battleground is the regulatory layer, which confers the structural power of governance to limit or enable ranges of options for technological design, in turn affording and limiting the potential of civil society and industrial projects.

Strange's framework's decentring of the state sensitises us to pay attention to where, across many areas of the international political economy, power has shifted to private actors. This insight, too, has implications for those who seek to intervene in the dynamics of information, network, sharing, and the platform society. While states continue to wield structural power over private actors, private companies may also be fruitful targets of intervention, whether through strengthening the capacity for state intervention, through attempting to intervene in the direction of policy, or through activist intervention (Drahos 2017). Strange also suggested that power has shifted to international actors and to global governance—but

to a form of global governance marked by inequality and dominated by the most powerful states (1996, xiii).

Strange's framework may suggest a research programme more than it presents a fully developed theory (May 1996, 188). That it does not provide us with a theory of everything, however, does not take away from its usefulness for navigating the complexities of political change in the global political economy. Research into the role of changing knowledge structures in progressive change and social movements have produced conflicting arguments. In *Networks of Outrage and Hope* (2015), Castells outlines an optimistic reading of connected technologies, offering Occupy Wall Street and the Arab Spring as examples. Fuchs (2012) has criticised this view on the basis of its overly idealistic, and somewhat limiting rendering, of technology's role in protest—one that does not explain society's "structures, subjects and dynamics" more broadly (795). Understanding Strange's theory as a "research programme" corrects some of this "missing" theorisation into the role of technology in political change by directing scholarship towards the production, finance, and security structures that surround ICTs and communications devices. Scholarship that is interested in progressive change can take up Strange's work as a way to highlight the various, overlapping, yet discrete, structures that need tending to within progressive political praxis. A Strangean approach to information, network, sharing and platform societies draws attention to the relationships which produce and sustain changes not in the knowledge structure alone; it draws attention to the interrelated changes in knowledge, production, security, and finance.

References

Agger, Ben. 2015. *Speeding up Fast Capitalism: Cultures, Jobs, Families, Schools, Bodies*. London: Routledge.

Arquilla, John, and David Ronfeldt. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: Rand National Defense Research Institute.

Bannerman, Sara. 2016. *International Copyright and Access to Knowledge*. Cambridge: Cambridge University Press.

Bell, Daniel. 1976. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York: Basic Books.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven and London: Yale University Press.

Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. 2015. *Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*. Paper presented at 2015 IEEE Symposium on Security and Privacy (SP), San Jose.

Bruton, Garry, Susanna Khavul, Donald Siegel, and Mike Wright. 2015. New Financial Alternatives in Seeding Entrepreneurship: Microfinance, Crowdfunding, and Peer-to-Peer Innovations. *Entrepreneurship Theory and Practice* 39 (1): 9–26.

Castells, Manuel. 1997. An Introduction to the Information Age. *City* 2 (7): 6–16.

———. 2009. *The Rise of the Network Society. The Information Age: Economy, Society, and Culture*. Vol. 1. 2nd ed. Chichester, UK: John Wiley & Sons.

———. 2015. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Hoboken: John Wiley & Sons.

Comor, Edward A. 1996. Introduction. In *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*, ed. Edward Comor, 1–18. Berlin: Springer.

Dapp, Thomas, Lars Slomka, Deutsche Bank AG, and Ralf Hoffmann. 2014. *Fintech – The Digital (R)evolution in the Financial Sector*. Frankfurt am Main: Deutsche Bank Research.

Dragiewicz, M., D. Woodlock, B. Harris, and C. Reid. 2018. Technology-Facilitated Coercive Control. In *The Routledge International Handbook of Violence Studies*, ed. Walter S. DeKeseredy, Callie Marie Rennison, and Amanda K. Hal-Sanchez, 266–275. London: Routledge.

Drahokoupil, Jan, and Brian Fabo. 2016, July 14. The Platform Economy and the Disruption of the Employment Relationship. *ETUI Research Paper – Policy Brief*. https://ssrn.com/abstract=2809517.

Drahos, Peter, ed. 2017. *Regulatory Theory: Foundations and Applications*. Canberra: ANU Press.

Drummer, Daniel, Stefan Feuerriegel, and Dirk Neumann. 2017. Crossing the Next Frontier: The Role of ICT in Driving the Financialization of Credit. *Journal of Information Technology* 32 (3): 218–233.

Farrell, Henry, and Abraham Newman. 2018. Weaponized Interdependence. Paper presented at the International Studies Association Conference, April 4, 2018, San Francisco.

Fuchs, Christian. 2012. Some Reflections on Manuel Castells' Book "Networks of Outrage and Hope. Social Movements in the Internet Age". *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 10 (2): 775–797.

———. 2014. *Digital Labour and Karl Marx*. London: Routledge.

Gabor, Daniela, and Sally Brooks. 2017. The Digital Revolution in Financial Inclusion: International Development in the Fintech Era. *New Political Economy* 22 (4): 423–436.

Germain, Randall. 2016. Chapter 1: Susan Strange and the Future of IPE. In *Susan Strange and the Future of Global Political Economy*, ed. Randall Germain. London: Routledge.

Gillespie, Tarleton. 2010. The Politics of Platforms. *New Media & Society* 12 (3): 347–364.

Glezos, Simon. 2013. *The Politics of Speed: Capitalism, the State and War in an Accelerating World*. London: Routledge.

Haggart, Blayne, ed. 2017a. Special Issue. *Journal of Information Policy* 7.

———. 2017b. Introduction to the Special Issue: Rise of the 'Knowledge Structure': Implications for the Exercise of Power in the Global Political Economy. *Journal of Information Policy* 7: 164–175.

Haggart, Blayne, and Michael Jablonski. 2017. Internet Freedom and Copyright Maximalism: Contradictory Hypocrisy or Complementary Policies? *The Information Society* 33 (3): 103–118.

Hassan, Robert. 2008. *The Information Society: Cyber Dreams and Digital Nightmares*. Cambridge: Polity.

Horten, Monica. 2016. *The Closing of the Net*. Cambridge: Polity.

Huws, Ursula. 2014. *Labor in the Global Digital Economy: The Cybertariat Comes of Age*. New York: NYU Press.

Jin, Dal Yong. 2015. *Digital Platforms, Imperialism and Political Culture*. New York: Routledge.

Kenney, Martin, and John Zysman. 2016. The Rise of the Platform Economy. *Issues in Science and Technology* 32 (3): 61–69.

Kshetri, Nir. 2014. Big Data's Impact on Privacy, Security and Consumer Welfare. *Telecommunications Policy* 38 (11): 1134–1145.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

MacKenzie, Donald. 2006. Is Economics Performative? Option Theory and the Construction of Derivatives Markets. *Journal of the History of Economic Thought* 28 (1): 29–55.

May, Christopher. 1996. Strange Fruit: Susan Strange's Theory of Structural Power in the International Political Economy. *Global Society: Journal of Interdisciplinary International Relations* 10 (2): 167–189.

McGowan, Michael J. 2010. The Rise of Computerized High Frequency Trading: Use and Controversy. *Duke Law & Technology Review* 9 (1): 1–25.

Mills, Karen G., and Brayden McCarthy. 2014, July. The State of Small Business Lending: Credit Access During the Recovery and How Technology May Change the Game. Working Paper 15-004, Harvard Business School. http://www.hbs.edu/faculty/Pages/download.aspx?name=15-004.pdf.

Morozov, Evgeny. 2012. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Mueller, Milton. 1999. ICANN and Internet Governance: Sorting Through the Debris of "Self-Regulation". *Info, the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media* 1 (6): 497–520.

Philippon, Thomas. 2016. *The Fintech Opportunity*. National Bureau of Economic Research, Working Paper No. 22476. https://www.nber.org/papers/w22476.

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

Strange, Susan. 1986. *Casino Capitalism*. Oxford: Basil Blackwell.

———. 1989. Toward a Theory of Transnational Empire. In *Global Change and Theoretical Challenges*, ed. Ernst-Otto Czempiel and James N. Rosenau, 161–176. Lexington, MA: Lexington Books.

———. 1994. *States and Markets*. 2nd ed. London: Bloomsbury Publishing.

———. 1996. *The Retreat of the State*. New York: Cambridge University Press.

Treleaven, Philip. 2015. Financial Regulation of FinTech. *Journal of Financial Perspectives* 3 (3): 114–121.

Vaidhyanathan, Siva. 2006, May 30. The Dialectic of Technology. *Out of the Crooked Timber of Humanity No Straight Thing Was Ever Made Blog*. http://crookedtimber.org/2006/05/30/the-dialectic-of-technology/.

Virilio, Paul. 1986. *Speed and Politics: An Essay on Dromology*. New York: Columbia.

———. 2006. *Speed and Politics*. Los Angeles: Semiotext(e).

Webster, Frank. 2006. *Theories of the Information Society*. 3rd ed. New York: Routledge.

Winseck, Dwayne. 1998. *Reconvergence: A Political Economy of Telecommunications in Canada*. Cresskill, NJ: Hampton Press.

———. 2017. The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy* 7: 228–267.

Zins, Chaim. 2006. Conceptual Approaches for Defining Data, Information, and Knowledge. *Journal of the American Society for Information Science and Technology* 58 (4): 479–493.

Reflection I

Randall Germain

In this reflection, which is a mix of my initial discussant comments on these two chapters and a more general, post-workshop reflection on this project, I want to highlight three issues: the utility of Strange's framework for thinking about knowledge governance and International Political Economy (IPE) in general; issues related to knowledge as an object of analysis; and what a multidisciplinary reading of Strange can tell us about what her approach downplays or obscures, and how we might address some of the silences in her work.

1 The Benefits of a Strangean Analysis: The Big Picture and Granularity

This volume is concerned with big-picture issues: what is the nature of knowledge governance? What are the connections between various forms of knowledge governance and the larger global political economy? It is therefore fitting and appropriate that the editors and authors engaged with Strange, since her work is very much focused on the big picture. Strange was identified by Robert W. Cox as a critical theorist, someone

R. Germain (✉)
Carleton University, Ottawa, ON, Canada
e-mail: RandallGermain@cunet.carleton.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_4

interested in the potential for change in the constitutive underpinnings of society (Cox 1996, 177). As such, her approach is particularly appropriate for understanding those moments when, such as now, the global tectonic plates of social, technological and economic change are grinding against each other, putting into play previously taken-for-granted assumptions and practices.

Adopting a Strangean perspective pushes one towards looking for cross-social connections. Both of the chapters I comment on are diligent in examining the presence and two-way effects of the knowledge structure on the other structures Strange was concerned with, while the other chapters in this volume similarly explore the connections between the knowledge structure and the rest of the global political economy. For example, Tusikov looks at how the changing knowledge structure affects ownership in physical goods, while Fish's fascinating account of border surveillance highlights how changes in information technology have affected our conceptualisations of security (and vice versa).

Strange, however, is a very peculiar big-picture thinker. Perhaps because she started her professional career as a journalist, her broader framework is driven by agency. While she is primarily concerned with what she terms *structural power*, power does not emerge, as in many (often Marxist) structuralist accounts, from agents' position within a structure, but rather from agents' actions and their attempt to exert control over the rules and norms that govern human activity. While structural power exists at the macro level, Strange is more interested in who wields this structural power and to what ends; in other words, she is interested in authority—who has it and how do they use it? Her focus on how agents exert power provides us with a way to think organically about the role of power as something that agents can assemble and then exert. She does not provide us with a functionalist account of power as an objective, almost inanimate "thing"; rather, power is a capacity that is brought into being and used by agents and actors. When power is a key subject of analysis, there are always winners and losers. That is why the question, *cui bono?*, pervades Strange's work.

All theories imply specific methods, and Strange's framework is no different. Her conceptualisation of power as something that exists at a macro level but that is shaped by individual actions implies a very hands-on, empirical approach to analysis. Strange's framework requires that we get into the weeds of the issues. As she has noted, if you want to understand the global political economy, learn about a part of it (Strange 1984, 184). The granularity of this approach, meaning its embrace of empirical research

and prioritising the details of a particular part of the global political economy, allows us to understand how power works, and to whose benefit, in the larger scheme of things. (Although, as I will discuss later, this IPE-based conceptualisation of granularity is itself open to critique about what exactly granularity means, and whether this form of granularity obscures as much as it reveals.)

It is fitting, then, that almost all of the chapters in this volume employ empirically focused case studies to a greater or lesser extent. Even those chapters, such as the one by Fish, which are not primarily concerned with interrogating Strange's theory, fit nicely within this volume because they all share the same concern with sweating the details about how actual power is wielded by agents, and to what specific ends. This focus on case studies, on the facts of a situation, perhaps also suggests the utility of Strange's approach for facilitating multidisciplinary collaboration. In the case of this volume, almost all that is required is a commitment to constrained individual agency, agreement that the ability to set the framework within which others operate is a key form of power, and that control of knowledge is a key regulatory concern. It is not even essential that we all share the same definition of knowledge, as my comments in the next section suggest.

Finally, it is worth noting that the departure point in Strange's work is always power, which is well reflected in the Bannerman and Orasch, and Haggart chapters. It is a key contribution that Strange—and IPE studies in general—make to the study of knowledge and communications. For example, the four theorists used by Bannerman and Orasch do not fully engage with the issue of power, nibbling around the edges of the power question—who has power, what resources do they have at their disposal and how are these used to pursue policies that benefit them? A more direct concern with relational and structural power, a more thorough examination of the asymmetrical gains and losses that come with the ability to shape the context within which others operate—in other words, a more *Strangean* analysis—may have tempered some of their optimism and illuminated their pessimism, as Bannerman and Orasch suggest.

2 Knowledge as an Object of Analysis

While Strange paid attention to what she called the knowledge structure, the bulk of her life's empirical work focused on finance. Consequently, as Haggart's chapter notes, her thinking in this area was not as developed as her consideration of the other primary structures of the global political

economy. It was also slightly muddled, as Haggart and Bannerman and Orasch both suggest, suffering from poor specificity and confusion over the basic elements at play in its operation (cf May 1996; Cutler 2000; Tooze 2000). Nevertheless, even though Strange lacks a sharp specification here, the value of her conceptualisation of the knowledge structure lies in her identification of its importance and in the links that she makes between this structure and the other salient aspects of the global political economy. She teases out a fruitful way to operationalise the knowledge structure by focusing not only on "what knowledge is discovered, how it is stored, and who communicates it by what means to whom and on what terms," but also on what is considered to be the "right," most desirable form of knowledge (Strange 1994, 121). This opening presents us with a problem that can inspire productive and clarifying discussions of the type we see in this section.

The distinction between knowledge and information lies at the heart of this specification problem. Strange, for her part, argued that the difference between the two was unimportant, with knowledge being merely a more sophisticated form of information (Strange 1994). It goes without saying that this is a central issue for anyone claiming to study knowledge governance: we have to be able to define our object of analysis—both what it is and how it interacts with the wider world. It also matters for public policymaking. Is data just information, or is it something else? Is it a special form of knowledge with its own particular characteristics?

It is worth noting that all of the chapters in this volume correctly oppose Strange on this point. They argue that there is a distinction between knowledge and information, with knowledge being a social construct and information being, as Haggart puts it in his piece, more a natural phenomenon that exists independent of human observation. But the implication that knowledge is socially constructed invites more detailed questioning. For example, in defining the knowledge structure, both chapters in this section identify an ideological component—the power to determine what counts as knowledge—as distinct from other knowledge-structure components. But how are these components related to each other? This is an important feature to address, as the relationship among the components of the knowledge structure are, in fact, one of two ways in which dynamism and movement are built into its operation. The other way—which is actually captured by Strange—lies with who "controls" access to the various components of the knowledge structure. Here, both chapters very much advance our understanding because they are entirely about the issue of control over knowledge.

Strange's framework, applied to knowledge or any other issue, asks us to think about questions of authority and control: who has it, and how is it exercised? What we think knowledge is—how we define it—will affect our normative judgements about how it should be regulated. One of the big questions about knowledge concerns whether it is a public good. Both chapters in this section seem to assume that it is, but if knowledge is socially constructed, then it is so only because we have decided that it should be a public good. This decision has normative and positive implications. For example, Haggart argues that the inclusion of strong intellectual property rights in trade agreements amounts to a form of protectionism. However, it can only be seen as such if we see knowledge as a public good. This is not to argue that this is an improper approach to the analysis of intellectual property and trade agreements. Rather, it highlights the extent to which taking on board the assumption that knowledge is socially constructed (which seems to be the right move) highlights how far structural power—the ability, in this case, to influence the norms of what knowledge is—is even more important than Strange herself might have realised. It also returns us to the question of agency: who is able to influence or control these rules, and to whose benefit? In other words, we are back at the *cui bono?* question.

2.1 From Finance to Knowledge, from Tangible to Implicit

One of the strongest reasons to return to Strange for the key to understanding the global political economy is her sense that the creation of wealth in our economies is changing from the production of tangible objects to the production of intangible objects. This perception placed her somewhat in opposition to Marxist scholars, who claim that "in the end," it is production that drives everything. While Strange agreed that production was important, she did not give it pride of place, placing it alongside finance (her specialty), knowledge and security as being equally important primary structures of the global political economy. These intangibles did not include just knowledge. Her empirical work on the finance structure convinced her that money and credit—themselves intangibles in certain critical respects—had become increasingly central to wealth creation. Against the Marxist assertion that you had to accumulate in order to invest (thus making production prior to finance), Strange argued the opposite—that the ability to create credit precedes the capacity to invest. From this insight, it is but a short jump to understanding the ways the commodification

of intangible knowledge in the form of intellectual property and data could drive wealth creation. Crucially for public policy, the change in what constitutes the most profitable forms of value creation has completely disrupted the ways in which value had previously been created. In a capitalist economy, wealth is appropriated through private property; if knowledge is increasingly appropriated, this necessarily creates a new dynamic of accumulation. It is not the existence of data, for example, that is the main issue but rather the way in which data can be appropriated and used that is essential for understanding processes of innovation, knowledge and wealth creation, including value appropriation. It also suggests the need to join a political economy analysis to the types of analyses that traditionally have been concerned with, for example, data and intellectual property. It is an argument for political economy to concern itself with the relevance of domestic and international law around these issues, and especially with those who write these rules.

3 Gaps: Identity, Representation and Different Meanings of "Granularity"

This reflection has made the case that Strange's framework offers a productive way to consider issues of knowledge governance. This is not to say, however, that her approach is flawless. I have already noted her blind spots with respect to delineating exactly what the knowledge structure is. One of the benefits of a multidisciplinary project such as this one is that simply by virtue of bringing together such a wide-ranging group of scholars, the different approaches to a broad topic reveal or highlight gaps in one's preferred theories. One such gap related to Strange's take on knowledge that came up at the workshop was her neglect of issues of oppression related to the global political economy.

Of course, any multidisciplinary exercise such as this project carries with it the potential for misunderstanding to arise from the way that different disciplines use a familiar terminology. Yet, in this workshop, the way in which these contested understandings were worked through allowed for a very productive discussion to unfold. For example, as an IPE scholar, I find Strange's "granular" approach very attractive, for its essence consists of an appeal to empirical investigation into how the world is organised. It allows a framework or theory of how the world works to be built from the ground up, as it were. She was a strong critic of existing

efforts at the quantification of the social sciences because she believed that the gaps in our understandings of, for example, the finance structure, were too big to ensure that whatever metrics we use would offer an accurate representation of reality (Strange 1986, Chap. 4). Without appropriate metrics, any findings would be partial at best and misleading at worst. We need granularity to understand the world, but it must be a certain type of granularity. Yet, this term means something completely different in other disciplines, which means that we need to explore and build on the contested meaning of such ideas across disciplines if we want to understand the full spectrum of the knowledge structure's various components.

In the case of Strange's embrace of granularity, she was often criticised throughout her career as a blunt empiricist, where her efforts to be granular led her to frame problems in material terms at the expense of representation and/or social construction. This emphasis on materiality has at least two consequences relevant to this project. The first has to do with representation and different meanings of granularity. In Women's and Gender Studies, for example, as well as fields with strong ethnographic traditions such as Anthropology, looking at these more granular features entails a close and detailed focus on bodies and actors in context, accounting for them and their perspectives in terms of how they are implicated in systems of power. While Strange argues that agents are purposive, and she highlights how the exercise of structural power creates winners and losers, her analysis often loses sight of the nuances observable at these more micro levels. As such, it is perhaps not surprising that her work fails to account for—let alone analyse systematically—issues of identity formation, (mis)representation and interlocking forms of inequality, which can take on gendered, class, racialised, ableist and nationalist contours. The hierarchies of importance she constructed for her research—based on what she herself thought was of more or less "significance" for how the world was organised—meant that, for her, a subject such as inequality was secondary to what she saw as governments' colossal mismanagement of the financial system.

This lack of concern with interconnected inequalities and her commitment to materiality is evident in her parsing of the knowledge structure. Her conflation of knowledge and information, as May (1996), Langley (2009) and others (Cutler 2000; Tooze 2000) have noted, is a necessary move if she wants to argue that the knowledge structure is co-equal with the other structures. However, if knowledge is socially constructed—if understanding precedes actions—then Strange's deeply held belief in

materiality can be challenged. Doing so means that logically, the knowledge structure might be seen to "lead" other structures, or at the very least, be totally implicated in their formation and continuation. As Palan (1999, 126) has suggested, it might seem ironic that such an empirically minded scholar has opened the door to analyses that take seriously the role of ideas and their consequences, when she herself emphasised so much the materiality of the world. But for her, there was a philosophical root at the heart of everything, real or empirical. *Cui bono*, just maybe, is not only an empirical question.

4 Conclusion: Strange's Productive Problems

I have suggested, among other things, that Strange's commitment to a relatively narrow conception of materiality might constrain the applicability of her framework to fully understand some of the changes in the contemporary knowledge structure. But even if Strange herself did not go down any of the pathways offered by the contributors to this project, can her approach to granular analysis inform their appreciation of knowledge and its place, role or weight in today's world, especially with reference to the impact of how knowledge is used and/or controlled on people?

Other chapters in this book, particularly those by Harb and Henne, Henne, and Fish, and the reflection by Musto, offer their direct and indirect takes on this question. Another way to answer it is to consider the messiness, or eclecticism, of Strange's approach, particularly when it comes to the knowledge structure. Although she was a committed empiricist, her conception of the knowledge structure focuses on the power to decide what is considered to be legitimate knowledge, which is very much non-materialist. Similarly, although she did not focus on identity and representation, she placed individual agency at the very heart of her understanding of how the world works, and was deeply focused on the reality that structural power benefits some at the expense of others. Combine those two ideas and you might have the start of an intersectional, one might even say *granular*, analysis.

In the end, Strange's framework is just that, a general orientation for thinking about the world. Unlike a grand theory designed to answer questions about how the world works, Strange's framework is useful for the questions that it generates. Strange herself was no revolutionary—in the financial sector, her major criticism of the United States was that it was

acting irresponsibly as the dominant actor, leading to instability. She wanted it to lead, but in a responsible manner, because in the end, she thought that it was the only form of authority capable of righting the "ship-of-state" for global finance. But her framework, in laying out certain precepts about how the world works, could be used as a revolutionary tool as much as to maintain or improve the status quo. As this volume demonstrates, it offers a useful starting point for thinking about some big issues, while generating both productive problems and constructive questions.

References

Cox, Robert W. 1996. Take Six Eggs: Theory, Finance and the Real Economy in the Work of Susan Strange. In *Approaches to World Order*, ed. Robert W. Cox with Timothy J. Sinclair, 174–188. Cambridge: Cambridge University Press.

Cutler, Claire A. 2000. Theorizing 'No-Man's-Land' Between Politics and Economics. In *Strange Power: Shaping the Contours of International Relations and International Political Economy*, ed. Thomas Lawton, James N. Rosenau, and Amy Verdun, 159–174. Burlington, VA; Aldershot: Ashgate.

Langley, Paul. 2009. Power-Knowledge Estranged: From Susan Strange to Poststructuralism in British IPE. In *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*, ed. Mark Blyth, 126–139. New York: Routledge.

May, Christopher. 1996. Strange Fruit: Susan Strange's Theory of Structural Power in the International Political Economy. *Global Society: Journal of Interdisciplinary International Relations* 10 (2): 167–190.

Palan, Ronen. 1999. Susan Strange 1923–1998: A Great International Relations Theorist. *Review of International Political Economy* 6 (2): 121–132.

Strange, Susan. 1984. What About International Relations? In *Paths to International Political Economy*, ed. Susan Strange, 183–197. London: George, Allen & Unwin.

———. 1986. *Casino Capitalism*. Oxford: Basil Blackwell.

———. 1994. *States and Markets*. 2nd ed. London: Pinter.

Tooze, Roger. 2000. Ideology, Knowledge and Power in International relations and International Political Economy. In *Strange Power: Shaping the Contours of International Relations and International Political Economy*, 175–194. Burlington, VA; Aldershot: Ashgate.

PART II

Internet Governance and Regulation

Internet Infrastructure and the Persistent Myth of U.S. Hegemony

Dwayne Winseck

The idea that U.S.-based internet giants such as Amazon, Apple, Facebook, Google, Netflix, and Microsoft dominate the internet the world over is common—in academic writing across disciplines, the popular press, and everyday conversation. Derisory acronyms such as FAANG—Facebook, Amazon Apple, Netflix, and Google—capture the spirit of this idea. For some, this is not surprising, but rather the expected end result of neoliberal economic globalisation, and the liberalisation of global telecoms and internet policy that have been remaking the world in the U.S. image since the 1980s. Edward Snowden's disclosures about the U.S. National Security Agency-led internet surveillance programme have further galvanised claims about the extent of U.S. dominance of the internet (Carr 2016, 118–20;

This chapter is a modified and updated version of an article that originally appeared as "The Geopolitical Economy of the Global Internet Infrastructure," *Journal of Information Policy* 7 (2017): 228–267.

D. Winseck (✉)
Carleton University, Ottawa, ON, Canada
e-mail: Dwayne.Winseck@carleton.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_5

Powers and Jablonski 2015, 14–16, 109–110; Jin 2014; Kiss 2013; Fuchs 2010; Hill 2013; McChesney 2014).

This superficially persuasive conventional reading relies, however, on a partial consideration of the internet ecosystem. Expanding our frame of reference to include the internet's physical infrastructure paints a picture of internet governance that does not fit into a simple story of now-and-future U.S. hegemony. The United States certainly played a hegemonic role in the founding and early years of the internet, and U.S.-based internet giants certainly dominate much of the internet's middle and top layers, including operating systems (iOS, Windows, Android), search engines (Google), social networks (Facebook), online retailing (Amazon), over-the-top TV (Netflix), browsers (Google Chrome, Apple Safari, Microsoft Explorer), and domain names (the Internet Corporation for Assigned Names and Numbers, i.e. ICANN). However, U.S. firms and capital do not rule the hardware—or material infrastructure—of the internet. In fact, as this chapter shows, ownership and control of core elements of the global internet infrastructure such as the fibre optic submarine cables, autonomous system 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). The relative decline of U.S. hegemony and the emergence of an ever-more multipolar world are moreover captured by the fact that the U.S. share of global internet traffic fell from half the total in 2004 to 25 per cent in 2017. So, too, as we shall see, the global distribution of internet users reveals a similar pattern (Arrighi 1994; Desai 2013; Telegeography 2018a, b).

Such trends complicate the dominant conception of hegemonic U.S. control over what the influential political economist Susan Strange (1994) refers to as the knowledge structure. Rather than American internet imperialism, what Eli Noam (2013) refers to as a "federated internet" seems increasingly realistic, as ownership, control, and power over the material foundations of the internet become more multipolar in nature, shared and contested by an increasing number of state and non-state actors. This outcome will likely erode support for the current multi-stakeholder model of internet governance. This model is supported by many commercial interests, technical experts, and non-government organisations as well as the United States and other capitalist democracies instead of a more state-centred, multilateral model promoted by those who are critical of the unaccountable power of business interests and countries such as India, China, Russia, and Brazil, which—each in their own way—seek to counter what they see as the United States and Western capitalist countries'

dominance of internet governance. Ironically, all of this is taking place just as the United States has essentially walked away from its role as a pivotal player in these affairs in light of the Trump Administration's nativist inclinations and actions—a stance that China, Russia, the European Union (EU), and others are all too eager to use to their advantage. This might not be a bad thing, however, and is exactly the kind of scenario anticipated by Noam's view of a federated internet, backstopped by multilateral agreements at the international level through the century-and-a-half-old International Telecommunications Union (ITU), for instance.

The approach of this chapter follows Strange's focus on structural power, emphasising the changing relationship between markets and states—or the "market-authority nexus" (Strange 1994, 22)—over time and how hegemonic states act both on their own *and* in concert with others to structure the conditions under which other state and non-state actors operate. It also draws on David Harvey's (2003) concept of capitalist imperialism to help highlight the changes taking place and to counteract the dominant instrumentalist view in much of the literature, which sees communications media primarily as "weapons of politics" and "tools of empire" at the expense of market, technological and other considerations.

This chapter begins by placing the current debate in its proper historical context, noting both the similarities and radical differences between the internet and its nineteenth- and twentieth-century predecessors. The next section examines the question of U.S. internet dominance and the balance between states and market forces by tracing the rise of the internet's infrastructure as it now exists. The chapter concludes with some comments on the implications for internet governance and the structure of the internet arising from the potential emergence of Noam's idea of a federated internet.

1 Theorising Global Media History[1]

News and information have followed channels of trade, migration and cultural contact for millennia, but media historians often take the second half of the nineteenth century to the turn of the twentieth century as the moment when modern global communication and media systems took shape. The dominant view in the literature tends to adopt an instrumentalist

[1] The following two sections draw extensively from Winseck and Pike (2007) and Winseck (2011).

view of communications media as "tools of empire" and "weapons of politics" (Headrick 1991), or what David Harvey (2003) calls "territorial imperialism." To be sure, control over the medium and the message did confer commercial and strategic advantages to Great Britain, the dominant power of the era, and its free trade policy in general. Submarine telegraph cables in particular were designed to attract cables and capital in a bid to maintain London as the hub of the world economy and communication. Kelley Lee also crystallises this view by emphasising how "the integration of … European imperialism … was reinforced by telegraph (and later radio and telephone) networks *whose reach was historically defined by the boundaries of empire*" (Lee 1996, 60; emphasis added). The rapid ascent of U.S. commercial, political, and military interests from World War I on is also usually cast as having allowed it to displace Britain and Europe as the centre of world communication, and more fully after World War II when Pax Americana overtook Pax Britannica. Some claim that this is where things still stand today, especially in relation to America's imperial—or at least hegemonic—hold over the global internet (Carr 2016, 118–120; Powers and Jablonski 2015, 14–16, 109–110; Jin 2014; Kiss 2013; Fuchs 2010; Hill 2013; McChesney 2014).

This view is deeply problematic, however. For one, it gives far more attention to politics than economics. It also emphasises territorial imperialism at the expense of Harvey's second understanding of imperialism, capitalist imperialism, which he defines as a system of power that aims to allow capital accumulation and "economic power to flow across and through continuous space," and where models of development are emulated and consent is preferred to coercion. Harvey also draws on Giovanni Arrighi to suggest that while power is mainly the preserve of single hegemonic states under territorial imperialism, under capitalist imperialism the emphasis is on "the *accumulation of collective power* [amongst states and capital] as the only solid basis for hegemony within the global system" (Harvey 2003, 37; emphasis added). He also does not view corporate interests as subordinate to state interests or nation-states as the simple handmaidens of capital. This view captures the essence of the global cable systems of the nineteenth and twentieth centuries remarkably well. It is also a better, if incomplete, explanation of the global internet in the twenty-first century than the more one-dimensional views recounted a moment ago.

Communication history should start with the point that capitalism has been a globalising force since its inception, and this motive force has been inextricably tied to advances in communication (Arrighi 1994). As Karl Marx famously observed:

> Capital by its nature drives beyond every spatial barrier. Thus the creation of the physical conditions of exchange—of the means of communication and transport—*the annihilation of space by time*—becomes an extraordinary necessity for it …. [T]he production of cheap means of communication and transport is a condition for production based on capital, and promoted by it for that reason. (Marx 1867/1972, 459)

Imperialism played a crucial role in the development of these cable systems, but modernising economic forces within China, the Ottoman Empire, Persia, and the post-imperial nation-states of South America were also vital sources of demand. Moreover, while rickety telegraph cable networks had been developed in some of the imperial territories of the Caribbean and Southeast Asia in the 1860s and 1870s, they only encircled the continent of Africa a decade later, in the mid-1880s. In other words, the far-flung territories of the British, European, Japanese, and American empires—with the major exception of India—were tied into the world communication system only a decade or more later than the rest of the world. This typically happened only after large state subsidies were granted, mostly to private firms, and occasionally by several governments at once. This was the case, for example, when a subsidiary of the Eastern Telegraph Company laid, owned, and operated the cables to and around Africa after receiving substantial subsidies from Britain, France, Germany, and Portugal (Britain 1902, Appendix E). Private enterprise generally ruled the industry. Even at the height of the new imperialism (1880–1910), less than 20 per cent of cables were state-owned. Even then, however, the areas that they served were still amongst the least connected, worst served places in the world, in contrast to the conditions assumed by the "struggle for control" model of communication outlined earlier.

1.1 Foreshadowing the Future: From Copper Cables to the Global Internet Infrastructure

The massive scale of submarine telegraph cable construction in the late 1860s and the first half of the next decade, the product of a speculative financial bubble that burst in 1873, was not matched again until the turn of the twenty-first century, when a speculative flood of investment led to a 100-fold rise in telecommunications capacity before the dotcom bubble crashed in 2000–2001—a point we return to below (FCC 1999, 5). Just as submarine telegraphs were a general-purpose technology with pervasive

effects, the critical communications infrastructure underpinning the then-new world order, today fibre optic cables play a similar role with respect to the global internet. Then as now, undersea cables were regulated by governments in terms of landing licences. The monopoly landing rights that they typically gave the submarine telegraph companies in the early years of development varied considerably, as did the terms of service they demanded with respect to privileges given to local officials, interconnection with local telegraphs, as well as their need to monitor (surveillance) and block (censorship) messages perceived as threats to public morality or national security. These landing licences typically reflected the strength of the state that negotiated them. The stronger the state, the less likely it was to grant monopoly rights to a company, as was the case in Britain and the United States. The weaker the state, the longer the right to a monopoly, the more restrictive the terms-of-service obligations, and the less likely companies were to cooperate in ways other than those that advanced their business interests. In the United States, by convention, the president had the authority to grant or withhold cable landing licences before 1921, after which that authority was formalised with the passage of the *Cable Landing Licenses Act*—a measure that ensured that the use of such powers took place at the highest level of authority *and* outside Congressional oversight and, thus, steeped in secrecy—as it has remained until this day (United States 1921).

The basic geography of the internet follows that of its telegraph predecessor. Indeed, the routes laid down in the nineteenth century are still the dominant routes now, even if under very changed conditions. While the geography remains similar, the capacity of the world's information infrastructure has exploded. At the end of 2017, the global internet's backbone consisted of around 370 international submarine cables. Currently, nearly 99 per cent of all international internet traffic travels through these cables, and a single fibre pair in a cable (which typically have a dozen or so fibre pairs) can carry as much traffic as all the geosynchronous satellites orbiting the planet (Telegeography 2018c; OECD 2014, 12). Today, more than an exabyte of data transits the internet every day, which is the equivalent of 212 million DVDs or the entire contents of the British Library or U.S. Library of Congress several hundred times over (van der Berg 2012). Given all this, these international cables really are the main arteries of the internet.

While a speculative mania in the early 1870s led to the collapse of the financial bubble within a few years, it still left behind the copper cables

that really did serve the world for decades to come. So, too, in recent times did the global boom in submarine cable construction between 1998 and 2003 leave behind 16 new trans-Atlantic cables that have served as the arteries of commerce and communication between North America and Europe ever since. Cables were laid elsewhere, of course, but it was in the North Atlantic that most of the significant activity took place. During the dotcom era of the last three years of the twentieth century alone, the carrying capacity of the trans-Atlantic cables multiplied 100-fold (FCC 1999; Terabit 2018, 21). Similar patterns took place within countries as well: Some $90 billion of new investment was injected into the internet backbone and 36,000 kilometres of optical fibre laid in the United States alone at the height of the boom (Troainovski 2012).[2] The speed and magnitude of the boom—and bust—of the dotcom bubble can also be seen in the spike of capital investment in submarine cables from 1998 to 2001, and the plunge in investment thereafter (Fig. 1).

Of the $7 trillion lost when the market crashed between 2000 and 2002, $2 trillion could be laid at the feet of telecoms companies (Starr 2002). Repeating the events of more than a century earlier, when many of the new operators collapsed, their assets were acquired cheaply by

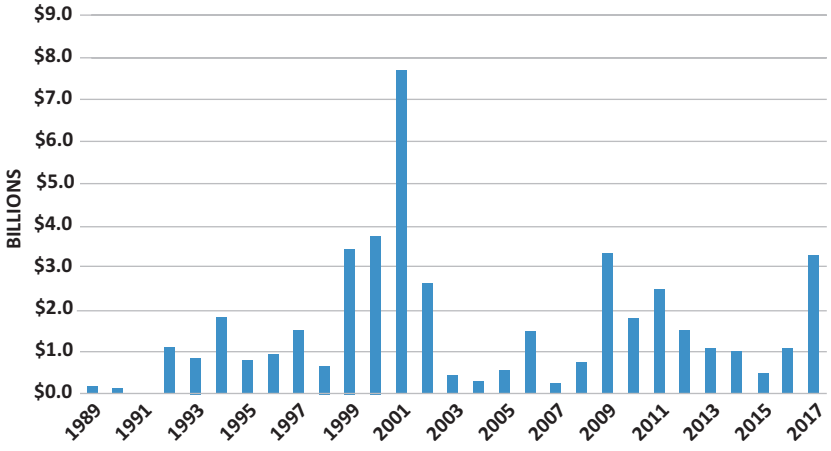

Fig. 1 Construction costs of submarine cables, 1989–2017. Source: Terabit (2018), Submarine Telecoms Industry Report, Figure 25

[2] All dollar values are in USD.

well-established telecoms carriers while a new class of more resilient rivals such as Level 3, Cogent, XO, Reliant, Zayo, and Content Distribution Networks (CDNs) also emerged. As a result, bandwidth was "dumped" onto the market and prices plummeted.

So much new fibre optic cable was laid at the time that 90 per cent or more of the capacity across the Atlantic was never "lit up" during the next decade. Instead, cable capacity was stockpiled as "dark fibre" that was not outfitted with the electronics needed to transmit traffic to avoid compounding the glut of bandwidth already in the market. No new trans-Atlantic cables, consequently, were laid for a decade and a half after the "Great Crash" (Telegeography 2016). As result, during this time, "the transatlantic market [was] served exclusively by the cable systems that were deployed between 1999 and 2003" (Terabit 2018, 21–22).

This reliance for more than a decade and a half on cables laid during the dotcom era has changed in the past two years with the construction of three new trans-Atlantic cables—two in the North (MAREA and Greenland) and another in the South (South Atlantic Inter Link or SAIL)—as well as a new cable between North and South America (Monet), and two smaller links between cities in the latter region (the Tannat and Junior Cables), with more currently on the drawing board. Indeed, there is once again talk of a renewed boom in submarine cable building in the region, and in many areas of the world—as the following paragraphs discuss.[3]

2 The Internet Outgrows Its U.S. Cradle

The real resurgence of capital investment in new submarine cables since 2008, however, initially took hold in the Asia-Pacific region before spreading to Africa, South America, and the Middle East in recent years. Total worldwide investment between 2008 and 2017 was an estimated $18 billion. Most of the investment involved the BRICS ($10.7 billion, or 60 per cent), largely due to six ambitious Asia-Pacific region cable proj-

[3] The MAREA cable is jointly owned by Telefonica, Facebook and Microsoft; the Greenland Cable by a resurrected Canadian company from the dotcom era, Hibernia Networks; the Monet Cable is jointly owned by Angola cables, Antel Uruguay, Algar Telecom and Google; the Tannat Cable by Google and Antel Uruguay; the Junior cable by Google; while the SAIL cable is jointly owned by Cameroon Tel and China Unicom, and links the west coast of Africa to the east coast of South America (Telegeography 2018c). Dates cited are for when the cables began service, unless stated otherwise, and from this source.

ects: UNITY (2010); the South-East Asia Japan Cable (2013), the Asia Pacific Gateway (2016), FASTER (2016), the Pacific Cable Light Network (2018), and the New Cross Pacific Cable (2018).

As in the past, Africa and some of the most downtrodden economies of the world have been the last to be tied into the world's internet infrastructure and have been among the least competitive, worst served, most expensive places for internet bandwidth on the planet. This too, however, is changing fast. In fact, a quarter of the investment since 2008 ($3.8 billion) has been in new cables to and around sub-Saharan Africa, with at least four new cables laid along the west coast and four along the east. In the process, South Africa, Nigeria, Kenya, and Ghana have emerged as internet hubs for the region and these links, in turn, are driving fibre optic cables to be built more widely within more African cities than has ever been the case, even into townships outside the big cities that have been badly underserved historically. As of late 2018, there were eight new cables linking India together with the Middle East and Europe in various stages of development ($2.9 billion) as well (Song 2018; Telegeography 2018c; Weller and Woodcock 2012; OECD 2014).

Government ownership and development bank financing of fibre optic submarine cables remains modest, but is on the upswing, rising from just 1 per cent of cable investment in the early twenty-first century to 11 times that amount in 2017. Now, however, it is not the "new imperialists" making the capital investments, but nation-states in the Global South, especially in Asia, sometimes in tandem with international development banks, but typically with capital from national and regional telecoms carriers, many of which are government-owned, but also with sizeable investment and ownership stakes from Google, Facebook, and Microsoft in several instances (Telegeography 2018c; Terabit 2016, 14–22; Terabit 2018, 28–31). This can be seen by examining the key players in cable system ownership, content delivery networks and Internet Exchange Points.

2.1 Changing Players and the Rise of the Post-American Internet

The number and type of submarine cable system owners and operators has expanded and diversified greatly over time. As mentioned earlier, by the end of 2017, there were 370 international undersea cables in operation. Roughly a quarter of these cables (85 in total) are owned and operated by the consortia of legacy national telecoms carriers and about that many

again are owned individually by these carriers. Over the last two decades, however, a new roster of competitors and Content Distribution Networks (CDNs) such as Amazon Web Services, Akamai, Level 3, and China Cache have emerged as significant rivals to the legacy telecoms operators. Google, Facebook, Amazon, and Microsoft have also recently entered the fray to become significant owners and operators of cables systems, sometimes by working in tandem with one or another of the aforementioned carrier groups but at other times on their own and in direct competition with the legacy telecoms-operators consortia, the new competitors and CDN operators *en masse*. The upshot overall, however, is that geographically, structurally, in terms of the composition of the consortia that own and operate the overwhelming majority of undersea cables, and in terms of national origins, the world's internet infrastructure has become vastly more complex, heterogeneous and "post-American" than ever.

Amongst the group of new competitors, three companies stand apart and typify the trends being analysed here: the U.S.-based Level 3 and two others with headquarters in Mumbai, India—Global Cloud Xchange and Tata (Telegeography 2018c). There are several other second-tier companies of this type, with several that are non-U.S.-centric as well. They include Cogent (U.S.), PCCW (Hong Kong), XO (U.S.), Global Transit (Malaysia) and Hurricane Electric (U.S.) (Zmijewski 2014). A second type of operator consists of CDNs. They are specialised niche players that carry internet traffic for large corporate and government users, media, and entertainment companies such as Netflix, Google, Amazon, Facebook, Baidu, and so on. Seven CDN operators stand out amongst the rest: Amazon, Akamai, Level 3, Edgecast (Verizon),[4] China Cache, Limelight, and Highwinds (Rayburn 2015). The first four entities on the list control roughly three-quarters of all revenue in this niche area and are U.S.-based, as are the latter two. The only non-U.S. CDN operator among the group is China Cache. While this would seem to cut against the grain of the argument of this chapter, it must be kept in mind that the CDNs compete in a wider market of much bigger players that include the incumbent carriers, competitive bandwidth wholesalers and, increasingly, the global internet giants such as Google, Facebook, Amazon and Microsoft, who are building their own networks, sometimes single-handedly but often by joining other consortia to do so as well. Overall, the consortia approach,

[4] Verizon is not a new company but entered the CDN business after acquiring Edgecast in 2013.

with its deep historical roots in the cartels of the nineteenth and twentieth centuries, continues to be a mainstay of the universe, but they now consist of a much more heterogeneous mix of private and state actors. This complex reality helps to explain why the former national monopoly carriers see international markets as being highly competitive, but given the interplay of national, state, and corporate interests in most consortia, it is also why we should be cautious about being too quick to pin a national identity on these actors—at least the corporate ones—as if private capital and the complex technological systems they command are merely "tools of empire" and handmaidens of their respective governments.

Beyond the undersea cables, there are approximately 2000 Internet Exchange Points (IXPs) around the world. They are essential elements of the internet infrastructure where traffic is handed off between all the networks that make up the internet system. Indeed, 99 per cent of internet traffic is handled by peering arrangements at IXPs and occurs without any money changing hands or a formal contract (van der Berg 2012; Weller and Woodcock 2012). The biggest IXPs are in New York, London, Amsterdam, Frankfurt, Seattle, Chicago, Moscow, Sao Paulo, Tokyo and Hong Kong. These are the "switching centres," where international internet backbone providers, internet content companies, and the CDNs interconnect with one another, and local internet service providers (ISPs), media and entertainment companies, and other big "content service" providers. In developed markets, internet companies such as Google, Baidu, Facebook, Netflix, Youku, and Yandex use these IXPs to interconnect with local ISPs such as Deutsche Telekom in Germany, BT or Virgin Media in the United Kingdom or Comcast in the United States to gain last-mile access to their customers—and vice versa back up the chain.

Crucially, IXPs help to establish accessible, affordable, fast, and secure internet service. Where they do not exist or are rare, as in Africa, or run poorly, as in India, the cost of bandwidth is astronomically more expensive. This is a major factor that helps to explain why internet service is so expensive in areas of the world that can least afford it. It is also why developing countries are being encouraged to make IXPs a cornerstone of their economic development and telecoms policy work (Song 2018; Telegeography 2018c; van der Berg 2012; Weller and Woodcock 2012).

In addition to the undersea cables and IXPs underpinning the internet, there are also thousands of local, national, and regional networks of a wide variety of kinds and sizes that interconnect with one another to form "the internet." Every network that connects to the internet is given a num-

ber—autonomous systems number (ASN)—and you can count the number of such networks by the number of ASNs that have been assigned. In 1997, there were 3,212 ASNs that comprised the entire internet; by early this year, that number had soared to 84,414 (OECD 2015; Maigron 2018; Hawkinson and Bates 1996). Crucially, the geography of where these networks are located has changed dramatically over the past two decades. Thus, in 1997, for instance, 56 per cent of ASNs were located in the United States. Adding Europe and Japan raised the total share of these core regions of the global economy at the time to 79 per cent, while the BRICS accounted for just 5 per cent. A decade later, the U.S. share of ASNs had dropped to 39 per cent while that of the transnational core countries fell to two-thirds. The BRICS share, in contrast, was double what it had been ten years earlier. Fast forward to early 2018, and the trend towards a post-American internet continues. By this time, the United States' share of ASNs had continued to slide to 31 per cent, and the "transnational core" countries had fallen to 57 per cent. Taken on its own, in contrast, the EU's share rose significantly to 25 per cent, while the BRICS' share had soared to 18 per cent—almost four times what it had been, despite under-representing the true scope of the changes, given that the number of ASNs in China is not well-captured because they are hidden behind the country's "great firewall" (Fig. 2).

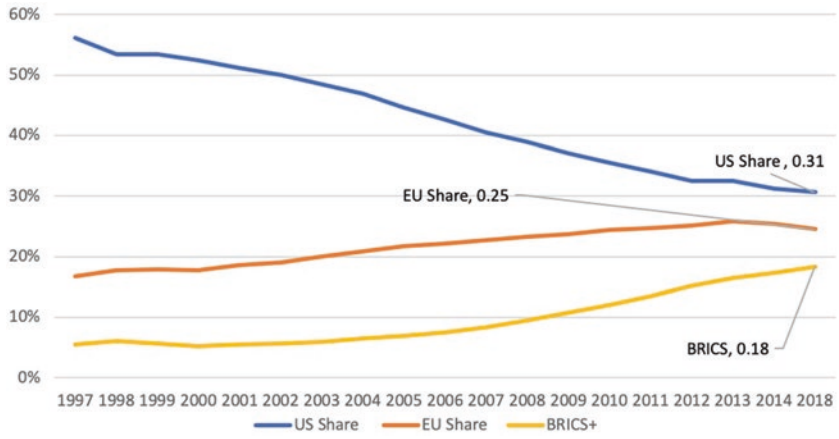

Fig. 2 Country and region share of autonomous system numbers, 1997–2018. Sources: OECD 2015, Table 2.44; Maigron 2018

Who uses the internet from where and for what purposes has also changed dramatically over time. Fibre optic cables, and the mobile wireless and internet system that they gird, are no longer the "rich man's post" as during the days of international telegraphy and telephony. Indeed, the cost of internet transit has plunged in recent years to "about $0.0000008 per minute—or 100,000 times lower than typical voice rates" (van der Berg 2012). As prices have plunged, internet and mobile phone use has exploded. Thus, while the number of people who used the international telegraph could be counted in the thousands in the late nineteenth century, there were already 400 million regular internet users and 800 million mobile wireless subscriptions by the end of the twentieth century (i.e., roughly 5 per cent and 10 per cent of the world population, respectively). Fast forward to 2017, and there were 5 billion unique mobile wireless subscribers and 3.6 billion regular internet users (Broadband Commission 2017, 10; ITU 2018).

Who uses the internet has also shifted decisively to the BRICS countries and the Global South. Whereas two-thirds of internet users lived in the United States in 1996, by 2017 Americans constituted less than 5 per cent of the world's internet users, while China alone now accounts for nearly 20 per cent of the total. In sum, the vast majority of growth in terms of internet and mobile phone use has been in the Global South, and this is changing how the internet is used, is being developed, and the policy responses that will shape its future. None of this should obscure the fact, however, that there is an estimated four billion people, or 52 per cent of the world's population, that still lack internet access, and the gender divide continues to be stubbornly difficult to bridge (Broadband Commission 2017).

Given these developments, it is unsurprising that the United States' share of internet traffic has declined. The United States undoubtedly dominated global internet traffic during the first decade of the commercial internet—which also put it at the nexus of a powerful system of mass internet surveillance—but its position has declined steadily since. In 2004, half of all internet traffic globally flowed through the United States, but by 2017, that number had fallen to less than one-quarter (Telegeography 2018a, b). Figure 3 illustrates the point.

2.2 United States Still Dominates Internet-Based Audiovisual Media and Gaming Applications

The idea of an underlying shift to a post-American internet based on the changes just described should not be overblown, however. Take, for

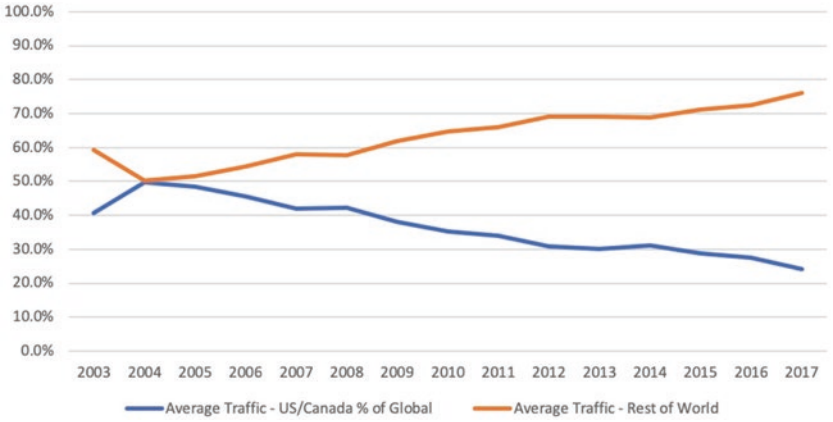

Fig. 3 U.S. share of international internet traffic, 2003–2017. Sources: Telegeography, Global Internet Geography (Figure 8): Global International Internet Traffic, 2013–2017 (Gbps), 2018a; Telegeography, Global Internet Geography (Country Profiles: U.S.), 2018b

example, the fact that while billions of people use the internet for many reasons, the most popular uses are to watch television and movies, listen to music and to play games. Consequently, audio/video-based media and gaming made up nearly three-quarters of internet traffic worldwide in 2016 and are expected to surpass 80 per cent within five years, with U.S. firms leading the way (Cisco n.d.). Indeed, Netflix accounts for a third of all internet traffic. YouTube is the second largest source of traffic on fixed and mobile networks worldwide. Combined, the big five internet giants—Google, Amazon, Facebook, Netflix and Microsoft—currently account for nearly 60 per cent of all "prime-time" internet traffic, a phrasing that deliberately reflects the fact that internet usage swells and peaks at exactly the same time as the classic prime-time television period, that is, 7 pm to 11 pm (Table 1).

2.3 Two Approaches to Building Internet Infrastructure

The idea that the internet has become an entertainment distribution system during "prime-time" is fundamentally influencing the current phase of internet infrastructure development. Such realities are driving, for

Table 1 Prime-time internet traffic composition, North America, 2016

Upstream		Downstream		Aggregate	
BitTorrent	18.37%	Netflix	35.15%	Netflix	32.72%
YouTube	13.13%	YouTube	17.53%	YouTube	17.31%
Netflix	10.33%	Amazon Video	4.26%	HTTP - OTHER	4.14%
SSL - OTHER	8.55%	HTTP - OTHER	4.19%	Amazon Video	3.96%
Google Cloud	6.98%	iTunes	2.91%	SSL - OTHER	3.12%
iCloud	5.98%	Hulu	2.68%	BitTorrent	2.85%
HTTP - OTHER	3.70%	SSL - OTHER	2.53%	iTunes	2.67%
Facebook	3.04%	Xbox One Games Download	2.18%	Hulu	2.47%
FaceTime	2.50%	Facebook	1.89%	Xbox One Games Download	2.15%
Skype	1.75%	BitTorrent	1.73%	Facebook	2.01%
	69.32%		74.33%		72.72%

Source: Sandvine *Global Internet Phenomena*, 2017, 4

instance, the emergence of specialised CDNs and the internet giants' efforts to build undersea cable systems and data centres around the world—sometimes jointly with the legacy telecoms operators; at other times, with the new competitive carriers; and other times, all on their own in stiff competition with both of those groups.

Worldwide, the public internet is also being eclipsed by private internets built, owned and operated by the world's largest internet companies, traditional telecoms carriers and a relatively new class of CDNs and internet bandwidth wholesalers such as Level 3, Tata, Global Cloud Xchange, Cogent, XO, Hurricane Electric, and CDNs. These trends may also be altering these large American internet companies' such as Google, Facebook, and Netflix stance on network neutrality/common carriage and other internet and public policy issues as well, given that once they own their own networks or contract heavily with CDN providers, they rely less on the transit services of either the incumbent or the relatively new generation of competitive carriers. As a result, the internet giants achieve their aims through competition and contracts rather than regulation and public policy. This appears to be the case with Google since 2010, for example, when its support for network neutrality/common carriage wilted relative to what it once was, while Netflix has toned down its support for such measures in recent years as well (Stevenson 2014). In essence, parallel private internets have been developed outside the orbit of the public internet in order to bring the services of Google, Baidu, Facebook, Netflix, Youku, and so forth as close to the doorsteps, desktops, and devices of their users as possible.

The internet giants are generally taking two different approaches—depending on the availability of capacity, costs, and region—to internet infrastructure: one based on direct investment and ownership stakes in fibre optic submarine cables where capacity is low; the other based on obtaining access to bandwidth from carriers and CDN providers *and* building data centres at each end of the cable where capacity is abundant and cheap. Google and Facebook, for instance, are pursuing the first strategy mostly in relation to several new cables across the Pacific and along the Asian coastline from Korea to Thailand, a consequence of the relative scarcity of bandwidth in the Asia-Pacific (see below). In the North Atlantic region, in contrast, rich in "dark fibre" left over from the dotcom crash, capacity is abundant and cheap, and therefore the internet giants have stayed away—until recently—from laying their own cables in favour of buying capacity from either the incumbent carriers, new competitors such as Tata or CDN providers. As the same time, they are also building huge data factories on either side of the Atlantic Ocean that allow them to warehouse the vast stores of data they collect and to bypass the undersea cables as much as possible altogether.

In the last two years, however, this too has begun to change with the announcement of two new northern trans-Atlantic cables. The first of those cables—the MAREA cable between the United States and Europe, with ownership shared between Telefonica (50 per cent), Facebook (25 per cent), and Microsoft (25 per cent)—began operating last year. Google has also built three cable systems during this time between cities in Brazil and Uruguay—Junior and Tannat—with a link to Miami (the Monet cable, which is jointly owned by Google, 33.3 per cent; the Angolan-based Angola Cables, 33.3 per cent; the Uruguay-based Antel, 16.7 per cent; and the Brazil-based Algar, 16.7 per cent). It is also building a major cable system to link Los Angeles with Chile on the Pacific coast of the Americas—the Marie Curie cable system. The idea that key internet infrastructure is shifting towards the Global South can also be seen in the plans by Telefonica to bring its Brazil-USA (BRUSA) cable to life in 2018, while yet another, the Seabras cable (Seaborn Networks), is slated for development in the next year (Telegeography 2018c). In short, as demand begins to catch up to capacity, and shift from the west to the east and the north to the south, and from the "public internet" to "private internets," new investment is taking place. Obviously, the very large place that Google, in particular, has carved out for itself in many of these projects certainly requires that any claims about a wholesale shift to a "post-American internet" come with caveats.

At their core, however, most of these projects are multinational in character and criss-cross private and public lines, or between "states and markets" with relative ease. The Google-led Monet project and the MAREA joint venture between Telefonica, Facebook and Microsoft both exemplify the point.

Conditions in the Asia-Pacific region have been somewhat different because bandwidth there has been scarcer for a longer period of time. Therefore, the need for new cables has been far greater. This is reflected in the fact that the four biggest undersea optical fibre cable projects of the past decade have been in the Asia-Pacific region: UNITY (2010), the South-East Asia Japan Cable (SJC) (2013), the Asia Pacific Gateway (2016), and FASTER (2016). Two more major projects are also on the drawing board and slated to begin service soon: the New Cross Pacific Cable (NCP) and the Pacific Light Cable Network (PLCN). Once again, Google and Facebook loom large in all of these projects, reflecting their extraordinary growth in the Asia-Pacific region and their own interest in surmounting the lack of bandwidth that has characterised the region.

In many ways, these developments represent the physical emergence of a federated internet wherein many different actors—that is, legacy telecoms carriers, new competitors, mobile wireless operators, government-owned carriers and the global internet giants—coalesce across national lines to build the infrastructure of the internet. The physical existence of a federated internet is nicely illustrated by some of Google's activities in Asia. Google, for example, played a key role in such ventures in 2008 when it acquired a substantial ownership stake in the $300 million UNITY Cable, a cable that runs from California to Japan. The lead role in the UNITY consortia, however, is not played by Google, but Vodafone (40 per cent), followed by the regions' major national carriers, many of which are state-owned. Beyond Vodafone, however, how much of this venture each party owns is not known (Telegeography 2018c; Chowdhry 2014). In 2011, Google acquired an ownership stake in the South-East Asia Japan Cable, a $400 million system of spurs that run from the trans-Pacific cables to Brunei, China, Hong Kong, Japan, the Philippines, and Singapore, with a second phase of the project slated to extend the network to Thailand (Telegeography 2018c). The make-up of the ownership group behind this cable is larger than in the UNITY project but still includes many of the same players: China Telecom, China Mobile, Singtel, Singtel Optus, Chunghwa Telecom, KDDI, Google, Globe Telecom, the Telephone Organisation of Thailand, Telkom Indonesia, Brunei International

Gateway, and Airtel. Again, we have little insight into how much of this venture is owned by Google and the others involved, but state-owned telecoms operators appear to dominate the consortia, given the role of China's two biggest government-owned telecoms operators (China Telecom and China Mobile), Singtel and its affiliate Singtel Optus, and incumbent national carriers from Taiwan, Brunei, and Thailand. KDDI, Globe Telecom and Airtel are from the relatively new category of competitive telecoms and/or mobile network operators from Japan, the Philippines, and India, respectively, with ownership stakes in this system. While Google stands out in this area, both Facebook and Microsoft are engaged in a number of similar ventures.

The surge in internet-infrastructure construction activity is not confined to Asia. There has also been an explosion of bandwidth and connectivity to the coastal perimeter of Africa, with at least eight new cables laid since 2010. The recent push for new IXPs on the continent is also being met (Song 2018). Both developments have also helped to overcome the historically entrenched imperial geography of communications whereby messages first had to traverse the metropoles of empire (e.g. London, Paris) en route to other places within Africa or to locations wholly unrelated to this imperial geography. They have also contributed to a rapid drop in prices, thereby further adding to the "mobile wireless" revolution which has seen the number of mobile phone subscribers soar from 12 per 100 people to 78 per 100 between 2005 and 2017 in Africa (ITU 2018). Such developments have also underpinned the emergence of a unique kind of mobile internet on the continent, with unique applications and services—most notably, m-banking (mobile banking) taking off in Africa in ways that resemble trends in India, Southeast Asia, China, and some other developing countries, but with only poor analogues in Europe and North America (Broadband Commission 2017).

These changes are also resulting in a new generation of African-based companies such as Liquid Telecom that are not only connecting the continent with the rest of the world but also laying fibre to the doorstep within cities and beyond. Of course, this is being done first in the affluent gated communities of major cities, but it is also taking place in some of the townships that have previously been neglected. Companies such as Liquid Telecom are also using the internet infrastructure they have built as a base from which to start pay-television services that are challenging the previously insurmountable dominance of sub-Saharan Africa's largest media conglomerate, Napster, and especially its pay-TV service, MultiChoice

(Kwese/Econet 2017). In short, the massive growth in bandwidth throughout the continent and between it and the rest of the world is not only increasing access to the internet but fostering changes across the media, society and economy. At the same time, however, keen observers worry that despite these changes, it is unlikely that more than half of Africans will benefit from these developments unless fundamental changes in politics, policy, justice, and how these issues are thought about take place (Song 2018).

2.4 Emerging Trends

Two major points stand out from this extensive overview. First, U.S. companies, most prominently Google but also firms such as Facebook and Microsoft, have carved out a large place for themselves in key internet infrastructure ownership initiatives. This is a relatively new trend and one that should be watched in the years ahead.

Second, while some of the ownership details are incomplete (such details are a tightly guarded secret in the industry), U.S.-based companies' control over core elements of the global internet—undersea cables, IXPs, internet traffic, and internet users—has steadily slipped over the past two decades. In general, the centre of gravity for the internet has shifted away from the United States towards the Asia-Pacific region and the BRICS countries, but also to the Global South and the European Union. Chinese interests have emerged as key players not just within the Asia-Pacific region but in many areas around the world. Two of its big three telecoms operators—China Telecom and China Mobile—are involved in several key regional projects, while the country's third major operator, China Unicom, has interests in several other key ventures (e.g. the Asia Pacific Gateway, New Cross Pacific, South Atlantic Inter Link (SAIL), amongst others). The big three Chinese telecoms operators cut the most prominent figures in the Asia-Pacific region, but their interests also extend beyond Asia to include cable links to India and the Arab world, from there to Europe, and from Africa to South America. That the Pacific Light Cable Network is also majority-owned by a Chinese real estate and investment firm bolsters the assessment that China is a dominant force in the region—and increasingly, across the world.

Neither is China the only player in this area. National telecoms operators from Japan—the incumbent carrier NTT and the competitive telecoms and internet operators, KDDI and Softbank—have sizeable ownership

stakes in several Asia-Pacific cable systems built over the last decade, as do government-owned carriers from Taiwan, South Korea, Thailand, Indonesia, Brunei, and Vietnam, and national telecoms firms from Malaysia, the Philippines and India. Their emergence is an indicator of the growing clout of a wider range of countries in the region and the rise of competition within them, and the fact that whatever divide one might imagine between "states and markets" when it comes to who owns the world's internet infrastructure, especially in this region of the world, there is far more harmony of interests than often assumed. As a matter of fact, state-owned enterprises routinely sit cheek-by-jowl with historical telecoms monopolies from the private sector, the roster of relatively new competitive operators (e.g. Tata and Level 3) and, now, the internet giants such as Google, Facebook, Amazon and Microsoft. In short, we can see the emergence of a federated internet in which entities and interests cut across national lines and the boundaries between states and markets are represented in microcosm in the many consortia that have built, own, and operate core elements of the global internet infrastructure. When these arrangements do not hold, however, the internet giants, especially Google, are also building and operating their own systems to meet their soaring demand and to bring their services as close to end users as possible, for example: the Pacific Light Cable Network and the Tannat and Junior cables.

A preliminary view based on the available information is that the U.S. internet companies are important but subordinate players within consortia that are dominated by a mix of private- and state-owned national carriers as well as some relatively new competitors. Keen to wrest control of core elements of the internet infrastructure that they perceive to have been excessively dominated by U.S. interests in the past, Asian governments and private investors have also joined forces to change things in their favour. In terms of the geopolitical economy of the internet, there is both a shift towards the Asia-Pacific region *and* an increased role for national governments. A similar phenomenon extends beyond Asia, however, insofar that state and development bank investment, while miniscule at just 1 per cent between 1987 and 2010, has soared to 11 per cent since then (Terabit 2018, 20–28). These changes in ownership and control of internet infrastructure point to much bigger geopolitical and economic changes afoot that are fundamentally reshaping how the internet will develop in the decades ahead, much along the lines that Ronald Deibert has suggested as the next billion internet users—mostly from the Global South—come online (Deibert 2013, 101).

3 From a Universal Dream to the Federated Internet?

While the preceding discussion suggests a world in which the primary competition is between what Strange would call the market and state authority, it is in Edward Snowden's disclosures of mass internet surveillance by the National Security Agency and its Five Eyes partners (i.e. the United States, Australia, Britain, Canada, and New Zealand) and European intelligence services (e.g. Germany, France, Spain and Sweden) that we can see the other tension in this story—namely, that the stature of U.S. structural power in the geopolitical economy of the internet is shrinking (European Parliament 2014). The extent of state surveillance revealed by Snowden, in fact, reveals not so much U.S. hegemony, but rather, that the erosion of the U.S.-centric model of the internet has, in essence, required the U.S. government to work in league with others to carry out its mass internet surveillance programmes. Although the United States and key American internet companies are still in command with respect to some core elements of the internet such as operating systems, internet content, social networks, and search engines, it is complex global alliances and transactions that actually underpin the global internet infrastructure.

These developments indicate an emerging new phase in internet governance and control. In the first phase, circa the 1990s, technical experts and organisations such as the Internet Engineering Task Force played a large role, while the state sat relatively passively on the sidelines. In the second phase, circa the early to mid-2000s, commercial forces surged to the fore, while global internet governance revolved around ICANN and the multi-stakeholder model. More recently, the revelations of mass internet surveillance by many states, and ongoing disputes over the multi-stakeholder/"internet freedom" agenda versus the national sovereignty, multilateral model (which would have the ITU and United Nations system play a larger role in internet governance) all indicate that significant changes are afoot where the relationship between states and markets is now in a heightened state of flux, with a wide variety of new actors on all sides assuming a more prominent role than the past (Schackelford et al. 2015; Powers and Jablonski 2015).

As the locus of the material infrastructure of the internet tilts away from the United States and towards other countries, it stands to reason that they will gain more influence over the policies and practices that shape it.

The emergence of a federated internet therefore has the potential to reshape the internet as we currently know it, with significant consequences for the currently dominant multi-stakeholder model of internet governance. This form of governance, itself an outcome of U.S. internet hegemony (Carr 2016; Powers and Jablonski 2015), is supported by many commercial interests, technical experts, and non-government organisations as well as the United States and Western capitalist democracies. It is pitted, however, against a more state-centred, multilateral model promoted by those who are critical of the unaccountable power of business interests as well as countries such as India, China, Russia and Brazil which—each in their own way—seek to counter what they see as the United States' and Western capitalist countries' dominance of internet governance.

An even fuller response in terms of this "return of the state" idea can also be seen in the efforts being taken by some illiberal countries to build semi-autonomous, national web 3.0 spaces based on the following: (1) systematic filtering and blocking of certain kinds of internet content and websites; (2) fostering national champions (Alibaba, Baidu, and Tencent in China and Yandex and Vkontakte in Russia); and (3) turning to large internet-media-communication campaigns (propaganda and disinformation) to shape national and foreign information spaces (Deibert and Rohozinski 2010, Chap. 2; Noam 2013; Powers and Jablonski 2015). Russia and China are also trying to add international legal norms steeped in nineteenth-century views of state security that would further entrench the semi-autonomous, national web 3.0 model in a multilateral approach to international internet governance. The U.S. declaration a decade and a half ago that cyberspace is the fifth frontier of war (in addition to land, sea, air, and space) has not helped in the least in this regard (United States Department of Defense 2003).

It is also of interest that just as these structural possibilities open up for a significant remaking of the rules of engagement with respect to global internet governance, the United States has essentially walked away from its role as a decisive player in these affairs with the election and subsequent 18 months of the Trump Administration's nativist inclinations and actions. In other words, the mantle in such matters has passed from the United States to China, the EU, and other countries that are more inclined towards multilateral institutional arrangements, rather than the hegemony by proxy implicit in multi-stakeholder governance (Powers and Jablonski 2015). This result, in and of itself, is not necessarily a negative outcome.

More to the point, the logical endpoint of such trends would seem to take us to Noam's concept of a federated internet, possibly structured by multilateral agreements through established entities such as the ITU.

4 Conclusion

In seeking to understand the exercise of power, Susan Strange advocated focusing on structural power—that is, the ability to set the context within which other actors operate—and the balance between state and non-state/market actors. An examination of both issues raises questions about hegemony, and who will win and lose from a particular set of rules. In this case, by examining the development of, first, submarine cable telegraph networks, and, later, internet infrastructure, we can gain insights into the question of the extent of U.S. hegemony in this area and, critically, the scope and direction of changes over time.

The idea that the world was being remade in the image of the U.S. model of economic and technological globalisation has not panned out. Instead, like the world economy overall, the geography of the internet is tilting away from the United States and towards Europe, the BRICS, and the "rest-of-the-world" (Arrighi 1994; Desai 2013). The U.S. internet giants do dominate the "code" and "content layers" of the internet: that is, operating systems (iOS, Windows, Android), search (Google), social media (Facebook), online retailing (Amazon), and over-the-top TV services (Netflix), although in some countries, they hardly figure at all: China, Russia, Korea and Japan. The United States, however, does *not* rule the "guts and the gears"—the hardware, the material infrastructure—of the internet. These core components of the internet are becoming more plentiful outside of, and less dependent on, the United States.

Google is involved in three of the four major undersea cable projects in the Asia-Pacific region that are already up and running, and two more that will be pressed into action in short order. Facebook is also a partner with Google and a Chinese investment firm in the Pacific Light Cable Network currently in the works. Microsoft has joined the fray as well. Based on what we know, the U.S. internet giants' stakes are not dominant in any of these new ventures, however. Instead, a mixture of telecoms carriers, governments, competitive telecom and mobile network operators, and investment funds from the region loom large. The outsized role of China stands out in each case, with China Mobile, China Telecoms and China Unicom having ownership interests in five of the region's six major, recent cable

projects. The fact that there were no new north Atlantic cables laid after 2003 until two recent initiatives—the MAREA and Hibernia cable projects, respectively—also illustrates the point about how the global internet's centre of gravity is shifting to the Asia-Pacific region. The fact that much of the trans-Atlantic capacity that does exist remains to be unlit dark fibre also strikes one as an effort to hold back the extraordinary carrying capacity that already exists in the name of profit over access to affordable communications.

Lastly, parallel private internets are being built by bandwidth wholesalers (Level 3, XO, Cogent, etc.), CDNs (Amazon, Akamai, Level 3, China Cache, etc.), and others to serve the needs of the internet giants and voracious appetites of those they serve. The private internets that are being laid on top of the public internet are meant to bring the services of Google, Baidu, Facebook, Netflix, Youku, and so forth as close to the doorsteps, desktops, and devices of these services' users as possible. By 2014, these private internets were carrying more internet traffic than the public internet in the Euro-American zone, with similar results expected to take place in Asia and the rest of the world in the next few years. The internet is not only fragmenting along geopolitical and regional lines, in other words, but between public and private internets as well.

In sum, there is no longer a single, universal internet—if there ever was—but rather, a multitude of internets. The centripetal forces nudging things in this direction are also fortifying the push for national internets in China, Russia, and Iran as well, amongst others. In this light, perhaps we are at another critical juncture, equivalent to the "big bangs" of the late twentieth century that brought about the kinds of regulated telecoms-internet competition that we have seen for the last 25 years, or similar to the consolidation of the "industrial communications infrastructure" in the late nineteenth and early twentieth centuries. The question that hangs in the balance now is whether we will see the triumph of the "federated internet," as Noam (2013) suggests, or redoubled efforts to build on the two-decade-old dream of a universal, worldwide internet based on a common commercial model and the cultural values of liberal democracy. While the hegemonic vision of a universal, liberal internet may still prevail—history is always in motion—the material evidence suggests its displacement by a federated internet is not an unrealistic prospect.

References

Arrighi, Giovanni. 1994. *The Long Twentieth Century: Money, Power and the Origins of Our Time*. London: Verso.

Broadband Commission. 2017. *The State of Broadband 2017*. Paris: ITU and UNESCO.

Carr, Madelaine. 2016. *US Power and the Internet in International Relations*. London: Palgrave Macmillan.

Chowdhry, Amit. 2014. Google Invests in $300 Million Underwater Internet Cable System to Japan. *Fortune*, August 12.

Cisco. n.d. Visual Networking Index. *Cisco*. Accessed April 15, 2018. http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html.

Deibert, Ronald. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland Stewart.

Deibert, Ronald, and Rafal Rohozinski. 2010. Control and Subversion in Russian Cyberspace. In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 15–34. Cambridge: MIT Press.

Desai, Radhika. 2013. *Geopolitical Economy: After U.S. Hegemony, Globalization and Empire*. London: Pluto Press.

European Parliament. 2014. *Draft Report on the U.S. NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on E.U. Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*. Accessed December 12, 2016. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/moraes_101470_/moraes_1014703_en.pdf.

Fuchs, Christian. 2010. New Imperialism: Information and Media Imperialism? *Global Media and Communication* 6 (1): 33–60.

Great Britain. 1902. *Second Report of the Interdepartmental Committee on Cable Communications*, Cmd 1056. London: Darlington and Sons.

Harvey, David. 2003. *The New Imperialism*. London: Oxford.

Hawkinson, John, and Tony Bates. 1996. Guidelines for Creating, Selection and Registration of an Autonomous System (AS). Request for Comments 1930. *Internet Engineering Task Force*, March 1996. Accessed December 28, 2018. https://www.ietf.org/rfc/rfc1930.txt.

Headrick, Daniel. 1991. *The Invisible Weapon*. London: Oxford.

Hill, Richard. 2013. *The New International Telecommunications Regulations and the Internet*. Zurich: Schulthess.

International Telecommunications Union. 2018. *World Telecommunications Indicators Database*. Geneva, Switzerland: ITU. Accessed August 23, 2018.

Jin, Dal. 2014. *Platform Imperialism*. New York: Routledge.

Kiss, Jemima. 2013. NSA Furore Has Roots in U.S. Internet Imperialism. *The Guardian*, November 13. http://www.theguardian.com/technology/2013/nov/01/nsa-furore-roots-us-internet-imperialism.

Kwese/Econet. 2017. *Submission by Econet Media Limited on the Authority's Discussion Document: Inquiry into Subscription Television Broadcasting Services.* Johannesburg: Independent Communications Authority of South Africa. Accessed December 28, 2018. https://www.icasa.org.za/uploads/files/Econet-MediaKwes%C3%A9-Submission-on-Discussion-Document-Inquiry-into-Subscription-TV-Broadcasting-Services.pdf.

Lee, Kelley. 1996. *Global Telecommunications Regulation*. London: Cassell/Frances.

Maigron, Patrick. 2018 *Regional Internet Registries Statistics*. Accessed August 23, 2018. https://www-public.tem-tsp.eu/~maigron/RIR_Stats/index.html.

Marx, Karl. 1972. Capital: Volume One. A Critical Analysis of Capitalist Production (Orig. 1867). Reprinted in *The Marx-Engels Reader*, ed. Robert Tucker, 294–361. London: W. W. Norton & Co.

McChesney, Robert. 2014. *Digital Disconnect*. New York: New Press.

Noam, Eli. 2013. *Towards the Federated Internet If One Internet Has Been Good, Multiple Internets Will Be Even Better*. New York: Columbia University. Copy of Article on File with This Chapter's Author.

OECD. 2014. *International Cables, Gateways, Backhaul and International Exchange Points*. Paris: OECD. Accessed December 12, 2016. https://doi.org/10.1787/5jz8m9jf3wkl-en.

———. 2015. *Digital Economy Outlook*. Paris: OECD. Accessed December 12, 2016. https://doi.org/10.1787/9789264232440-en.

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

Rayburn, Dan. 2015. The State of the CDN Market. *Content Delivery Summit* (blog). Accessed December 28, 2018. https://www.streamingmediablog.com/wp-content/uploads/2015/08/2015CDNSummit-Rayburn-Pricing.pdf.

Sandvine. 2017. *Global Internet Phenomena: Latin America and North America*. Toronto: Sandvine. Accessed August 23, 2018. https://www.sandvine.com/hubfs/downloads/archive/2016-global-internet-phenomena-report-latin-america-and-north-america.pdf.

Schackelford, Scott, Enrique Oti, Jaclyn Kerr, Elaine Korzak, and Andreas Kuehn. 2015. Spotlight on Cyber V: Back to the Future of Internet Governance? *Georgetown Journal of International Affair*. Accessed December 12, 2016. http://journal.georgetown.edu/back-to-the-future-of-internet-governance/.

Song, Steve. 2018. Africa's Telecom Infrastructure in 2017. *Many Possibilities*, January 10. https://manypossibilities.net/2018/01/africa-telecoms-infrastructure-in-2017/.

Starr, Paul. 2002. The Great Telecom Implosion. *The American Prospect*, August 19. https://prospect.org/article/great-telecom-implosion.

Stevenson, John H. 2014. The Master Switch and the Hyper Giant: Google's Infrastructure and Network Neutrality Strategy in the 2000s. *Telecommunications Policy Research Conference*, Arlington, VA. http://ssrn.com/abstract=2418784.

Strange, Susan. 1994. *States and Markets*. 2nd ed. London: Pinter.

Telegeography. 2016. *Global Broadband Research Service, Executive Summary*.

———. 2018a. *Global Internet Geography – Figure 8: International Internet Traffic*, 2013–2017 (Gbps). https://www.telegeography.com/products/global-internet-geography/analysis/capacity-and-traffic-trends/index.html (subscribers only).

———. 2018b. *Global Internet Geography – Country Profiles: U.S.* https://www.telegeography.com/products/global-internet-geography/capacity-and-pricing-data/country-profiles/united-states/index.html (subscribers only).

———. 2018c. *Global Broadband Research Service, Submarine Cable and Carrier Profile Exports* (subscribers only).

Terabit. 2016. *Submarine Telecoms Industry Report* (Issue 5). Cambridge, MA: Terabit. Accessed August 23, 2018. https:/subtelforum.com/Report5/mobile/index.html?doc=D2C63844C07ABF9C60E4BE6591014FCE.

———. 2018. *Submarine Telecoms Industry Report* (Issue 6). Cambridge, MA: Terabit. Accessed August 23, 2018. https://issuu.com/subtelforum/docs/stfindustryreportissue6final.

Troainovski, Anton. 2012. Optical Delusion: Fiber Booms Again, Despite Bust. *Wall Street Journal*, April 3. http://www.wsj.com/articles/SB10001424052702303863404577285260615058538.

United States, 66th Congress, 3rd Session. 1921. *Cable-Landing License Hearings*. Washington, DC: Government Printing Office.

United States Department of Defense. 2003. *Information Operations Roadmap*. Washington, DC: Department of Defence. Accessed December 12, 2016. http://nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

United States, Federal Communications Commission (FCC). 1999. *Cable Landing Licenses*. Washington, DC: FCC.

van der Berg, Rudolf. 2012. Internet Traffic Exchange: 2 Billion Users and It's All Done on a Handshake. *OECD Insights*, October 22. Accessed December 28, 2018. http://oecdinsights.org/2012/10/22/internet-traffic-exchange-2-billion-users-and-its-done-on-a-handshake/.

Weller, Dennis, and Bill Woodcock. 2012. *Internet Exchange: Market Developments and Policy Changes*. Paris: OECD. Accessed December 12, 2016. http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826.

Winseck, Dwayne. 2011. Submarine Telegraphs, Telegraph News, and the Global Financial Crisis of 1873. *Journal of Cultural Economy: Special Issue on Financial Crises* 5 (4): 197–212.

———. 2017. The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy* 7: 228–267.

Winseck, Dwayne, and Robert Pike. 2007. *Communication and Empire: Media Power and Globalization, 1860–1930*. Durham, NC: Duke University Press.

Zmijewski, Earl. 2014. A Baker's Dozen, 2014. *Dyn Research*. Accessed December 12, 2016. http://research.dyn.com/2015/02/bakers-dozen-2014-edition/.

Precarious Ownership of the Internet of Things in the Age of Data

Natasha Tusikov

Farmers might be surprised to find out that the tractor they purchased may not belong to them—at least that is what John Deere claimed in a government policy review to the U.S. government in 2014. The company's argument rests on the claim that tractor buyers do not own the networked software systems that are integral to the operation of modern tractors. Tractors, like many other vehicles, household appliances, and common electronic devices are increasingly no longer just mechanical devices: many depend on software for their functionality. Consumers purchase the hardware, John Deere argues, but that purchase does not encompass the all-important software. Buyers of John Deere products "cannot properly be considered an 'owner' of the vehicle software," the company argued, because a "vehicle owner does not acquire copyrights for software in the vehicle" (Bartholomew 2014, 5).[1] Instead, "the vehicle owner receives an *implied license* for the life of the vehicle to operate the vehicle"

[1] John Deere made this statement in its 2014 contribution to the U.S. Copyright Office, which was holding hearings into whether the copyright law should be amended to allow the diagnosis, repair, or modification to vehicle software (see Bartholomew 2014).

N. Tusikov (✉)
York University, Toronto, ON, Canada
e-mail: ntusikov@yorku.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_6

(Bartholomew 2014, 6, emphasis added). In other words, "It's John Deere's tractor, folks. You're just driving it" (Wiens 2015).

John Deere is not alone in its claim of extended control over the products it sells. Companies including General Motors, Nest, the Google company that supplies smart home products, and the wearable firm Fitbit express similar sentiments with respect to the physical products they produce for sale—vehicles, thermostats, fitness monitors—and which people tend to believe that they straightforwardly own. These companies all produce internet-connected physical goods termed Internet-of-Things (IoT) products or, more colloquially, "smart" products.

At the core of these claims is the embedded software (or series of software systems) within IoT products, which is governed by copyright law, paired with restrictive licensing agreements between manufacturers and users. This software is integral to the products' functionality: if something happens to the software, the goods' functionality will be impaired. Those who control the copyrighted software have the legal authority to set rules governing how the software—and by extension, the product—works and how it can be used or repaired, or even in the most extreme case, whether the product will continue to work. Manufacturers typically prohibit their customers from modifying or repairing their IoT goods if such acts involve altering the products' software, arguing that doing so violates the software's copyright. Thus, evoking copyright law and licensing agreements with their customers, John Deere can control how its tractors can be used or repaired, even after purchase. Control over software enables the companies' control over physical products.

To explain how the control over software became key to governing smart goods, this chapter draws upon an analysis of IoT companies' licensing agreements for their smart goods and the regulatory theory literature of private regimes. It argues that these companies are fundamentally redefining ownership in a way that rebalances it away from purchasers and towards sellers and their economic interests. This shift in how physical goods are governed—and more broadly, the role of privately set rules in this process—highlights the importance of the regulation of knowledge to the wider economy and society. Some scholars, focusing on the changes to the legal landscape in relation to the IoT, are warning of the "end of ownership" (Perzanowski and Schultz 2016; see also Farkas 2017), and a shift to a neo-feudal society (Fairfield 2017). The chapter contends that IoT companies are strategically crafting a private regulatory regime that relies

upon a hybrid arrangement of copyright law and contractual licensing agreements to exert post-purchase control over software-embedded physical goods. Enforcing this restricted model of ownership relies upon companies' pervasive automated surveillance of their customers to detect any violations to the software's copyright or the licensing agreements. This continuous connection between software-enabled products and their manufacturer not only enables companies to monitor how customers use their devices, but also facilitates the collection and distribution of data that enables the devices to function.

IoT companies' use of copyright law to govern physical goods with embedded software challenges the long-standing "simple distinction" between software and physical objects, and the legal understanding of a "distinction that software is one thing and physical objects another thing" in terms of ownership (Duan 2016). In short, applying a governance framework designed for digital content such as music, movies, and (unembedded) software in order to govern software-enabled physical products represents a significant shift in how we conceive of and regulate property (see Mulligan 2016).[2] The IoT thus blurs the formerly clear boundaries between digital content and physical goods. Most people, however, would likely say that there is a difference between purchasing a digital version of a movie from Apple and buying a tractor, a home security system, or a television. The shift to a licensing model, and concurrently, the expansion of copyright owners' power over physical goods, has the consequence that consumers are constrained within a "new digital serfdom" in which consumers are digital peasants (see Fairfield 2017). The newly restricted nature of consumers' ownership of software-enabled goods is demonstrated in the near-ubiquitous use of the term "user" rather than "owner" in licensing agreements, and more broadly, the discourse around the IoT (Mulligan 2016, 1124).

Concurrent to this blurring of boundaries between digital content and smart goods is the change in the economic landscape with the rise of data-driven economies. Data and, more broadly, the control over knowledge are not simply a foundational element of economic success: they are also a source of power. The contemporary period is characterised by the dominance of the data-driven economy, typified by the world's most valuable companies, the U.S.-based Apple and Alphabet, the parent company of

[2] For comparisons of real property and intangible intellectual property in legal history, see Mulligan (2016).

Google. The growing centrality of data to the global economy is evident in what scholars alternatively term "data capitalism" (West 2017), "surveillance capitalism" (Zuboff 2015), the "information-industrial complex" (Powers and Jablonski 2015), and "platform capitalism" (Srnicek 2017). These concepts each accord primary importance to the control over information, especially data within the global economy, and recognise the economic and political importance of actors that have the capacity to accumulate, store, and process mass amounts of data. The expansion of the data-driven economy opened the way for private actors to commodify and monetise all manner of data, while the incorporation of networked software into physical goods, backed by copyright law and contracts, affords private actors a mechanism to extend their control over their products.

IoT companies' control of smart products is a form of knowledge governance, which this chapter explains by drawing upon Susan Strange's concept of the knowledge structure. At the core of these regulatory arrangements is an effort to exert control over knowledge, both in the form of proprietary software and data collected and generated by IoT products, with the latter becoming increasingly central to the global economy. Studying how IoT companies are fundamentally reshaping the governance of physical objects through the control over software (knowledge governance), importantly reveals the politically contested nature of ownership in which the benefits of ownership of software-enabled objects largely flow to companies. Moreover, policymakers and consumers do not fully understand the inherent differences between smart and traditionally "dumb" products.

The rest of the chapter proceeds as follows. First, it outlines how IoT firms are operating as a private regulatory regime to exert post-purchase control over smart goods. Next, the chapter turns to examine IoT makers' regulatory authority—copyright law and contractual agreements—and then outlines how companies use surveillance to govern their customers' use of IoT products. Then, the chapter explains the varying forms of post-purchase restrictions that companies can impose on their customers, including the limitations on modifying or repairing smart goods, and changing the functionality of those goods. The chapter briefly considers the wider implications of the governance of smart devices before providing a short conclusion.

1 Private Regulation of Knowledge

Strange's knowledge structure provides a useful starting point to consider the governance of smart devices, especially with her emphasis that power lies in the capacity to convey knowledge, as well as in the ability to exclude others from knowledge (Strange 1994, 119). Knowledge governance refers to how knowledge is created, stored, legitimised, communicated and in whose interests (Strange 1994, 121), as well as the regulatory and ideological systems that govern the knowledge economy (Haggart 2017). Of particular relevance to this chapter is the regulatory aspect of knowledge governance, that is, the formal and informal rules governing how data is defined and controlled, by whom, and with what technologies (see Haggart 2017, 187). The two mechanisms governing smart devices are copyright law and contractual agreements that, collectively, set the rules governing the use of IoT products and the data generated.

IoT companies' strategic expansion of their control over smart goods constitutes a private regulatory regime, which refers to the actors, norms, and rules making up a particular regulatory arrangement (Eberlein and Grande 2005, 91), where those actors are involved in making, implementing, and/or enforcing rules and standards (see Picciotto 2002). Companies' post-purchase control over their products occurs not through legislation or publicly debated policy changes, however, but through the hybrid arrangement of intellectual property laws and legal contracts (Langenderfer 2009, 209). Through copyright law, and in particular, their considerable latitude in drafting their contractual agreements, IoT companies have a quasi-legislative power to set and enforce rules over their users and a quasi-executive power to enforce those rules through technical means (Belli and Venturini 2016, 4; see also Langenderfer 2009; Schulz and Dankert 2016). IoT companies, similar to internet intermediaries such as Google, typically grant themselves the right in their contractual agreements to restrict and sanction unwanted behaviour regarding their products, and they can unilaterally issue sanctions against users that they contend violate their policies (on intermediaries' capacity, see Tusikov 2016).

This regime regulates through surveillance: IoT companies monitor their customers' use of smart products, the products themselves, and the related data flows. These companies employ business models reliant upon the post-purchase control of their smart goods. IoT goods are inextricably linked to their manufacturers through their software, which enables companies to update software or downgrade its functionality automatically,

remotely, and without their customers' agreement or knowledge. As a result, how consumers use their internet-connected products is "contingent on rules established by an external authority" (Perzanowski and Schultz 2016, 122). Copyright owners of the software have legitimised politico-legal authority to determine the balance between rights and access (Carolan 2017, 12), thereby sharply tilting the balance of control between copyright owners and users in favour of IoT companies. In doing so, IoT companies exemplify Strange's idea of knowledge governance in their design of rules for the collection and distribution of data relating to the IoT, their control over software, and their deliberate practice of restricting their customers' capacity to fully control or own smart goods (see Strange 1994, 119).

1.1 Redefining Ownership

Despite the novelty of governance mechanisms designed for digital content being applied to physical goods with embedded software, ideas regarding what constitutes property and the nature of ownership have always been "contested" (Banner 2011, 3). The concept of ownership is particularly complex when intellectual property is involved, as there are additional questions of what ideas are considered property and in what manner, who can lay claim to that property, and how ideational and technological changes can alter or lead to changes in law (Sell 2004). Understanding contemporary ideas of property and ownership also necessitates examining the underlying power arrangements as particular groups shift "conventional understandings of property in one direction or another" (Banner 2011, 3).

Shifting perceptions of ownership regarding smart goods are related to changes in the rights regarding the use, transfer, or control of purchases of physical goods (Perzanowski and Schultz 2016, 23). These changes involve the transfer of rights from purchasers, who historically enjoyed such rights, to intellectual property owners that are often large institutional actors (Perzanowski and Schultz 2016, 23). With the incorporation of software into hardware, there is a rebalancing of the idea of ownership between sellers and buyers, with owners of intellectual property rights being accorded a greater proportion of rights over the intellectual property than if it were a physical object. Consumers are only entitled to a "precarious" form of ownership of smart products, which only entitles them to a licence to use—not to control and use as they see fit the goods they purchase—and companies can change the conditions of "ownership" after purchase.

Technological innovation also drives changes in how we conceptualise property, sometimes opening new markets for property and fundamentally altering existing ones. Propertising airspace, for example, followed the invention of airplanes (Fairfield 2017), as a shift in the perceived value of a resource often triggers a struggle among interest groups to create and enforce property rights in that resource (Banner 2011, 289). In the Internet of Things, data is "both the modus operandi and raison d'être," as IoT devices require data to deliver services and data is also a valuable commodity (Shelton et al. 2015, 16). In other words, data is not only fundamental to the operation of the IoT, but data is also the product (see, e.g., Farkas 2017). By deciding to measure and commodify certain information, such as heartbeats or soil conditions, IoT manufacturers are creating data they anticipate will have commercial value, and then using copyright and licensing agreements to control the data collected by their products' software.

2 Governance of IoT

Embodied in the IoT is a blurring between physical and digital worlds in which physical products are designed to collect, sort, and transmit data (Friedland 2017, 102, 105). The purpose of IoT products is to add internet connectivity to hardware in order to enable virtually any type of physical good to collect and transmit data using embedded sensors, thereby creating networks that connect "people-people, people-things, and things-things" (Morgan 2014). IoT devices are becoming ubiquitous throughout the economy and society. While general discussions of IoT devices tend to focus on consumer products such as Fitbits and Amazon Echo speakers, consumer-oriented IoT goods represent only one category. Alongside these smart goods are industrial-oriented goods, such as vehicles, including tractors, medical diagnosis and treatment equipment, and traffic control systems in cities (see DeNardis and Raymond 2017). While the industrial IoT is often associated with safety-critical products and services relating to oil and gas, healthcare, and power sectors, some consumer-oriented IoT products can also have health-and-safety-critical functions, particularly when they are included in goods such as vehicles (think crash-avoidance systems), home security systems, and fitness wearables such as Fitbit.

As noted earlier, at the heart of IoT devices is software, usually proprietary and governed by copyright law and restrictive licensing agreements. Those who own this copyright—namely, the manufacturers of the smart

devices or related companies[3]—can govern the use of the IoT product and the data generated in its use. Copyright law, which governs music, movies, books, and art, along with software, lays out rules that determine how knowledge and creative works can be accessed, used, and shared, by whom, with what technologies, for what reasons, and with what restrictions. In the 1990s, two international treaties—the *World Intellectual Property Organisation (WIPO) Copyright Treaty* and the *WIPO Performances and Phonograms Treaty*—expanded copyright to include protection for what are called digital rights management (DRM) tools. DRMs are a broad set of policies and tools that manage access to content and monitor consumer behaviour to enforce licensing agreements that establish the terms of use for the underlying copyright content (Kerr 2007, 6). An important type of DRM is a technological protection measure that can be understood as a digital lock that enables the copyright owner to control access to or the use of the copyright-protected content. As interpreted by many countries, particularly the United States, DRM protection enables manufacturers of IoT devices to set rules governing how those products are used, for what purpose, and even the life span of the products.

In most jurisdictions, the protection of technological protection measures is codified within copyright legislation, prohibiting the creation and distribution of technologies (termed "circumvention devices") that break or bypass these digital locks.[4] Fitbit, for example, does not allow users to "modify, decompile, disassemble, reverse engineer, tamper with or otherwise attempt to derive the source code of any software that Fitbit provides to you or any other part of the Fitbit Service" (Fitbit 2017a).

Exemptions for the legal circumvention of these digital locks are often narrow. In practice, this means that even if the activity in question is

[3] John Deere, for example, explains that the vehicle manufacturer (i.e., Deere) may not own the copyright to the vehicle software or software systems (Bartholomew 2014, 5). While John Deere does not provide further clarification on this point, the company appears to be saying that in some cases, the smart manufacturer may not necessarily own the copyright over all the software systems within the smart product, especially in the cases of complex machinery such as tractors or vehicles. This statement demonstrates the complicated nature of copyright ownership and the complexity of determining ownership in regards to objects with embedded software.

[4] The U.S. 1998 *Digital Millennium Copyright Act's* Section 1201 prohibits most circumstances of bypassing or breaking Technological Protection Measures (TPMs) set by copyright owners. Similarly, Canada's *Copyright Act*, amended in 2012, makes it illegal to break or circumvent a digital lock (Sec. 41.1).

granted under law, such as copying content from one device to another, if the rights holder applies a digital lock to that content, then the activity is prohibited. Breaking digital locks may not carry significant penalties for individuals, but the act of using technological measures to set rules generally prevents people from accessing content or using their IoT device in ways that are permitted under law.

2.1 Licensing Agreements

Alongside copyright law, IoT companies commonly attach contractual agreements to each IoT product governing the software embedded within the goods. End-user licensing agreements (EULAs), which are also often called software licences, govern software applications, for example, your (licensed) copy of Microsoft Word.[5] These agreements are legal contracts that set out terms governing issues such as copyright ownership and penalties for violation of the contracts.[6] Users have the option of either clicking "accept" or "I do not accept" (with "I do not accept" meaning they cannot use the software).

For IoT makers, the question of ownership of smart devices is clear: copyright holders retain ownership over the software within the IoT product. General Motors, for example, argues that customers who wish to access or modify the vehicle's software in order to repair or tinker with the vehicle "incorrectly conflate ownership of a vehicle with ownership of the underlying computer software in a vehicle" (General Motors 2015, 10). According to General Motors, then, the customer purchased all non-software elements of the vehicle, not its software-enabled elements. Similarly, in its agreement, Nest informs its users that its product software "is licensed to you, not sold" (Nest n.d.).

By incorporating their digital rights management policies into contractual agreements with their customers, IoT companies can impose their

[5] For a detailed analysis of EULAs, their origins in the software industry, and their implications for ownership, see Perzanowski and Schultz (2016).

[6] In addition to EULAs, technology companies may use terms-of-service agreements (also called terms of use or terms and conditions), which are much broader than EULAs and set out terms governing issues such as copyright ownership and penalties for violation, the collection and use of customers' data, as well as rules governing payment and security of the website or application in question. For the sake of clarity, this chapter refers to EULAs only, but recognises that companies may incorporate policies governing their software under the terms-of-service agreements.

rules unilaterally on their users, and enforce those rules through technical means (Belli and Venturini 2016, 4; see also Langenderfer 2009). Companies typically grant themselves the latitude to restrict and sanction unwanted behaviour regarding their products, and they can unilaterally issue sanctions against users they contend violate their policies (see Tusikov 2016). IoT manufacturers typically include a clause that gives them the right to terminate service at any time for any reason. The wearable company Fitbit, for example, tells users: "We reserve the right to suspend or deactivate your account or your access to certain aspects or all of the Fitbit Service, or to terminate these Terms, at our sole discretion, at any time and without notice or liability to you" (Fitbit 2017a). Even if the behaviour in question is legal, companies have the discretion to terminate users' access to or disable the product itself.

Customers, meanwhile, may not even be aware of the rules that govern their use of the IoT product, as these agreements are "contracts of adhesion" that "stick to you whether you want them to or not."[7] According to the (now defunct) wearable fitness company Jawbone, "if you access or use our site(s), you accept these terms and become bound by a legal contract between you and Jawbone based on these terms" (Jawbone 2017). However, people generally do not read or fully understand these often lengthy and complexly worded agreements (see Bakos et al. 2014; Tene and Polonetsky 2013). Consumers, therefore, do not wholly appreciate how software-enabled goods differ from their non-smart counterparts and are unaware of the manufacturer-imposed restrictions upon smart goods. This lack of public awareness is borne out in consumer research that demonstrates consumer confusion in regards to the IoT (see Consumers International 2017).

Privately drafted contractual agreements thereby enable companies to institute their preferred rules. Software and the rules protecting software enable rights holders to maintain control over their internet-connected products even after their sale. As the following sections explore, IoT companies are able to exercise the post-purchase control over smart goods through their continual surveillance of smart devices and their users. This surveillance, coupled with the companies' capacity to remotely change the products' software, enables smart manufacturers to alter or degrade the software (and thus, the product).

[7] Interview in 2016 with a lawyer in Ottawa, Canada, specialising in internet law.

3 Regulation Through Surveillance

For manufacturers of IoT goods, surveillance is both a business model (Schneier 2013) and a regulatory mechanism. "Smart" can be usefully understood as an acronym for "Surveillance Marketed as Revolutionary Technology," argues technology critic Evgeny Morozov (Timm 2016). This point aptly captures the data-intensive nature of the IoT, and its normalisation of pervasive, continuous corporate surveillance of consumers. This monitoring performs two interrelated functions: data collection and customer/device monitoring. Data-intensive products are emblematic of the "sensor society," a world in which complex, often corporate, infrastructures enable the massive collection, storage, and processing of sensor-generated data from interactive, networked devices (Andrejevic and Burdon 2015, 21). Integral to these infrastructures are "always-on, ubiquitous, opportunistic ever-expanding forms of data capture" (Andrejevic and Burdon 2015, 19). Fitbit, for instance, tells its users that its devices collect data on "steps you take, your distance traveled, calories burned, weight, heart rate, sleep stages, active minutes, and location" (Fitbit 2017b). Fitbit customers use this data to track their sleep patterns and fitness levels, while data analytics companies acquire the data produced by fitness wearables, in an anonymised, aggregated format, in order to determine patterns, for example, relating to mortality and chronic disease risks that they can sell to insurance companies, governments, and healthcare providers (see Tiku 2014).

IoT surveillance also acts as a regulatory mechanism. IoT companies' model of post-purchase control relies upon constant surveillance of customers. Every time someone uses an internet-connected product, depending on the product type, the software may collect information to authenticate the user or the activity, or the software may scan the device for potential violations to the software copyright or the product's licensing agreement. For example, SambaTV, a content-recommendation app for smart televisions, gathers detailed data on users in order to provide personalised recommendations for viewers, including what viewers watch, when, for how long, and the devices used to access content. However, on the regulatory side, in its privacy policy, SambaTV states that it also monitors its customers in order to "detect, investigate and prevent fraudulent transactions and other illegal activities and protect the rights, safety and property of Samba and others" (SambaTV 2016).

The intensity of smart devices' communication with their home servers, in order to receive instructions and distribute data necessary to their proper functioning, further demonstrates the ubiquitous nature of surveillance within the IoT. A study that monitored smart home products' frequency and patterns of communication found the products regularly communicated with their servers to confirm they had power, were online, and to look for updates, even when the products were not in use or no one was present in the house (Hill and Mattu 2018). All products communicated daily, some several times daily, and an outlier, the Echo, communicated with Amazon's servers every few minutes (Hill and Mattu 2018).

Prior to the advent of digital licensing agreements paired with aggressive rules protecting intellectual property rights, companies did not have the means to conduct wholesale monitoring of their users or to control goods after their purchase. In the case of books banned by courts for obscenity, profanity, or graphic sexual content, for example, publishers could recall shipments from retailers, but could not track down each book from customers, even if they so desired. As IoT products function through pervasive data collection, companies have the capacity to monitor closely their products' use, customers' behaviour, and actions that may violate company policies.

3.1 Restricted Ownership

Traditionally, companies could cancel or change the conditions relating to product warranties, altering or denying coverage or product replacement. In these cases, the warranty—repairing, replacing, or substituting products—is the service. In the IoT, however, the software enabling the smart good is the service, and the customers' ability to use this good is governed through a complex licensing agreement. Most consumers would reasonably expect that similar to traditional goods, they can use or treat smart devices as they wish. One issue that highlights the precarious nature of ownership of IoT products and how IoT companies can broadly determine how consumers use their products is the "right-to-repair" debate. This right, which is sometimes termed the "freedom to tinker," can be understood as the "freedom to understand, discuss, repair, and modify the technological devices you own" (Felten 2013 cited in Samuelson 2016, 565). Proponents argue that the freedom to take apart, fix, and modify objects they have purchased is a fundamental aspect of ownership and an

integral part of innovation (see Duan 2016; Samuelson 2016). The right-to-repair movement specifically argues that consumers should have access to manufacturers' diagnostic software, repair manuals, and service parts, and the ability to choose whether they patronise independent repair shops or those authorised by the IoT company.[8]

In the United States, where the right-to-repair movement is most prominent, advocates and opponents have clashed over what restrictions, if any, manufacturers should be allowed to impose on the repair or modification of their smart products. While the right-to-repair movement is prominently associated with legal battles to give consumers the right to have cell phones repaired at independent shops, it encapsulates a broad range of goods with embedded software—from common household appliances to vehicles, medical devices, and farm equipment (see Matchar 2016). As of late 2018, there were 19 bills that were pending or shelved within state legislatures in the United States dealing with the right-to-repair goods. Most of these bills, however, faced well-funded opposition from manufacturers of smart goods. Apple, for instance, has long opposed bills in the United States that would make it easier for independent repair shops to fix Apple products and obtain replacement parts and diagnostic software, as has John Deere (see Koebler 2018).

Of all the devices and groups implicated by the IoT, it has been farmers seeking the right to repair their farm equipment that has emerged as a flashpoint in this debate, particularly in the United States, where their plight has generated widespread media coverage. Farmers' stance promoting the right to repair is easily understandable. Farmers have a long history of repairing and modifying their tractors, a necessity borne out of working on isolated rural properties, the high cost of transporting equipment to and from authorised mechanics, and the significant financial losses from broken equipment, especially during harvest season (see, e.g., Carolan 2017). Farming equipment, moreover, is a more expensive, long-term investment than a cell phone. Consequently, John Deere's requirement that farmers—both in the United States and Canada—use authorised mechanics because "the diagnostic equipment used to manage and adjust and modify the equipment software is proprietary" to the company has

[8] The Repair Association, for example, a U.S. non-governmental umbrella association of industry and civil-society groups, advocates for consumers to have the right to access product information, parts and tools, unlock products for repair and reuse, as well as unencumbered resale and repairable products. See https://repair.org/association.

been a flashpoint for activists (CBC Radio 2017a). Specifically, according to a U.S. John Deere executive, the company considers "'an unauthorized repair' [to be] an attempt to modify or change the embedded code that is part of the control system that manages that tractor" (CBC Radio 2017b). The breadth of this prohibition appears to preclude many repairs or changes that farmers may want to make or have their independent repair person undertake.

In defence of prohibitions on farm equipment modifications, proponents argue that repairing or tinkering with safety-critical goods, such as tractors, raises potentially serious security and safety complications. Customers altering the product's software could introduce vulnerabilities into the operating system, a possibility that IoT companies routinely warn of in their arguments for prohibiting software modification. John Deere, for example, states that tinkering with its vehicle software could introduce "viruses, Trojan horses, or other nefarious software" that could "shorten vehicle longevity or lead to unpredictable vehicle operation" (Bartholomew 2014, 18). Further, John Deere contends that the average consumer does not "have the technical expertise, training, test equipment, staff, resources, or funding" to repair vehicle software properly and verify its conformity with industry standards (Bartholomew 2014, 22). These concerns may be valid in some cases, as modifying complex software systems requires specialised technical knowledge. However, this argument strategically overlooks the key complaint of many customers who merely want the option of taking their smart products to independent repair shops instead of being required to deal with individuals authorised by the rights holders. Equally important, not all smart products meet the same safety-threshold concerns as a motor vehicle.

Lacking legitimate channels to access diagnostic software independently and prohibited from working with mechanics not authorised by John Deere, farmers have few other legal repair options. Such restrictions have led some farmers in Canada and the United States with John Deere tractors to acquire cracked John Deere software[9] from illicit websites in Poland and Ukraine to run diagnostic tests on their tractors, as well as fix or customise the vehicles (Koebler 2017). Farmers forced to use illicitly acquired software to undertake their own necessary repairs of legally purchased

[9] Cracked software generally refers to code that has been modified, typically without the permission of the copyright owner and in violation of copyright law, in order to allow users to bypass authentication or authorisation security features such as passwords.

tractors because of rights holders' restrictive policies underlines the degree to which customers are being unfairly locked into company-specific platforms instead of choosing the products and service providers they prefer.

For many proponents of the right-to-repair movement in the United States, advocating for amendments to copyright legislation is an important, albeit highly difficult route to achieve the legal right to diagnose, modify, and fix their software-enabled products. Every three years, the U.S. Copyright Office releases new rules regarding U.S. copyright law, the *Digital Millennium Copyright Act* (DMCA), and these rules are enacted by the Librarian of Congress. The rules, termed "exemptions," make the circumvention of digital rights management legal in the specific cases granted by the Copyright Office. As a result, individuals can legally bypass DRMs in regards to those specific exemptions.

In 2015, for example, the Copyright Office granted an exemption to allow the modification of vehicle software for the purpose of "the diagnosis, repair, or lawful modification of a vehicle function" (United States Copyright Office 2015, 248–249). This exemption applied to vehicles, including tractors, but did not allow individuals to hire third parties such as mechanics to undertake the repair. In 2018, the Copyright Office again granted exemptions regarding repair, but this time allowed them to apply to a broader category of goods: vehicles, including tractors, and small goods, specifically "a home appliance or home system, such as a refrigerator, [or] thermostat" (United States Copyright Office 2018, 51). The 2018 exemptions also permit farmers to hire third parties to repair tractors, provided that items relating to the diagnosis and repair are "lawfully acquired" (United States Copyright Office 2018, 49). Even here, however, a significant problem remains: many companies make it difficult for consumers and independent repair shops to legally acquire parts, repair tools and manuals, and diagnostic software equipment necessary to identify problems and fix products.

Even when copyright legislation is amended to permit activities such as repair, companies can override those changes through their licensing agreements. Following the U.S. Copyright Office's exemptions granted in 2015 that allowed DRM circumvention for vehicle repair discussed earlier, vehicle manufacturers strongly objected (see United States Copyright Office 2015). In particular, John Deere began requiring farmers to agree to licensing agreements that effectively recreate the DMCA's pernicious effects, placing restrictions on owners who want to diagnose, repair, and

modify their tractors as they are legally permitted to do, with violations of this policy deemed a breach of contract (see John Deere 2016). In short, John Deere's licensing agreement forbids most repair and modification of its vehicles by the owner and requires owners to deal only with its authorised repair shops (see John Deere 2016, 1). By setting restrictions on the use of their products in their licensing agreements, companies can deny individuals rights granted in law and sharply curtail people's ability to use smart goods as they wish. It is not yet evident how John Deere may respond to the 2018 exemptions from the Copyright Office that permit individuals to hire third parties to repair tractors.

3.2 Changing IoT Functionality Remotely

In addition to curtailing consumers' capacity to repair goods or work with unauthorised repair shops, IoT companies also limit consumer control over their software-embedded products through automatic software updates, which are an inherent feature of IoT goods. IoT manufacturers reserve the right in their contractual agreements to install software updates automatically without the users' consent or notification, as the products' functionality is dependent upon continued software updates. Tethered products, enabled by companies' continual surveillance of their customers, are highly regulable (see Zittrain 2008). Automatic updates can be an efficient way to ensure that products receive necessary upgrades, such as essential security patches, particularly as customers may not reliably install updates independently. According to Nest, the Google company and maker of smart home products, the company may

> develop patches, bug fixes, updates, upgrades and other modifications to improve the performance of the Product Software and related services ("Updates"). These may be automatically installed without providing any additional notice or receiving any additional consent. You consent to this automatic update. If you do not want such Updates, your remedy *is to stop using the Product*. If you do not cease using the Product, you will receive Updates automatically. You acknowledge that you may be required to install Updates to use the Product. (Nest n.d., emphasis added)

By controlling the product's software, IoT companies have the capacity to change a product's functionality remotely. Depending on the product's features, companies may have the capacity to improve or downgrade func-

tionality. Tesla, for example, remotely upgraded Tesla vehicles in Florida to expand their mileage capacity with the approach of Hurricane Irma in 2017 in order to facilitate evacuation efforts (Westbrook 2017). More controversial, however, is the practice of forcing customers to choose between unwanted software updates and the continued functionality of their devices, as with the Nest example. The electronics company Sonos announced in 2017 that if users declined to accept an updated privacy policy, their smart sound systems may "cease to function" (Whittaker 2017). Consumers have little choice when it comes to accepting or rejecting IoT companies' actions. As in the Nest case, the choice often boils down to accepting the company's decision or "to stop using" the *physical* product you have already purchased.

Control over software also enables IoT companies to decrease product functionality deliberately, which this chapter terms "regulation by bricking." Bricking is the remote destruction of IoT products by manufacturers who strategically withhold software updates, which can contain essential security patches, or issue software updates designed to degrade the product's functionality. Depending on how products are bricked, they may cease to operate immediately or slowly lose functionality over time. Bricking devices can be an effective, appropriately rapid practice for products that are dangerously defective or pose a public health or safety risk, especially given the challenges of implementing wide-scale product recalls. In 2016, for example, Samsung released a software update designed to prevent U.S. Galaxy Note 7s from charging as the phones' batteries had a problem of overheating and catching fire. This software update eliminated the phones' "ability to work as mobile devices" (Samsung 2017), and Samsung issued its customers with replacement phones.

With smart products, manufacturers have the capacity to set and enforce rules in ways that were not previously possible. When companies cancel a product line or go out of business, they can brick all goods, even those they have already sold. Nest decided in 2016 to discontinue the Revolv smart home system that the company had purchased in 2014. The Revolv hub communicated with light switches, garage door openers, motion sensors, and thermostats, and enabled users to programme these devices and operate them remotely. Nest's announcement was blunt: "As of May 16, 2016, Revolv service will no longer be available" (Lawson 2016). As a result, Revolv customers' lighting, temperature control, and security systems ceased to function.

Corporate requirements that customers accept unwanted alterations to their goods, especially those unrelated to the products' security, reveals the precarious nature of ownership in regards to software-embedded goods with a substantial shift in control away from individual "owners" and towards those who own the software. At best, IoT ownership is tenuous and subject to changes in business operations. At worst, it is dependent upon companies' whims. IoT goods remain firmly tethered to those who control the software, and the products' functionality is dependent upon continued software updates. Further, smart products' dependence on cloud software services means that they are highly susceptible to disruption and highly regulable by IoT manufacturers.

Bricking, in particular, raises critical questions about the responsibilities of businesses to their customers, consumers' expectations about the products they buy, and the vulnerability of IoT products to post-purchase restrictions. The cases discussed highlight the intertwined hardware and software components within the IoT. Those who control the product's software can affect the overall functionality of the product.

4 You Don't Own Your IoT Device

With the expansion of the IoT, a fundamental question is whether buyers of IoT products are "owners" who fully control their goods or "licensees" with limited rights of ownership (Samuelson 2016, 588). Confusion over this point is endemic: even after more than a decade of consumer experience with digital content from iTunes and Amazon, studies of consumer behaviour find that consumers erroneously think they own the digital files they have purchased and are legally entitled to share, sell, give away, or bequeath their digital collections in their wills (see Perzanowski and Hoofnagle 2017). Simply put, consumers are deeply misinformed about restrictions on ownership relating to digital content.

The confusion multiplies when it comes to the IoT and smart devices. The U.S. Federal Trade Commission (FTC), in a letter to Nest following the company's bricking of the Revolv hub, pointed out that "reasonable consumers would not expect the Revolv hubs to become unusable" (Engle 2016). Similarly, in a report on IoT products, the FTC concluded that consumers "generally expect that the things they buy will work and keep

working, and that includes any technical or other support necessary for essential functioning" (Rich 2016). According to the FTC, it is unclear whether IoT manufacturers are selling hardware (devices), software (services), or both, and the degree to which consumers understand what they are purchasing (Rich 2016). When hardware and software are interconnected, as they are in IoT devices, it is unclear whether consumers fully understand that they have a more precarious relationship with IoT goods than with non-software-connected goods.

As John Deere, General Motors, and Nest make clear, customers currently do not own software-embedded goods outright. Ownership of software-embedded physical goods is "contingent" as these products are essentially "rented instead of owned, even if one pays up front for them, since they are subject to instantaneous revision" (Zittrain 2008, 107). Purchasing smart goods, then, may be more properly understood as effectively a type of rental in which the buyer purchases a licence to use the goods. Consumers may enjoy certain benefits traditionally associated with ownership, such as driving a tractor or car, but not others such as tinkering, repairing, or modifying goods as they see fit.

Some IoT companies are exploring the idea of a subscription model in which customers pay a monthly fee for the continued operation of their smart devices. A key benefit here for IoT companies is that the licensing of smart goods provides a continued revenue stream that comes from supplying the software as a service. Instead of buying a smart television or smart home security system, consumers are purchasing the use of the television and security system as software-enabled services. Speaking in relation to this licensing model, Tony Fadell, founder of Nest, said: "We'll get more and more services revenue because the hardware sits on the wall for a decade" (Rowe 2016). Customers purchase the hardware but rent access to the software.

For consumers, a licensing model could include useful, valuable services such as regular software upgrades and security patches. The tethered nature of IoT goods to their manufacturers, however, is not apparent to consumers, nor are the restrictions that companies impose through their licensing agreements. Given the general lack of consumer awareness of the restrictive nature of ownership of IoT goods, it is reasonable to assume that few people will understand the implications of a licensing or monthly subscription model in regards to IoT products. Many IoT companies would likely offer legitimate software updates, but such services can be costly as companies must pay for servers and employees to support the

products and security updates. Unscrupulous businesses, moreover, may threaten to withhold critical or security updates until customers pay. With smart goods, there is an always-present possibility that the company may change the conditions under which their customers use the smart products after purchase.

Constraining ownership also diminishes people's creativity and innovation by stifling people's ability to reverse-engineer or repair their own products. Tinkering is a broad concept that can encompass learning how things work, discerning flaws, building skills, and tailoring and repairing artefacts (Samuelson 2016, 564). Being able to tinker with a product "means that if there is a problem with it, you can figure it out and you can publicize, and you can tell people" (Duan 2016). Importantly, tinkering involves the intellectual freedom to test, analyse, and share one's research with others, as well as innovating and sharing those innovations (Samuelson 2016, 563). Not everyone has the interest or, more importantly, the capacity to tinker with their IoT goods. Ordinary people, however, can become "the beneficiaries of others' creative tinkering" (Samuelson 2016, 590) when those with the capacity and interest to tinker can usefully modify goods, identify vulnerabilities, or create new uses. As not all of us have the drive or ability to tinker or repair our devices, how software owners permit repairs and modifications are important because there can be "a 'grey zone' between what people have rights to and what they merely have access to" (Sikor and Lund 2009, 2, cited in Carolan 2017, 9).

Consumers' precarious ownership of software-enabled goods underlines the broader phenomenon of the data-intensive nature of IoT companies' business models, which tend to favour the companies' interests over those of consumers. IoT products exist to collect and transmit data—to each other, to their owners, and to the manufacturer—in order to perform their smart functions. This data, once accumulated and processed, is a valuable commodity. The emphasis on the mass collection of data through smart devices' always-on sensors has the goal of opening up "new data-collection frontiers" in which new datasets complement existing ones, generating "new patterns of correlation" that can be repurposed indefinitely (Andrejevic and Burdon 2015, 23–24). Ubiquitous data collection has the purpose of not only servicing existing IoT products but also applying the data in anticipation of developing new products or services. By its very nature, then, such data collection is opportunistic and speculative, as the value or use of some data only becomes clear in the future. Patent applications filed by Amazon and Google, for instance, show the

companies are interested in capturing data on people's emotions and desires, for example, by determining a speaker's mood based on voice volume, breathing rate, crying, or laughing (Maheshwari 2018).

Companies characterise the data-collection practices via smart products as voluntary as users expressly or implicitly consent to monitoring (Friedland 2017, 106). People may decide that giving away or selling their personal data, whether anonymised or not, is a good deal if they receive a valuable service or product in return. There is, however, a long history of companies not informing their customers in advance before they decide to monetise customer data or making it difficult for customers to opt out of corporate surveillance practices (Fernback and Papacharissi 2007). Even if people read and understood corporate policies—which research shows is not the case (see Bakos et al. 2014)—they may not have a choice in opting out because in order to "access essential technologies, relinquishing control over their personal data is the price they must pay" (Crawford et al. 2014, 1670). Similarly, consumers may not have the opportunity to choose non-smart products, which has the result of locking people into a situation in which smart devices harvest their data, a key characteristic of surveillance capitalism (Zuboff 2015). Just as software-enabled devices are inextricably linked to their manufacturers, so too are the customers as data on their activities, movements, and behaviour is integral for existing smart products and provides the basis for developing future products and services in the data-intensive economy.

5 Conclusion: "New Digital Serfdom"

The shift in the ownership model of physical goods to licensing, and concurrently, the expansion of copyright holders' power to the world of physical goods, means that the licensing physical products can be characterised as the "new digital serfdom" (see Fairfield 2017) in recognition of the restrictions on software-embedded products. Thanks to the interaction between contracts and copyright law, rather than owning physical products outright, consumers' purchase of IoT goods only entitles them to a licence to use the products they have purchased. Consumers are thus only entitled to a precarious form of ownership of smart products subject to the discretion of IoT makers who can arbitrarily change conditions after purchase. When consumers buy a product "that's designed to update itself automatically and the company reserves to itself in law the right to take away something [that device] had when you bought it," says Cory

Doctorow, an advisor to the Electronic Frontier Foundation, a digital-rights group, "that's a feudal relationship, in which you are a tenant of these things that you've nominally purchased" (Barrett 2016).

Applying copyright law to govern software-enabled physical goods blurs the boundaries between digital and physical objects (Duan 2016) and represents a significant shift in the regulation of physical goods and our understanding of ownership (see Mulligan 2016). Prior to the growth of the IoT, it was simple to distinguish computers from other physical goods; however, now it is now relatively difficult to differentiate smart devices from those without software (see Mulligan 2016, 1147). This chapter has detailed the key problems related to the governance of smart goods through copyright law and licensing agreements: restricted ownership, limitations on repair and modifications, bricking, and pervasive corporate monitoring. This type of expanded corporate control will likely result in "an incremental winnowing of consumer rights" and a situation in which product ownership, once well understood by consumers, become a "minefield of unanticipated restrictions and rules that may be learned only after the buyer runs afoul of them" (Langenderfer 2009, 208).

Given the problems outlined in this chapter, there is a critical need to strengthen governance practices regarding the IoT and the data-intensive economy more widely. Industry and civil-society groups are proposing principles to strengthen data protection, transparency, and security. The Principles for an Open Internet of Things Certification Mark, a community-led project started in 2017, for example, recommends that IoT makers must allow customers to repair and transfer the ownership of IoT products, be clear about the expected timeframe that the software will support the products, and not degrade products' functionality (Deschamps-Sonsino and Haque 2018). These principles are a useful starting point to kick-start a public dialogue on the governance of the IoT.

As this chapter demonstrates, the private post-purchase control that IoT companies exert over smart goods represents a significant change in private actors' regulatory capacity to set rules governing knowledge in the form of software and flows of data. Companies' use of contractual agreements, paired with intellectual property laws are not only rewriting long-held assumptions about ownership, but also establishing regulatory regimes with the potential to affect fundamentally how certain types of knowledge are controlled in society and the global economy. By drawing upon a Strangean framework, this chapter underlines the importance of investigating the actors and mechanisms of knowledge governance, the

ways in which knowledge is conceptualised, governed, and wielded, and the resulting social, political, and economic implications. Policymakers interested in IoT regulation should focus on working to ensure a proper balance between the seller and buyer and to ensure greater consumer awareness of corporate control over smart goods and data flows. Further research is needed to examine the long-term implications of rights holders' control over software-enabled physical goods and the data generated by IoT products, as well as fundamental shifts in the concept of ownership.

References

Legislation

Copyright Act (R.S.C., 1985, c. C-42, R.S., c. C-30, s. 1.). http://lawslois.justice.gc.ca/eng/acts/C-42/.

Digital Millennium Copyright Act (Pub. L. 105–304, October 28, 1998), 105th Congress, 1997–1998. www.govtrack.us/congress/bills/105/hr2281.

World Intellectual Property Organisation Copyright Treaty. 1996. http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html.

World Intellectual Property Organisation Performances and Phonograms Treaty. http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html.

References

Andrejevic, Mark, and Mark Burdon. 2015. Defining the Sensor Society. *Television & New Media* 16 (1): 19–36.

Apthorpe, Noah, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *Cryptography and Security*: 1–16. https://arxiv.org/pdf/1708.05044.pdf.

Baack, Stephan. 2015. Datafication and Empowerment: How the Open Data Movement Re-articulates Notions of Democracy, Participation, and Journalism. *Big Data & Society* 2 (2): 1–11.

Bakos, Yannis, Florencia Marotta-Wurgler, and David R. Trossen. 2014. Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *The Journal of Legal Studies* 43 (1): 1–35.

Banner, Stuart. 2011. *American Property: A History of How, Why, and What We Own*. Cambridge: Harvard University Press.

Bartholomew, Darin. 2014. Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201. John Deere & Company. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection System for Access

Control Technologies, Notice of Proposed Rulemaking, Fed. Reg. Vol. 79, No. 239, 73856, 73869. December 12. https://www.copyright.gov/1201/2015/comments-032715/class%2022/John_Deere_Class22_1201_2014.pdf.

Barrett, Brian. 2016. HP Has Added DRM to Its Ink Cartridges. Not Even Kidding (Updated). *Wired*, September 23. https://www.wired.com/2016/09/hp-printer-drm/.

Belli, Luca, and Jamila Venturini. 2016. Private Ordering and the Rise of Terms of Service as Cyberregulation. *Internet Policy Review* 5 (4): 1–17.

Carolan, Michael. 2017. 'Smart' Farming Techniques as Political Ontology: Access, Sovereignty and the Performance of Neoliberal and Not-So-Neoliberal Worlds. *Sociologia Ruralis* 58 (4): 745–764.

CBC Radio. 2017a. [Updated] Saskatchewan Farmer Hacks His 'Smart' Tractor to Avoid Costly Dealer Fees. *As It Happens*, March 29. Accessed December 28, 2018. http://www.cbc.ca/radio/asithappens/as-it-happens-mondayedition-1.4042503/updated-saskatchewan-farmer-hacks-his-smart-tractor-to-avoid-costly-dealer-fees-1.4042504.

———. 2017b. Chuck Studer, Director of Industry Relations for John Deere. *As It Happens*, March 29. Accessed December 28, 2018. https://www.cbc.ca/player/play/909545539721.

Consumers International. (2017). Testing Our Trust: Consumers and the Internet of Things 2017 Review. https://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf.

Crawford, Kate, Kate Miltner, and Mary L. Gray. 2014. Critiquing Big Data: Politics, Ethics, Epistemology. *International Journal of Communication* 8: 1663–1672.

Crawford, Kate, Jessa Lingel, and Tero Karppi. 2015. Our Metrics, Ourselves: A Hundred Years of Self-tracking from Weight Scale to the Wrist Wearable Device. *European Journal of Cultural Studies* 18 (4–5): 479–496.

DeNardis, Laura, and Mark Raymond. 2017. The Internet of Things as a Global Policy Frontier. *UC Davis Law Review* 51: 475–497.

Deschamps-Sonsino, Alexandra, and Usman Haque. 2018. *Principles for an Open Internet of Things Certification Mark*. Updates as of June 13, 2018. Accessed September 15, 2018. Copy on file with author.

Duan, Charles. 2016. Director, Patent Reform Project at Public Knowledge. Presentation at *Will Technology Make Ownership Obsolete*? Hosted by *Future Tense on Slate* at New America, Washington, DC, October 25, 2016. Accessed December 28, 2018. http://www.newamerica.org/future-tense/events/will-technology-make-ownership-obsolete/.

Eberlein, Burkhard, and Edgar Grande. 2005. Beyond Deregulation: Transnational Regulatory Regimes and the EU Regulatory State. *Journal of European Public Policy* 12 (1): 89–112.

Engle, Mary K. 2016. *Letter to Richard J. Lutton, Jr., Head of Legal and Regulatory Affairs, Nest Labs, Inc. from Mary K. Engle, Associate Director for Advertising Practices, Federal Trade Commission*. Accessed December 28, 2018. https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf.

Fairfield, Joshua A.T. 2017. *Owned: Property, Privacy, and the New Digital Serfdom*. Cambridge, UK: Cambridge University Press.

Farkas, Thomas J. 2017. Data Created by the Internet of Things: The New Gold Without Ownership? *Revista La Propiedad Inmaterial* 23 (enero-junio): 5–17. https://doi.org/10.18601/16571959.n23.01.

Fernback, Jan, and Zizi Papacharissi. 2007. Online Privacy as Legal Safeguard: The Relationship among Consumer, Online Portal, and Privacy Policies. *New Media & Society* 9 (5): 715–734.

Fitbit. 2017a. Fitbit Terms of Service. Updated September 28, 2017. Accessed September 7, 2018. https://www.fitbit.com/legal/terms-of-service.

———. 2017b. Fitbit Privacy Police. Updated September 28, 2017. Accessed September 7, 2018. https://www.fitbit.com/en-ca/legal/privacy-policy.

Friedland, Steven L. 2017. Drinking from the Fire Hose: How Massive Self-Surveillance and the Internet of Things Are Changing Constitutional Privacy. *West Virginia Law Review* 119: 100–122.

General Motors. 2015. *Comments of General Motors LLC. Before the United States Copyright Office, Library of Congress.* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. Docket No. 2014-07. Proposed Class 21: Vehicle Software – Diagnosis, Repair, or Modification. March 27. Accessed December 28, 2018. https://copyright.gov/1201/2015/comments-032715/class%2021/General_Motors_Class21_1201_2014.pdf.

Haggart, Blayne. 2017. Incorporating the Study of Knowledge into the IPE Mainstream, or, When Does a Trade Agreement Stop Being a Trade Agreement? *Journal of Information Policy* 7: 176–203.

Hill, Kashmir, and Surya Mattu. 2018. The House that Spied on Me. *Gizmodo*, February 7. https://gizmodo.com/the-house-that-spied-on-me-1822429852.

Jawbone. 2017. Terms of Use. Last updated August 18, 2017. Available from Wayback Machine. https://web.archive.org/web/20170818105427/jawbone.com/legal/terms.

Deere, John. 2016. License Agreement for John Deere Embedded Software. Accessed September 7, 2018. https://www.deere.com/privacy_and_data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf.

Kerr, Ian. 2007. To Observe and Protect? How Digital Rights Management Systems Threaten Privacy and What Policy Makers Should Do About It. In *Intellectual Property and Information Wealth: Copyright and Related Rights*, ed. Peter Yu, vol. 1. London: Praeger Publishers.

Kitchin, Rob. 2014. The Real-Time City? Big Data and Smart Urbanism. *GeoJournal* 79: 1–14.

Koebler, Jason. 2017. Why American Farmers Are Hacking Their Tractors with Ukrainian Firmware. *Motherboard*, March 21. https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware.

———. 2018. Apple Must Explain Why It Doesn't Want You to Fix Your Own iPhone, California Lawmaker Says. *Motherboard*, March 12. https://motherboard.vice.com/en_us/article/evmeya/apple-iphone-right-to-repair-california.

Langenderfer, Jeff. 2009. End-User License Agreements: A New Era of Intellectual Property Control. *Journal of Public Policy & Marketing* 28 (2): 202–211.

Lawson, Stephen. 2016. Why Nest's Revolv Hubs Won't Be the Last IoT Devices Knocked Offline. *PC World*, April 4. http://www.pcworld.com/article/3051760/hubs-controllers/why-nests-revolv-hubs-wont-be-the-last-iot-devices-knocked-offline.html.

Maheshwari, Sapna. 2018. Hey, Alexa, What Can You Hear? And What Will You Do with It? *New York Times*, March 31. https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html.

Manovich, Lev. 2001. *The Language of New Media*. Cambridge, MA: The MIT Press.

Matchar, Emily. 2016. The Fight for the 'Right to Repair.' *Smithsonian.com*, July 13. Accessed December 28, 2018. https://www.smithsonianmag.com/innovation/fight-right-repair-180959764/.

Mauritius Declaration on the Internet of Things. October 14, 2014. https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf.

Morgan, Jacob. 2014. A Simple Explanation of the 'Internet of Things.' *Forbes*, May 13. http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#545322076828.

Mulligan, Christina. 2016. Personal Property Servitudes on the Internet of Things. *Georgia Law Review* 50: 1121–1168.

Nest. n.d. End User License Agreement. Accessed March 8, 2018. https://nest.com/ca/legal/eula/.

Perzanowski, Aaron, and Chris Jay Hoofnagle. 2017. What We Buy When We *Buy Now*. *University of Pennsylvania Law Review* 165 (2): 315–378.

Perzanowski, Aaron, and Jason Schultz. 2016. *The End of Ownership: Personal Property in the Digital Economy*. Cambridge: MA: MIT Press.

Picciotto, Sol. 2002. Introduction: Reconceptualising Regulation in the Era of Globalisation. *Journal of Law and Society* 29 (1): 1–11.

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

Rich, Jessica. 2016. *What Happens When the Sun Sets on a Smart Product?* Federal Trade Commission, July 13. Accessed December 28, 2018. https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product.

Rowe, Adam. 2016. How the Internet of Things Erases Ownership. *IDGConnect*, May 2. Accessed December 28, 2018. http://www.idgconnect.com/blog-abstract/15820/how-internet-things-erases-ownership.

Samba TV. 2016. Samba TV Privacy Policy. Last updated March 25. Accessed September 7, 2018. https://platform.samba.tv/about/privacy-policy/.

Samsung. 2017. Samsung Expands Recall to All Galaxy Note7 Devices. January 22. Updated April 17, 2018. Accessed December 28, 2018. http://www.samsung.com/us/note7recall/.

Samuelson, Pamela. 2016. Freedom to Tinker. *Theoretical Inquiries in Law* 17: 563.

Schneier, Bruce. 2017. Security and the Internet of Things. *Schneier on Security* (blog), February 1. Accessed December 28, 2018. https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

———. 2013. Surveillance as a Business Model. *Schneier on Security* (blog), November 25. Accessed December 28, 2018. www.schneier.com/blog/archives/2013/11/surveillance_as_1.html.

Schulz, Wolfgang, and Kevin Dankert. 2016. 'Governance by Things' as a Challenge to Regulation by Law. *Internet Policy Review* 5 (2): 1–19.

Sell, Susan. 2004. Intellectual Property and Public Policy in Historical Perspective: Contestation and Settlement. *Loyola of Los Angeles Law Review* 38: 267–322.

Shelton, Taylor, Matthew Zook, and Alan Wiig. 2015. The 'Actually Existing Smart City'. *Cambridge Journal of Regions, Economy and Society* 8: 13–25.

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

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

Streitfeld, David. 2013. Google Concedes that Drive-by Prying Violated Privacy. *New York Times*, March 12. http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?pagewanted=all.

Tene, Omer, and Jules Polonetsky. 2013. A Theory of Creepy: Technology, Privacy and Shifting Social Norms. *Yale Journal of Law & Technology* 16 (1): 59–102.

Tiku, Nitasha. 2014 The Internet of Things Will Make Millions Selling Your Data. *ValleyWag*, April 18. Accessed December 28, 2018. http://valleywag.gawker.com/the-internet-of-things-will-make-millions-selling-your-1564733531.

Timm, Trevor. 2016. The Government Just Admitted It Will Use Smart Home Devices for Spying. *The Guardian*, February 2. https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government.

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

United States Copyright Office. 2015. Section 1201 Rulemaking: Sixth Triennial Proceeding. Recommendation of the Register of Copyrights. October 8. Washington, DC. Accessed December 28, 2018. https://www.copyright.gov/1201/2015/registers-recommendation.pdf.

———. 2018. Section 1201 Rulemaking: Seventh Triennial Proceeding. Recommendation of the Register of Copyrights. October 28. Washington, DC. Accessed December 28, 2018. https://s3.amazonaws.com/public-inspection.federalregister.gov/2018-23241.pdf.

West, Sarah Myers. 2017. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society* 58: 20–41.

Westbrook, Justin T. 2017. Tesla's Hurricane Irma Update Taps into Our Deepest Fears of 21st Century Driving. *Jalopnik*, September 10. Accessed December 28, 2018. https://jalopnik.com/teslas-hurricane-irma-update-taps-into-our-deepest-fear-1803081731.

Whittaker, Zack. 2017. Sonos Says Users Must Accept New Privacy Policy or Devices May "Cease to Function." *Zdnet*, August 21. Accessed December 28, 2018. http://www.zdnet.com/article/sonos-accept-new-privacy-policy-speakers-cease-to-function/.

Wiens, Kyle. 2015. We Can't Let John Deere Destroy the Very Idea of Ownership. *Wired*, April 21. https://www.wired.com/2015/04/dmca-ownership-john-deere/.

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

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30: 75–89.

Reflection II

Madeline Carr

As we move rapidly into what some are calling the Fourth Industrial Revolution, it is becoming increasingly clear that data will be fundamental to the acquisition and expression of power. Despite the centrality of the internet to daily life across much of the world and the rapidly growing market for internet-connected consumer and industrial products, both scholars and policymakers are struggling to understand and react to the rising importance of knowledge, broadly conceived, within the global political economy. Our understanding of this is shaped by important questions about the distinctions between information, data, and knowledge, as well as distinctions among infrastructure, devices, and data flows. Even more challenging perhaps, are not just the *distinctions* between these, but the *interactions* between them. What little we know about this now needs to be tested, validated, and challenged. If the discipline of International Political Economy (IPE) does not turn its collective attention to these crucial questions and their implications for power in the international system, it risks another stunning blunder comparable to the failure of the discipline of International Relations to predict the end of the Cold War.

M. Carr (✉)
University College London, London, UK
e-mail: m.carr@ucl.ac.uk

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_7

This volume takes an important step forward in this direction by considering knowledge governance through the work of Susan Strange. One of Strange's foundational contributions to International Political Economy is her theorisation of structural power, especially concerning how actors may wield authority, their means of doing so, and (critically, here) the ways in which different actors determine which forms and expressions of knowledge are legitimate. The chapters by Winseck and Tusikov explore these intersections among data, information, knowledge, infrastructure, and power through different aspects of the digital economy. They pay particular attention to the ways that state and market actors may exert authority in instituting rules and standards, as well as the consequences that these (quasi) regulatory efforts may generate. Through different empirical cases, both Winseck and Tusikov also reflect upon the nature of public goods and private actors, and the capacity and legitimacy of public and private rule-making efforts in regards to the internet infrastructure and personal data. In my reflection, I discuss three key themes that run through their chapters: materiality, state–market dynamics, and data governance—all of which are, of course, themselves interconnected.

1 Materiality

Materiality is an often-overlooked element in internet governance literature, where the discourse has predominantly revolved around processes, institutions, and societal impacts of internet access, content regulation, multi-stakeholder governance, and social media platforms. Strange's focus on materiality, covered by Haggart and Germain in this volume, makes her framework a useful way to insert materiality into discussions of internet governance. Tusikov and Winseck address two aspects of the physical dimension that have been less examined in order to illustrate the interplay between materiality and knowledge governance. Winseck focuses on the macro—the internet infrastructure, including submarine cables, exchange points, and routers—while Tusikov turns her attention to the micro, the devices through which we all leak data into the Internet of Things (IoT). In doing so, both chapters explore the complex and subtle dynamics between public and private actors and the fundamental debate over public interest and private ownership.

Winseck is engaged with the international political economy of the internet infrastructure. He carefully and systematically charts changes to the ownership and control of the critical information infrastructure. These

are the "pipes" through which data flows, the little-examined scaffolding upon which the information age is built. Understanding the economics behind this macro materiality is critical and Winseck's detail about who owns what, how they monetise the infrastructure, and how regulatory layers impact upon and facilitate this economic activity goes a long way to illuminating it.

Winseck argues that geopolitical control over the internet's material infrastructure layer is shifting away from its traditional centre of gravity in the United States and towards Brazil, Russia, India, China, and South Africa as well as the Asia-Pacific, European Union (EU), and African regions. Given that these are the regions with significant potential for market growth in terms of internet penetration, it is not surprising that they are attracting the attention of the big players in communications technology. Winseck finds that internet infrastructure in the Asia-Pacific region and Africa is increasingly being constructed and controlled by complex consortia of public and private actors. These actors adopt differing approaches to building or leasing infrastructure, all of which have implications for power now and in the future.

Most interesting and useful here is Winseck's historical approach. Through a comparative analysis of the political economy of nineteenth- and twentieth-century communications infrastructure, he situates current practices in a comparative context—rather than viewing "everything as new again." Winseck persuasively establishes fundamental changes in the geopolitical economy of the internet's material infrastructure to more complex and heterogeneous consortia than in previous decades. What these changes mean in terms of a declining, or perhaps more specifically, an altered, form of U.S. hegemony over the internet, however, are less evident—and beyond the scope of Winseck's chapter. Even though direct U.S. government involvement in infrastructure construction may have lessened, it does not necessarily follow, of course, that U.S. political or economic influence is similarly eroding. Actors outside the United States may adopt U.S. rules, technologies, or norms relating to the construction or operation of internet infrastructure, which continue to preference U.S. security, commercial, legal, and technical interests (see Carr 2016; Powers and Jablonski 2015).

Tusikov's material lens is much closer to a socio-legal approach. She is concerned with the relationship between consumer-oriented internet-enabled devices and individuals, specifically how that relationship is moderated by state and corporate actors. Much of Tusikov's analysis is

concerned with practices or developments that *could* be justified in some circumstances, but which, if not checked, could threaten basic consumer or even human rights. These, we know from dystopian governance fiction writers such as George Orwell or William Golding, can be the most dangerous and the most easily overlooked.

Tusikov's previous work linking the protection of intellectual property to state and corporate interests within the information economy (especially in the United States) really comes into play here (Tusikov 2016). In this chapter, she extends this analysis to engage with the material factors evident in the emerging IoT, particularly the interplay between the physical and digital realms that characterise consumer IoT-enabled devices. In doing so, she builds an argument that the extension of copyright rules into this physical realm (as well as the software and data that run through them) enables IoT companies to significantly restrict consumers' ownership of and exercise an unwarranted level of control over IoT products and the data they generate.

Work like this on the IoT is both important and urgent. In the rapid expansion of the IoT, a "chip-centric mentality," which conceptualises internet connectivity as an inherent product improvement (Hartzog and Selinger 2016, 583) prompts manufacturers to embed sensors and/or software in a wide array of consumer and industrial products that have not previously been connected to the internet. In the rush to add internet connectivity to products, however, manufacturers often neglect security—an issue that policymakers have only recently begun to consider seriously (see DCMS 2018; Brass et al. 2017; Schneier 2016). There are many, sometimes complex, reasons for this but the simplest is that in the context of a fast-moving market, companies manufacturing inexpensive products designed to have a short lifecycle struggle to justify the additional cost of including effective (but not yet required) security features or the cost involved in understanding the complexities of data protection regulation. This lack of security in IoT devices threatens to significantly extend the attack surface for hackers and other malicious actors, thereby reducing overall cybersecurity by introducing potentially billions of vulnerable devices.

Even leaving aside malicious actors (if one can), there are other systemic concerns, including the viability of the "right to repair," which Tusikov also regard as a gateway for eroding consumer and human rights. The right to repair refers to the belief that consumers should retain the right to either repair their own goods themselves or allow anyone they

wish to repair them on their behalf. Emerging initially from the United States through particular sectors such as automobiles and mobile phones, the right to repair takes up similar issues of consumer ownership and control of physical devices that the U.S. *Digital Millennium Copyright Act* implemented for intellectual property. From the manufacturers' perspective, monitoring the ways that IoT devices are used is necessary for some functions, such as ensuring that the product software receives essential updates, detecting any malware or licensing violations, and verifying that only authorised (and fully qualified) personnel diagnose and repair the goods (Brass et al. 2017). In safety-critical systems such as vehicles, this can make sense as it has implications for liability in case of failure. However, as we are far from a clear understanding of all possible dangerous or negative implications of IoT devices (who imagined that an IoT-enabled teddy bear could be used as a surveillance tool?), there is scope here for "mission creep." Retaining control over repairs and use means that some companies effectively "license" the device to consumers. While we are familiar with this model of limited ownership for software, in applying the same model to consumer devices, Tusikov argues that IoT companies are employing copyright law and terms-of-use agreements not simply to strengthen security, but also to extend their control over the data generated by IoT devices.

Tusikov's chapter also points to possible problems with IoT device obsolescence. Unlike an iTunes or Amazon library, the IoT leaves a physical trail of goods that has been described as the "Internet of Heirlooms and Disposable Things" (Hartzog and Selinger 2016). As the typical lifecycle of software is approximately two years, many IoT products will outlive their software and linger as dumb or zombie products (Hartzog and Selinger 2016, 588–589). Some objects may still work even without updated software, although their smart features may be lost. Other products such as home security systems or fitness wearables are useless without properly functioning software. Designed-in obsolescence of many devices such as mobile phones is already widely accepted by consumers, but given the vast number of IoT goods expected to enter the market (IHS Markit 2017) and the heavy metals used in their manufacture, such as lead and cadmium, we face adding to the already significant problem of electronic waste (see Baldé et al. 2017).

The challenge here, as it has been in the past, is consumer awareness. Consumers have historically been willing to trade their privacy and the ownership of their personal data for free applications—or for the freedom from

reading onerous and inflexible terms and conditions. There is every reason to expect this behaviour will continue in the IoT. Even labelling schemes currently proposed for IoT devices (similar to energy labels on household appliances or food labelling, see Blythe and Johnson 2018) are problematic because they potentially create a cheaper market for less-secure devices—thereby introducing a security/privacy premium that some less affluent consumers will have to forgo. As Tusikov points out, the lack of understanding of the inherent differences between smart and traditionally "dumb" products, and of the new limited model of ownership of consumer devices, means that obtaining true informed consent is deeply problematic.

2 State–Market Dynamics

The dynamic between the state and the market is another key feature of Strange's work with which both Winseck and Tusikov engage. Through their different empirical cases, each chapter reflects upon what Strange terms the "market-authority nexus" (Strange 1994). This is an important—even a *central*—element in the work of both Tusikov and Winseck, and it is consequently worth delving into in more depth.

Tusikov's analysis of the IoT leads her to focus on underlying governance mechanisms which, she argues, are a blend of law and contract. They are underwritten by the state's intellectual property laws, but further extended by corporate licensing agreements, which fundamentally alter the individual's relationship to their physical devices—and, of course, to the data they generate for market purposes. She has argued elsewhere that this is based, in part, on industry lobbying efforts for stronger copyright enforcement, a dynamic which typifies Strange's market-authority nexus (Tusikov 2016).

In her exploration of the limitations on ownership within the IoT, Tusikov raises a number of considerations for policymakers in terms of wider societal impact. In line with the issue of modified ownership emerging through challenges to the right to repair, she considers how companies' extension of their control over IoT devices may affect the way people tinker and innovate. This can have implications for the digital economy, but also for the direction and shape of technological developments. Science and Technology Studies has established the links between the perceptions of "problems" by certain actors and the application of resources to address those problems (Carr 2016). This, of course, is a form of power and centralising it in the hands of corporations has implications for which "problems" will be addressed in the future.

Additionally, Tusikov points out, there will be challenges involved in transferring control or ownership of IoT devices between consumers in a way that protects personal data, such as when someone buys a home with pre-existing (and pre-used) smart thermostat and security systems (see, e.g., Roth 2018). Recent work points to the potential for IoT smart home devices to be employed in perpetrating domestic abuse (see Tanczer et al. 2018a, b, c), as smart devices enable abusers to track and control victims through, for example, smart metres, security systems, and wearable devices. This raises important questions about gender, power, and socio-technical processes, a dynamic that Fish and Henne critically engage with in their chapters, as does Musto in her analysis of those chapters.

It is unlikely that a market-led approach to IoT security of consumer devices will be adequate and this brings the state–market dynamic into centre field (see Tanczer et al. 2018d). Putting responsibility for the security of devices back in the hands of consumers is also unlikely to provide the level of IoT security necessary. As an example, the U.K. government has invested heavily in thinking through the policy implications of managing the emerging IoT in such a way as to maximise the significant potential benefits while mitigating against inbuilt insecurity (PETRAS.org.uk). Their proposed *Code of Practice* for "secure by design" IoT was guided by five principles, one of which was reducing the burden on consumers (DCMS 2018), recognising that it is unreasonable to expect consumers to have the understanding or skills to manage their IoT products independently. Any government's goal will be to maximise the potential of the IoT to improve societal outcomes while mitigating the considerable security vulnerabilities and other negative implications. How exactly to do so, will be the focus of policy experimentation, innovative thinking, and critical scholarship like this for the next decades. Hence, Tusikov's work in carefully highlighting the nuances of these arrangements takes on added significance and will provide support to those making difficult policy decisions in the future.

Winseck's focus on the state–market dynamics of internet infrastructure is developed through meticulous attention to historical detail, a particular strength that runs through his scholarship (see, e.g., Winseck and Pike 2007; Winseck 2017). He considers that the anticipated consequences of liberalisation and deregulation, specifically the reduction of state intervention in the market have been significantly overplayed in this context. Winseck points here to the increasing willingness of regulators to address market concentration, the adoption of national broadband initiatives (as

an expected service and measure of development), and the role of national security and intelligence services in the mix of factors shaping the development of the global internet. He does all of this in the historical context of other global communications developments, which has the advantage of situating contemporary market structures and state–market interactions within a much broader, global context than is commonly the case.

With regard to the market conditions of current internet infrastructure ownership, Winseck identifies two key trends. The first is that the consortia that own this material element of internet infrastructure are changing shape from predominantly U.S. privately owned corporations to a more diverse set of actors. These new consortia, Winseck argues, are more heterogeneous than those involved in building telegraph and telecommunications infrastructure during the nineteenth and twentieth centuries, but they are also different to those that dominated the initial build-out of internet infrastructure. In contrast to the free-market, small-government rhetoric that has underpinned the dominant narrative of (assumed) U.S. internet hegemony, Winseck observes an increased role for national governments, particularly in the Asia-Pacific region, where state control of critical infrastructure takes on an entirely different (and positive) meaning in post-colonial states. This shift can be explained as a changing relationship in the market–authority nexus (Strange 1994) in which Winseck contends that nation-states and private business interests not only compete but also cooperate with a shared goal of economic accumulation.

The second key trend that Winseck observes is the continued presence of U.S. information giants in these consortia. With U.S. technology giants Facebook, Amazon, and Google expanding beyond services and into financing and developing infrastructure projects, his chapter considers the political and socio-economic consequences of the relationship among these actors and state-owned telecommunications firms and national governments in the Asia-Pacific and African regions. Here, he builds on existing literature critical of the export of Western surveillance-oriented business models of companies that have been integral to the U.S. government's global surveillance programmes (e.g., Schneier 2016). Given the interdependent relationships between U.S. internet firms and U.S. intelligence agencies revealed by Edward Snowden, Winseck's work raises questions about the extent to which the U.S. government may exert its influence through these consortia and the internet infrastructure projects they are developing in those regions.

Winseck's methodical investigation into the complex, intertwined and sometimes opaque ownership of internet infrastructure elicits important questions for future research into links between materiality and the information economy. It also illuminates important areas of discussion for policymakers. The long-term implications of these trends are fertile ground for future research and Winseck essentially lays out a range of research questions that should be taken up by IPE scholars concerned with the information age. What are the likely implications of Western investment in internet infrastructure in Asia and Africa? What challenges arise for national governments from working with private technology companies? Who is setting the rules in these cases of infrastructure construction and critically, who stands to benefit most? The ownership of critical information infrastructure may not be the first thing that comes to mind for scholars working at the intersection of global internet governance and IPE, but it clearly should not be the last.

3 Data Governance

All of this leads, in one way or another, to one of the central questions of the Fourth Industrial Revolution. How should data be governed, by whom, and towards which goals?

Control and ownership of data, as Tusikov explains, are central to the data-driven economy and a form of knowledge governance, as well as an important public policy issue. The IoT poses particular data governance challenges as IoT goods function by gathering, analysing, and disseminating data, including individuals' (sometimes sensitive) personal information. Control over and commodification of this extremely valuable data is obviously the focus of technology companies. In many cases, such as smart cities, individuals essentially lose their right to withdraw, so governance of personal data takes on even more gravity with regard to consent and responsible use. The General Data Protection Regulation (GDPR), for example, developed and implemented by the EU demonstrates greater political awareness of data protection and is radically shifting expectations of data governance. The GDPR puts much more onus on those who gather and control personal data to do so in ways aligned with human and consumer rights (Edwards 2018).

From Winseck's view, an important element of data governance debates is the diversification of "internets," in part prompted by commercial interests. Amazon and Google, along with other large telecommunications

companies, are expanding their involvement in separate content distribution networks in order to facilitate the fast, reliable delivery of services such as Amazon Prime TV. Winseck argues that this resulted in the creation of a series of private internets that threaten to overtake the public internet. The effect that multiple, privately controlled internets run by large industry actors may have is not clear. Nor is it evident how the proliferation of private, parallel internets may shape infrastructure development in Asia and Africa. However, Winseck's point that the multitude of internets that he describes are fracturing along geopolitical, regional, and public–private divides raise critical questions for the future of internet and data governance.

Together, the chapters raise serious questions about how data and infrastructure should be governed and by whom, the responsibilities and limitations of data ownership, and how a balance may be struck between security and privacy, and between the private control of and public access to data (see Farkas 2017). Both authors also point to the regulatory challenges raised by the shift to a data-driven economy, as both industry actors and state regulators struggle to adjust to a rapidly evolving environment. It can be difficult, for example, to determine which actors are ultimately responsible for addressing data breaches or security problems as, in some complex global supply chains, multiple parties may be involved or at fault. More broadly, many manufacturers, policymakers, and regulators do not fully understand the significance of companies moving from "device 'makers' to 'service providers'" (Hartzog and Selinger 2016, 583). This is important because, as both authors point out, there is a critical necessity for informed policymaking in the realm of digital technologies and internet infrastructure.

4 Conclusion

In addition to the themes of materiality, state–market dynamics, and data governance, these chapters critically reflect upon one of fundamental questions that guided Susan Strange's research: who benefits? For Tusikov, the answer at this early stage is, primarily, the companies that manufacture devices because they have the capacity to set and enforce rules that further their commercial interests and impose intrusive frameworks upon largely unaware consumers. This is not a fixed future, as Tusikov reminds us, as long as we acknowledge that there is a clear role for government to play in regulating many aspects of the IoT. Governments will have to carefully balance the opportunities and vulnerabilities inherent in the IoT in order

to deliver the best outcomes, but how exactly they should do that is uncertain and probably culturally specific. Winseck, meanwhile, describes a complex, fast-changing environment in which technology companies, state-controlled telecoms, and state actors are rapidly creating new internet infrastructure in the Asia-Pacific and African regions. Which actors will accrue the greatest benefits, how this may affect the internet (or internets), and the further consequences to U.S. internet hegemony also remain unclear. With their detailed analysis that engages broad questions of power, knowledge, and the consequences to digital and communications technologies when actors wield unaccountable authority, both chapters identify critical areas for future scholarship and policymaking.

References

Baldé, Cornelis P., Vanessa Forti, Vanessa Gray, Ruediger Kuehr, and Paul Stegmann. 2017. *The Global E-Waste Monitor: Quantities, Flows and Resources.* Bonn, Geneva, and Vienna: United Nations University, International Telecommunication Union, and International Solid Waste Association. https://www.itu.int/en/ITU-D/Climate-Change/Documents/GEM%202017/Global-E-waste%20Monitor%202017%20.pdf.

Blythe, John M., and Shane D. Johnson. 2018. *Rapid Evidence Assessment on the Impact of Labelling Schemes and Implications for Consumer IoT Security.* Report for the Department for Digital, Culture, Media, and Sport. Accessed December 28, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775562/Rapid_evidence_assessment_IoT_security_oct_2018.pdf.

Brass, Irina, Madeline Carr, Leonie Tanczer, Carsten Maple, and Jason Blackstock. 2017. Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles. In *Connected and Autonomous Vehicles: The Emerging Legal Challenges*, 8–9. London: Pinsent Masons. https://www.pinsentmasons.com/PDF/2017/Freedom-to-Succeed-AMT/Connected-autonomous-vehicles-report-2017.pdf.

Carr, Madeline. 2016. *US Power and the Internet in International Relations: The Irony of the Information Age*. Basingstoke: Palgrave Macmillan.

Department of Digital, Culture, Media and Sport, UK. 2018. *Secure by Design: Improving the Cyber-Security of Consumer Internet of Things Report.* London. Accessed December 28, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

Edwards, Lilian. 2018. *Data Protection: Enter the General Data Protection Regulation*. May 21. Accessed December 28, 2018. https://doi.org/10.2139/ssrn.3182454. Also in Lilian Edwards, ed. 2018. *Law, Policy and the Internet*. London: Hart Publishing.

Farkas, Thomas J. 2017. Data Created by the Internet of Things: The New Gold Without Ownership? *Revista La Propiedad Inmaterial* 23, Universidad Externado de Colombia (enero-junio): 5–17. https://doi.org/10.18601/16571959.n23.01.

Hartzog, Woodrow, and Evan Selinger. 2016. The Internet of Heirlooms and Disposable Things. *North Carolina Journal of Law & Technology* 17: 581–598.

IHS Markit. 2017. *The Internet of Things: A Movement, Not a Market*. Englewood, CO: IHS Markit. Accessed December 28, 2018. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf.

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

Roth, Sheryl. 2018. Buying or Selling a 'Smart Home'? Read This. *Federal Trade Commission*, January 3. Accessed December 28, 2018. https://www.consumer.ftc.gov/blog/2018/01/buying-or-selling-smart-home-read.

Schneier, Bruce. 2016. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company.

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

Tanczer, Leonie, Simon Parkin, Trupti Patel, and George Danezis. 2018a. *Tech Abuse Guide: How Internet-Connected Devices Can Affect Victims of Gender-Based Domestic and Sexual Violence and Abuse*. Accessed December 28, 2018. https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/gender-iot-tech-abuse.

———. 2018b. *Gender and IoT (G-IoT) Resource List*. Accessed December 28, 2018. https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/g-iot-resource-list.

———. 2018c. *Response by the "Gender and IoT" Research Team: The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT)*. Accessed December 28, 2018. https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/domestic-violence-consultation.

Tanczer, Leonie, John Blythe, Fareeha Yahya, Irina Brass, Miles Elsden, Jason Blackstock, and Madeline Carr. 2018d. *Summary Literature Review of Industry Recommendations and International Developments on IoT Security*. Department of Digital, Culture, Media and Sport, London. Accessed December 28, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686090/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf.

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet.* Berkeley: University of California Press.
Winseck, Dwayne. 2017. The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy* 7: 228–267.
Winseck, Dwayne, and Robert Pike. 2007. *Communication and Empire: Media Power and Globalization, 1860–1930.* Durham, NC: Duke University Press.

PART III

Questions of Truth and Censorship

Weaponising Copyright: Cultural Governance and Regulating Speech in the Knowledge Economy

Debora Halbert

Given the range and scope of cultural activities falling under the auspices of copyright, copyright functions as a kind of cultural governance in the modern age. Take, for example, the recent decision by U.S. District Judge Michael Fitzgerald regarding the copyright infringement case between pop star Taylor Swift and the R&B girl group 3LW. Judge Fitzgerald determined that Swift did not infringe the copyright to 3LW's song, *Playas Gon' Play* when she used the phrase "players gonna play, haters gonna hate" in her 2004 hit *Shake it Off* (CNBC 2018). Despite the same phrase (playas gonna play) being the title of the earlier work and despite the use of the specific phrase in Swift's song, Fitzgerald found the lyrics were not sufficiently original (Fitzgerald 2018). Citing a long history of songs using the words "player," "playa," "hater," and so on, Fitzgerald determined that by the time Swift used the lyrics, they were sufficiently embedded in myriad cultural references to be banal and, thus, not subject to copyright protection (Fitzgerald 2018). Judicially determining who can use what words and in what context is a form of cultural governance that

D. Halbert (✉)
University of Hawai'i at Mānoa, Honolulu, HI, USA
e-mail: halbert@hawaii.edu

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_8

shapes future cultural expression by regulating the content of past creativity. This case demonstrates that aesthetic and cultural decisions about creative work are subject to judicial scrutiny—and also, as this chapter will argue, censorship.

Copyright's use as a tool for censorship has recently entered public consciousness as a method to combat offensive speech. In this chapter, I specifically inquire into how copyright has been weaponised to police expression. Certainly, efforts to use copyright as a weapon of censorship are not new. As this chapter discusses, the efforts of *Gone With the Wind* author Margaret Mitchell's estate to stop the publication of *The Wind Done Gone* by Alice Randall or the removal from publication of the O.J. Simpson parody *The Cat NOT in the Hat* are two clear examples where copyright worked to censor speech (Ochoa 1997; *Suntrust Bank v. Houghton Mifflin Company* 2001). Additionally, numerous scholars have highlighted conflicts between free speech and copyright (Nimmer 1969; Tushnet 2004; Lange and Powell 2009; Tehranian 2011).

This chapter builds on existing work by investigating the political and cultural implications of regulating and sanctioning speech via a privatised knowledge system (copyright) and the implications for cultural governance and individual expression. After an exploration of copyright governance within the context of Susan Strange's knowledge structure framework, this chapter discusses free speech and cultural governance as a mode of censorship. I take up two recent examples where copyright was weaponised to curb speech. The first is an effort to control the speech of a controversial YouTube star. The second is an effort to curb the association of a cartoon character with white supremacy. In both cases, we see copyright performing a normative—not commercial—function, as copyright owners exert their control over their creative work to limit the expression of others. There is much to be troubled by regarding both the resurgence of white supremacy and the use of copyright to shape what can and cannot be expressed, as will be discussed in the conclusion.

1 The Knowledge Economy

Intellectual property (IP) and its regulation and control at the global level are central to understanding what Susan Strange calls the knowledge structure (Haggart, this volume). As part of the larger argument of this book, this chapter draws upon Susan Strange's structural assessment of International Relations to glean insights into how power within the modern entanglement

of nation-states operates. For Strange, state power is not about sovereign territory as much as it is about assuring a global hegemony, economically and politically.

To understand who has hegemonic power in the modern world, one must look at who has established the structures of global governance and economic decision making. Strange frames the knowledge structure not only as the power of holding knowledge but also as the power "to deny knowledge, to exclude others, rather than in the power to convey knowledge" (1989, 131). In other words, while we prioritise information sharing and the "marketplace of ideas" as concepts aligned with the democratic value of free speech, the knowledge economy is as much about barriers to access to information and structures to control the flow of information as it is about knowledge transfer. Copyright becomes a way of exerting such power within a knowledge structure shaped by a private property regime.

In a previous article (Halbert 2017), I used Strange's framework of the knowledge structure to understand the politics of international trade structures focused on intellectual property (IP). Here, I focus my attention on the cultural governance IP produces within Strange's knowledge structure as a function of private censorship and regulatory control.[1] Understanding copyright as a tool of censorship, meaning to keep works from being published or limiting expression through copyright infringement claims, helps demonstrate the power of the knowledge structure. Copyright functioning as censor can prevent the dissemination of knowledge or creative work, and it can help designate certain types of knowledge as illegitimate and remove it from circulation.

While we do not tend to think of it as censorship, conventional modes of publication and creative processes govern what gets published and circulated as intellectual and creative work. The cultural governance role played by editors, producers, and others who filter future creativity through the lens of corporate profitability are hidden from view or understood as legitimate gatekeepers, rather than censors. Their work is not understood as censorship, but indeed, they are censoring, not necessarily for political reasons, but for profitability, the key ideological framing for modern creative work within a capitalist economy. Within this model, "sophisticated creators," like the movie industry, are protected via the regulatory structure of copyright, while "unsophisticated creators," such

[1] I borrow the concept of cultural governance from Shapiro (2004), who situates culture within a broader political economy of power.

as those trying to produce fan-fiction events, are not (Tehranian 2011, 116–117). Sophisticated creators, in short, can exert censorial power over those they deem a threat to their IP.

Aside from any function played by the courts in regulating speech, platforms have now become de facto private regulators (Tusikov 2016). In addition to legislatively mandated notice-and-takedown processes, the end-user licensing agreements accompanying virtually all social media sites upon which most content is now posted—platforms such as YouTube, Facebook, and Twitter—create rules that can stifle and halt speech that potentially infringes copyright (Halbert 2009). These private regulatory regimes are now common globally. Often, the removal of content is done at the behest of a copyright owner or in response to complaints about offensive language or violent content. To that end, private regulation of speech can go even further than the government in limiting what constitutes acceptable expression in the information age. As speech is privatised and made subject to terms-of-service rules created by the media platforms upon which the speech resides, the decisions regarding how it can be regulated becomes private and less transparent.

Despite its grounding in commercial interests, copyright owners also shape what can and cannot be said, recorded, shared, and displayed, based upon what they feel ought to be the way their works are used. As technology has made sharing easier, copyright owners attempt to control what is uncontrollable. Thus, efforts to censor using copyright have flourished in ways big and small. There are large-scale lawsuits against unauthorised uses of Hollywood films, like the recent cease-and-desist letter that shut down a Harry Potter Festival in Chestnut Hill, Pennsylvania (Cantor 2018), and there are cease and desist orders against fan fiction, such as the recently settled suit against *Star Trek* fan film *Prelude to Axanar* (Gardner 2017). As will be clear in the following sections, copyright can be used to pursue non-monetary objectives that are more overtly designed to censor. And as the more recent cases, discussed in Sect. 3 illustrate, enforcement can move beyond trying to protect the commercial interests (though one could argue that being associated with white supremacy detracts from the commercial viability of a product) and is, instead, about using copyright to shape what can and cannot be said. In all of these cases, copyright is being used as a form of cultural governance.

2 Free Speech, Copyright, and Cultural Governance

The cases discussed in this chapter highlight conflicts between copyright and free speech, along with emphasising the global reach of U.S. law in the knowledge structure. According to Nimmer, the distinction between the protection of free speech and protection of copyright is that the use of "other people's speech" as your own is not free speech, but a copyright violation. Nimmer did not envision the mashup appropriation of today when, in 1969, he stated that "free speech as a function of self-fulfillment does not come into play. One who pirates the expression of another is not engaging in *self*-expression in any meaningful sense" (Nimmer 1969, 1192). One look at YouTube's many derivative works, fan fictions, and home videos set to copyrighted music is an indication of how important such works are to self-expression.

Copyright includes the right to control any reproduction, public performance, or derivative work made from the original. While the idea/expression dichotomy may protect creative works that follow similar storylines, copyright does not allow for an individual to use specific works created by others without authorisation. So, for example, fan fiction, which uses the characters and fictional worlds created by someone else, has long been a challenge to copyright owners (Tushnet 1997; Schwabach 2011; Hellekson and Busse 2006). By making what is called a derivative work, fan fiction violates copyright law, but to pursue fan-fiction authors too vociferously is to alienate a creator's most dedicated fan base. Despite using the characters and fictional places of others, fan fiction can be quite expressive and original in its own right (see, e.g., Edonohana 2010). One might argue that strictly enforcing copyright stifles these expressive works, and in many cases, copyright owners turn a blind eye. Certainly, that has been true for video gamers, as discussed later.

Then, there is the issue of parody, a creative form that requires substantive reference to an original in order to be relevant. Some of the clearest cases of censorship as prior restraint in free speech terms can be found in the case law here. One famous case, where the court's copyright decision resulted in the removal of a work from circulation, was the U.S. 9th Circuit decision prohibiting the production of the parody *The Cat NOT in the Hat!* by Dr. Juice, a parody that used the style of the late Dr. Seuss, who passed away in 1990, to comment on the 1995 O.J. Simpson double-

murder trial. The decision in this copyright case has been roundly criticised as having failed to protect important aspects of parody and criticism through the application of the fair use criteria in U.S. law (Ochoa 1997). The expression of an author was removed from public circulation because a court determined it infringed too much upon the copyrighted characters or style of a copyright owner.

Another example, though one that ultimately avoided the censoring power of copyright, was *The Wind Done Gone* by author and songwriter Alice Randall. *The Wind Done Gone* was published in 2001 after a protracted court battle with the Margaret Mitchell estate. When Houghton Mifflin published this retelling of *Gone with the Wind* from the perspective of the illegitimate biracial half-sister of Scarlett O'Hara, the Mitchell estate filed for copyright infringement. They claimed that Randall's book was an unauthorised sequel, that it copied characters and key dialogue from the book, and that it copied other important elements of the original plotline (*Suntrust Bank v. Houghton Mifflin Company* 2001, 1364). The Mitchell estate had strict rules for authorising any creative work using the characters or settings of *Gone with the Wind*. While Mitchell's book glorifies Southern traditions while minimising the negative consequences of slavery, Randall's book takes on miscegenation, race, and homosexuality while making a commentary on Mitchell's version of the antebellum South.

Copyright control was a barrier Randall most likely did not consider when writing her retelling of *Gone with the Wind*. The retelling of older stories is an important literary tradition and one that has produced interesting new works (Frus and Williams 2010). That copyright could halt the publication of a book is telling of its power to censor and its ability to exert cultural governance. Controlling the publication of a book speaks to the clearest form of censorship the U.S. First Amendment is designed to halt. However, despite the role copyright law played in initially keeping the book from being published, the private nature of the parties involved meant issues of free expression were not relevant.

This brief foray into free speech and the power of copyright to censor is important for understanding the newest battles along the free speech/copyright infringement divide. These more recent cases have to do not with halting parody or other new works but rather with how one might weaponise copyright to fight racism. The argument here is that copyright is a form of cultural governance within the modern knowledge economy.

3 Weaponising Copyright…

3.1 …to Fight Offensive Appropriation on YouTube

PewDiePie, aka Felix Kjellberg, is an enormously successful YouTube star who has built the most-subscribed YouTube channel in the world by streaming his multiuser video game play, in addition to streaming other antics and commentary to an audience of over 65 million subscribers (as of September 2018) (Lewis 2018). With a reported net worth of $61 million, he has leveraged his YouTube success in a way virtually unparalleled (Lewis 2018). PewDiePie may, in part, be popular, or at least notorious, because of his alt-right flirtations, his racist jokes, and his general irreverence. The *New York Times Magazine* astutely sums up PewDiePie's YouTube presence:

> Kjellberg had, either instinctively or intentionally, constructed a political identity as YouTube's insider class-traitor, raging against a system that's—*trust him, but also he's just joking, but he would know*—totally rigged. Now he is sketching out what a far more toxic YouTube politics of *ressentiment* might look like, under the threadbare cover of ironic bigotry, the recent history of which is worryingly instructive. (Herrman 2018)

In other words, PewDiePie exemplifies concerns about racism in video gaming culture and, despite some effort to disavow the affiliation, is now linked with alt-right trolls that play a substantial role in gaming culture. PewDiePie would like to have it both ways—pretend to disavow his racism while embracing the language of white supremacy. Herrman, summing up his approach to white supremacy states, "Even as farce, Kjellberg's performance has been illustrative…." (Herrman 2018). Herrman goes on to quote alt-right game designer Vox Day, "If Pewdiepie wasn't #AltRight before, … he is now" (Herrman 2018).

One does not have to look far into his oeuvre to find examples of racist, anti-Semitic commentary. In February 2017, PewDiePie was dropped from a Walt Disney contract and from the YouTube Red programming option, which allows viewers to pay for ad-free viewing, for posting anti-Semitic and Nazi-related videos (Winkler et al. 2017). In one video, PewDiePie has two Sri Lankan men holding up a sign that says "Death to All Jews" and another included a man playing Jesus saying that Hitler was right (Winkler et al. 2017). PewDiePie defended his actions by simply

saying they were intended to be humorous. When the man playing Jesus had his account suspended, PewDiePie's stated that he found it ironic that "Jews had found another way to fuck Jesus over again." Both his "jokes" and his response have made PewDiePie a Nazi favourite, according to Neo-Nazi newspaper *The Daily Stormer* (Winkler et al. 2017).

PewDiePie ignores his own complicity in the production and distribution of racist videos, as well as failing to take responsibility for amplifying racist messages for his own personal profit. As one of the world's most popular vloggers, he appears to be willing to play to politically violent and racist sentiments to make money. He appears unwilling to understand how his words reinforce anti-Semitism and racial hatred globally.

The racist videos described here are the backdrop for a more recent controversy generated by PewDiePie. PewDiePie rose to popularity because of his ability to play video games. "Let's Play" streaming uses the copyrighted graphics and characters of a video game while juxtaposing the player's voice and commands to create a specific gaming experience. Gamers tune in to understand how to work through specific parts of a game and also to hear the in-game chatter of the players. As gaming lawyer Mona Ibrahim (2017) has stated, the permissiveness of the gaming world has led many to confuse "permissive use," a social concept, with "fair use," a concept based in U.S. law. Permissive use, as understood in this context, is when a copyright owner allows for copyright-infringing activity even if they could legally stop the infringement. Fair use, by contrast, are the legally codified exceptions to strict copyright enforcement that can be found in the law. Generally speaking, "Let's Play," while technically being an unauthorised public performance of a copyrighted work and/or an unauthorised derivative work, has been allowed by copyright owners.

Ibrahim goes on to note:

> all intellectual property law is censorship in some way, shape or form. It's designed to allow copyright owners an opportunity to prevent others from using their content. If my clients elect to permit streaming, that's a business decision and has little to do with any perceived claim of fair use by the Let's Play community. (Ibrahim 2017)

The ultimate boundary between fair use and copyright infringement in the gaming world is unclear. According to gaming journalists, how much and what gamers are allowed to upload ranges from entire play through videos to specific sequences (Hernandez 2017a). Within this context, in

September 2017, PewDiePie was playing the online multiplayer game *PlayerUnknown's Battlegrounds* (*PUBG*) when he recorded and live streamed himself shouting, "What a fucking nigger" (Charity 2017). Because of the scope of his audience, his social network immediately amplified his words.

Upon hearing of PewDiePie's most recent racist remarks, the owner of the game *Firewatch*, Sean Vanaman, issued a statement via Twitter that he was filing a complaint against PewDiePie using the U.S. *Digital Millennium Copyright Act* (DMCA). Under the DMCA's notice-and-takedown provisions, if a copyright owner notifies an online platform such as YouTube of possible copyright infringement, in order to avoid contributory liability, the company must take the potentially offending content down (Gordon 2017). Materials that allegedly infringe copyright must be removed if there is "a good fair belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law" (17. U.S.C. 512 (C)(3)(V)).

It is important to note that *PUBG* is a separate game owned by a different company. PewDiePie also streams content of himself playing *Firewatch*, and so this complaint mandated the removal of all streaming videos on his YouTube Channel for *Firewatch*, even though the offensive speech happened in a different game. In an even more unusual move, Vanaman issued a statement to other game owners: "I'd urge other developers & will be reaching out to folks much larger than us to cut him off from the content that has made him a millionaire" (Charity 2017). Vanaman, in a tweet, framed his actions as a legitimate method of controlling a commercial product: "Freedom of speech is freedom of prosecution[.] His stream is not commentary, it is ad growth for his brand. Our game on his channel =endorsement" (Hernandez 2017a). Vanaman followed through with his notice-and-takedown request and YouTube approved the DMCA takedown request.

This DMCA threat is not just about this one video but should be seen in the context of the role copyright owners might play in limiting offensive speech using their video game platforms. YouTube's terms of service have been shaped by the DMCA, and while not part of U.S. law, according to YouTube policies, if you receive three copyright infringement strikes, you can be removed from YouTube, a significant economic threat to an online gamer whose channel and viewers are how he made his millions. Vanaman may have been the first to use copyright over a gaming platform to halt offensive behaviour. Generally, game platform owners have been fairly generous to Let's Play streaming (Robertson 2017a), but using the DMCA in this manner was fairly easy to do and easy to replicate.

Vanaman's takedown of the PewDiePie streaming video is unmistakably a case where copyright law was used to punish a speech act because of its offensiveness. Vanaman was clear about his intent—to use copyright to censor the speech of another. While a full analysis under U.S. copyright law's fair use provisions will have to wait for a case to be brought to court, Vanaman's actions suggest that game platforms, and the advertisers that have their ads associated with folks like PewDiePie, may have reached the end of their tolerance for racist speech. Vanaman's actions also demonstrate that tools do exist for gaming companies and internet platforms to sanction and limit such speech, something that—until recently—they have been hesitant to do. While the "community standards" of the gamers themselves appear to be very low, the corporations who seek to attract new gamers may need to make a calculation about how much racism, sexism, and intolerance the larger population will tolerate and still use their products.

PewDiePie remains on YouTube, with over 65 million followers. Vanaman's game was review-bombed by PewDiePie fans who were unhappy with the effort to censor him for his speech using the DMCA (Hood 2017). Furthermore, Ben Fritz, who had the third byline on the *Wall Street Journal* article and video breaking the story about the earlier racist remarks and activities has been relentlessly harassed by PewDiePie fans (Hernandez 2017b). While PewDiePie did apologise for both his use of the n-word and for his seeming endorsement of the August 2017 Nazis' march in Charlottesville, Virginia, calling himself "extremely immature and stupid," he also remains largely ignorant of why his actions might be problematic (Romano 2017a). At a personal level, it is also clear that both he and his fan base are willing to position him as a victim and reproduce the casual racism that has come to be associated with many gamers.

Recent YouTube changes to their terms of service may have an impact on PewDiePie's ad revenue if he strays too far into offensive territory again (Hills 2018). In the wake of increasing revelations about how Russians used social media to introduce additional divisiveness into the American Presidential election of 2016, one of the largest advertisers, Unilever, has said that if social media platforms cannot get a handle on the hate speech, sexism, and racism that pervades their sites, then advertising money will be pulled (Ray 2018). Google already regulates for copyright infringement by demoting sites so far down a search list that they will rarely be found, effectively rendering them invisible in what Pasquale argues is "swift, secret, and arbitrary" justice (2015, 94–95).

The reason PewDiePie serves as an example of cultural governance within the knowledge economy is the role the knowledge economy plays in shaping the global ground rules on which content is served and upon which copyright claims are made. Companies such as YouTube are difficult to conceive of as anything but global. The platform hosts videos from around the world and PewDiePie exemplifies this global positioning with an audience spanning multiple continents. Despite this global reach, it is the American DMCA that serves as the basis upon which a legal claim of copyright infringement is made and through which YouTube responds. From a legal standpoint, one might simply suggest that the DMCA is relevant because YouTube's headquarters are in California and the company is American; therefore, there is nothing unusual about applying American law to this scenario. That analysis conceals the global power of American law to shape what can and cannot be said, what is and is not viewable, what remains online, and what is taken down. As mentioned earlier, it puts PewDiePie in a position of being held accountable to YouTube's policies and procedures which are framed by the American legal system. Such is the nature of power in the knowledge structure. As Strange noted in 1995, "it is the markets, not the enterprises, that are multinational" (1995, 79).

3.2 …to Fight White Supremacy

The path taken by Pepe to white supremacy is somewhat convoluted. When Matt Furie created the graphic novel *Boy's Club* in 2006, the ultimate fate of one of its characters was most likely inconceivable. Pepe the Frog originated as a slacker known for peeing on stuff and saying, "Feels good man." Pepe became a popular internet meme sometime in 2008 (Mullin 2017). It was tweeted and retweeted by pop stars such as Katy Perry and found its home on internet chat sites such as 4chan and Reddit (Weissmueller 2017). While these were technically copyright violations, Furie has indicated he did not initially oppose the unauthorised use of Pepe (Mullin 2017).

Pepe became identified with Donald Trump when his son, Donald Trump Jr., retweeted a meme that placed Pepe alongside other Republicans in a graphic that switched the heads on a poster for the movie *The Expendables* with the word "deplorables." The graphic was designed in response to Hillary Clinton's statement that half of Trump voters were a "basket of deplorables" (Givens 2016).

In parallel with Pepe's appearance in the Trump campaign, the Pepe meme also became a symbol for white supremacists. While the specific steps to becoming a white supremacist symbol are unclear, it likely began when the Pepe "sad frog meme" was transmogrified using swastikas, Klan hoods and the like via 4chan and Reddit (Beschizza 2016). As *Boing Boing* writer Rob Beschizza poetically puts it, "Pepe slid the rage-greased chute of chan culture into the toilet of offensive memes and popped up on the other side in the Anti-Defamation League's archives. There, he takes his place beside the swastika and the Confederate flag" (2016). Pepe was named as a hate symbol by the Anti-Defamation League in September 2016 (Chia 2017a).

In a 2016 interview with *The Atlantic*, Furie indicated that he was not bothered by the appropriation of Pepe by conservatives because he saw it as "just a phase." Rather, he wanted to focus on the positive appropriations that had occurred and Pepe's link to youth culture (Serwer 2016). However, since that interview, his view changed. Furie initially tried to "kill" Pepe by creating a storyline where Pepe dies to stop the right-wing memes, but memes are more powerful than comic book death—Pepe continued on as a meme (Chia 2017a). Having failed to kill off his creation, Furie began his legal effort to reclaim his creation by exerting his rights as a copyright owner.

The law firm Wilmer Cutler Pickering Hale and Dorr, working pro bono, supported Furie's efforts to control his copyrighted work. While the goal was to disassociate Pepe from white supremacy generally, they targeted the removal of Pepe images used in a commercial context by copyright-infringing white supremacists and conservatives. Prominent white supremacists using Pepe were sent cease and desist letters. This new effort to control Pepe is summarised by *Reason* blog writer Zach Weissmueller as a conflict that "is at the center of an important First Amendment battle in an era of unlimited replication, imitation, and mutation" (Weissmueller 2017).

One of the first to be targeted with copyright infringement was Eric Hauser, the author of *The Adventures of Pepe and Pede*, a children's book about a frog and a centipede. Hauser's book details the efforts of Pepe and Pede to fight a bearded alligator named Alkah who has been vanquished to a nearby pond on Wishington Farm. Once the copyright infringement case raised the visibility of the book, even though Hauser claimed he was not part of the alt-right, the book became immediately controversial (Wootson 2017). Hauser was removed from his position as assistant principal at the middle school where he worked. He admitted infringing the

copyright to Pepe and settled with Furie. According to the settlement, the book was removed from sale, all further sales have been prevented, and Furie required that all proceeds from the book ($1521.54 in profits) be donated to the Council on American-Islamic Relations (Gault 2017a).

Through his lawyers, the gauntlet of control over Pepe was thrown down. In a formal statement, they said,

> Furie wants one thing to be clear: Pepe the Frog does not belong to the alt-right. As this action shows, Furie will aggressively enforce his intellectual property, using legal action if necessary, to end the misappropriation of Pepe the Frog in any way that espouses racism, white supremacy, Islamophobia, anti-Semitism, Nazism, or any other form of hate. He will make sure that no one profits by using Pepe in alt-right propaganda—and particularly not by targeting children. (Gault 2017a)

Furie's use of copyright to selectively focus on right-wing content is what the U.S. Supreme Court would call content or viewpoint discrimination. However, private individuals using copyright are free to censor as they choose: copyright owners can choose what to authorise and what to restrict.

While Hauser settled quickly, other alt-right users of the Pepe meme have been less willing to cease and desist. Furie issued cease and desist letters against white nationalist leader Richard Spencer, alt-right media commentator Mike Cernovich, and Tim Gionet, who goes by the internet name Baked Alaska (Romano 2017b). The letter sent to Gionet states that "your use of Pepe the Frog in connection with your promotion of hate is unauthorized and unacceptable. Pepe is a peaceful frog who represents togetherness and fun—not hate" (Gault 2017b, quoting the cease and desist letter by attorney Louis W. Tompros). Baked Alaska has used Pepe without authorisation in several of his commercial products, including a video game called *Build the Wall: A Game* and in his book *Meme Magic Secrets Revealed*. The letter concludes that once infringement has ceased, Baked Alaska will be contacted to deal with the question of damages and payment for the unauthorised use of Pepe.

Similar letters were sent to other white supremacists that have appropriated Pepe for political and commercial purposes. The lawyer for Mike Cernovich replied, "should you file a suit against Mr. Cernovich, we will be delighted to embarrass the fuck out of you" (Romano 2017b). Cernovich and his lawyers make the argument that their use of Pepe is transformative and also that because the use is for political commentary

and satire, it is protected under fair use (Cernovich 2017). Despite the bluster, Cernovich's lawyer announced that he had removed the Pepe images "at his discretion," but that he reserved the right to publish other Pepe related works as fair use (Gault 2017c). The fair use claims are yet to be determined and will be subject to legal analysis if a case makes it to the trial phase. Richard Spencer, a white supremacist who popularised the term "alt-right," has also appropriated Pepe. As Richard Spencer said of his use of Pepe, "the artist isn't in control of his work once it enters the culture in the way it has" (Chia 2017b).

The cease and desist letters have led to many of the referenced links being cut so that the platforms upon which this content is based are not found liable as contributors to the infringement (Gault 2017b). So far, Google, Reddit, Redbubble, and Amazon have been sent DMCA notice-and-takedown requests and have complied by removing the infringing material (Romano 2017b). The game developer for the pro-Trump game *Make America Great Again: The Trump Presidency* removed its for-purchase emoticons of Pepe at the behest of the service provider Steam (Robertson 2017b). Because the DMCA allows for third-party protection from liability for copyright infringement if the procedures for taking materials down at the copyright owner's request are followed, even if the white supremacists themselves wish to challenge the claim of copyright infringement, their materials may be removed while this challenge moves forward. Even so, the response across the internet was to produce even more alt-right Pepe memes (Gault 2017c).

4 Tackling the Tough Questions

Does the use of Pepe by white supremacists and Donald Trump supporters violate copyright law, or could it be understood as fair use? What role, if any, should the hateful nature of the speech in question play in our thinking about the appropriate use of copyright in these instances? What about PewDiePie's live streaming game play? These cases open an opportunity to ask tough questions about the boundary between copyright and expression. Lange and Powell suggest that something appropriated with the intent of creating a new transformative work will be provided a more generous fair use reading than something that does not add anything new (2009, 49). However, they go on to suggest that fair use is an inadequate defence because it relies upon the opinion of a judge to determine what is sufficiently transformative (Lange and Powell 2009, 97).

In this case, some commentators argue the uses of Pepe by the alt-right have not been transformative, and thus, would not be considered fair (Mullin 2017). Furie clearly holds the copyright and the use of Pepe without authorisation for commercial purposes is an infringement of Furie's copyright. White supremacists, Trump supporters, and other extreme-right individuals who have appropriated Pepe have not changed the image—they simply traced the character in recognisable ways and thrust him into new situations. Thus, the use is not transformative, but instead, it appropriates the character of the frog for new commercial purposes, purposes with which the original creator disagrees. It could also be argued that even if the appropriation of Pepe is transformative, Pepe's new relationship with white supremacy will have a negative impact upon the market for the original work and thus is not fair (Ochoa 1997, 606, citing *Campbell*, suggests that if there is a "reasonably substantial" impact on the market of the original, then it cannot be a fair use). It is safe to say that once aligned with white supremacy, other possible uses for the Pepe character are tainted in such a way as to become unusable.

Others, however, are not so sure that the alt-right use of Pepe is unprotected. Citing Electronic Frontier Foundation fair use expert Mitch Stoltz, *Vox* questioned if the act of transforming Pepe from a stoner-peace-loving frog to a right-wing white supremacist frog was not intrinsically transformative (Mullin 2017). While the character is the same, its alignment with white supremacists and Trump-supporting identity politics is such that it plays an essential and thus transformative role in the meaning of the character. The characters in *The Wind Done Gone* were based upon the original and it was ultimately published. The "transformation" in *Prince v. Cariou* used the exact same pictures and added a few new items (*Cariou v. Prince* 2013)—so it is conceivable a court might see adding a swastika to the Pepe meme as transformative, given the political nature of the commentary.

Furthermore, using copyright to halt a mode of expression is suspect. In his analysis of the fair use dimensions related to the parody book *The Cat NOT in the Hat!*, Professor Ochoa notes that "if the copyright holder seeks to suppress the unauthorized use not to protect his or her own works from economic competition, but to suppress the third-party's point of view, that is an improper purpose that conflicts with the goals of both copyright and the First Amendment" (Ochoa 1997, 607). In this case, it might be difficult to distinguish between protecting a work from economic competition (Pepe becomes useless for non-white supremacist

uses) and viewpoint suppression, given that Furie via his lawyers has already indicated he seeks to suppress the use of the frog because it has been adapted to a political viewpoint he rejects.

But for the fact the defendants are white supremacists, those who advocate for a broader sense of fair use (myself included) may find themselves arguing this use is fair. Tehranian notes that identity is increasingly aligned with the use of unauthorised derivative works that "inevitably mingle elements of ourselves with the copyrighted works of others to create the mélange that represents self-definition in the twenty-first century" (2011, 64–65). Lange and Powell argue that freedom to appropriate is essential to the type of First Amendment expression rights we expect in the United States (2009, 175). Under this view, Pepe's use by white supremacists is a key factor in their twisted identity politics and would constitute a transformative work. For Tehranian, transformative uses should be exempt from copyright control and there should be some sort of intermediate liability standard created (2011, 156). This is a view I found compelling until faced with the racist appropriation of a character as the litmus test of expression.

Even under Tehranian's standard, the use of Pepe might not be fair. He notes, "thus, slavish imitation of a copyrighted work, even if accomplished with great skill, would not qualify as transformative. But, even vulgar transmogrifications of a copyrighted work, if infused with creative and original elements, would qualify" (Tehranian 2011, 161). In this case, it is not clear if Pepe's appropriation is a "slavish imitation" or a "vulgar transmogrification." A court would have to make this decision.

It looked as if we would see what a court would decide because one artist sued by Furie initially seemed keen on taking her case to trial. Jessica Logsdon initially refused to take down her artwork featuring Pepe (*Matt Furie v. Jessica Logsdon* 2017). Instead of taking them down, she initially argued that her rights to expression and her religious rights as a Kekistanian (a bizarre right-wing religious affiliation that has sprung up around Pepe and Trump) had been violated by Furie's copyright claims (Gault 2017d). However, she did ultimately settle in March 2018 and she agreed to remove her oil paintings from eBay (Kunzelman 2018). In a world of appropriation and cultural mashups, the boundaries of ownership, many argue, should flow more freely. Of course, this argument was made without the rights of white supremacists in mind.

5 Conclusion

Copyright as a form of cultural governance defines the scope of creative appropriation in the modern information age. Despite claims that copyright is consistent with free speech, there is ample evidence that it can be used to halt or regulate speech with which the copyright owner disagrees. Of course, such control is private action, not government censorship, and so, copyright can be used to stop what some governments cannot—hate speech, racist speech, and other offensive speech. When a private platform controls the gateway to public speech, a different calculation can be made, since free speech does not apply to the rules of engagement required in private spaces.

Weaponising copyright and shifting regulatory control to private platforms are powerful tools in defining the scope of appropriate speech. The fights over censorship via copyright law put into visible contrast the power of IP to act as a form of cultural governance, shaping creative work as private property and shifting the regulatory power to authorise speech out of the public sphere and into the private. We may celebrate the effort to curb hate speech; however, the vast majority of copyrighted works are corporately owned and controlled, and this private power suggests an even more wide-ranging form of censorship and control. We should be concerned about how expression and thought are governed in the information age and question the role private networks have in structuring knowledge production and power.

In many ways, the clarion call of free speech is nothing but a legal fiction. All speech has consequences and it should come as no surprise that racist speech is met with resistance. It is simply not the case that something called "free speech" happens in a vacuum, nor that simply because words are uttered, they cannot be countered, argued against, resisted, or sanctioned. A right to say something does not automatically mean that statement stands as a discrete act, but rather, it is simply one statement in a vast ongoing conversation. To pretend we do not live within a socially constructed world where statements can generate punitive consequences is to embrace a form of entitled speech that implies one should not ever be corrected or argued with. The cases discussed here make visible the uncomfortable tension between an abstract jurisprudence of free speech and the normative world of creating a tolerant society. In highlighting how cultural governance works through copyright, it is important to note that while predominantly about securing a stable commercial enterprise

for the culture industry, copyright can also function (and has functioned) to curb the speech of others—along normative lines of social life. We can argue about if copyright as censorship is good or bad, but first we have to acknowledge that it is happening.

References

17. U.S.C. 512 (C)(3)(V).

Beschizza, Rob. 2016. Pepe the Frog Listed Among Common Hate Symbols by Anti-Defamation League. *Boing Boing*, September 28. https://boingboing.net/2016/09/28/pepe-the-frog-listed-among-com.html.

Cantor, Andrea. 2018. Chestnut Hill Transforms 'Harry Potter Festival' into 'Witches & Wizards' Following Warner Bros Cease-and-Desist. *Philadelphia Weekly*, September 24. http://www.philadelphiaweekly.com/news/chestnut-hill-transforms-harry-potter-festival-into-witches-wizards-following/article_db9a7898-bd08-11e8-9375-a38b30d798ef.html.

Cariou v. Prince. 2013. 714 F.3d 694. 2d Cir.

Cernovich, Mike. 2017. Hillary Clinton's Lawyers Threatens Mike Cernovich with Frivolous Pepe Lawsuit (UPDATE). *Medium* (blog), September 18. https://medium.com/@Cernovich/wilmer-hale-threatens-mike-cernovich-with-frivolous-pepe-lawsuit-6e2b580798df.

Charity, Justin. 2017. Can Copyright Law Bring Down PewDiePie? *The Ringer*, September 11. https://www.theringer.com/2017/9/11/16292206/pewdiepie-racism-gaming-dmca-shift.

Chia, Jessica. 2017a. Matt Furie Kills Off Pepe the Frog After Hate Symbol Use. *Daily Mail Online*, May 9. http://www.dailymail.co.uk/news/article-4487364/Pepe-croaks-Cartoonist-kills-frog-turned-hate-symbol.html#ixzz4wOtBl1HI.

———. 2017b. Matt Furie Kills Off Pepe the Frog After Hate Symbol Use | Daily Mail Online. *Daily Mail*, May 9. http://www.dailymail.co.uk/news/article-4487364/Pepe-croaks-Cartoonist-kills-frog-turned-hate-symbol.html.

CNBC. 2018. Taylor Swift Gets Copyright Lawsuit Over 'Shake It Off' Thrown Out. February 14. https://www.cnbc.com/2018/02/14/taylor-swift-shakes-off-copyright-lawsuit-over-hit-song.html.

Edonohana. 2010. *No Reservations: Narnia*. https://archiveofourown.org/works/137185.

Fitzgerald, Michael W. 2018. *Hall v. Swift*. U.S. District Court, Central District of California. https://www.scribd.com/document/371458324/Hall-v-Swift-Dismissal.

Frus, Phyllis, and Christy Williams, eds. 2010. *Beyond Adaptation: Essays on Radical Transformations of Original Works*. Jefferson, NC and London: McFarland & Company, Inc.

Gardner, Eriq. 2017. CBS, Paramount Settle Lawsuit Over 'Star Trek' Fan Film. *The Hollywood Reporter*, January 20. https://www.hollywoodreporter.com/thr-esq/cbs-paramount-settle-lawsuit-star-trek-fan-film-966433.

Gault, Matthew. 2017a. Pepe the Frog's Creator Gets Alt-Right Children's Book Pulled, Vows to 'Aggressively Enforce His Intellectual Property.' *Motherboard*, August 28. https://motherboard.vice.com/en_us/article/ywwxj7/pepe-the-frogs-creator-gets-alt-right-childrens-book-pulled-vows-to-aggressively-enforce-his-intellectual-property.

———. 2017b. Here Are the Letters That Pepe the Frog's Lawyers Sent to the Alt Right. *Motherboard*, September 18. https://motherboard.vice.com/en_us/article/ne7nzz/here-are-the-letters-that-pepe-the-frogs-lawyers-sent-to-the-alt-right.

———. 2017c. The Great Meme War II: Amid Lawsuit Threats, the Alt-Right Says Pepe Belongs to Them – Motherboard. *Motherboard*, September 19. https://motherboard.vice.com/en_us/article/a3kvmk/the-great-meme-war-ii-amid-lawsuit-threats-the-alt-right-says-pepe-belongs-to-them?utm_campaign=sharebutton.

———. 2017d. This Is the First Copyright Infringement Lawsuit Filed Against a Pepe Meme Maker. *Motherboard*, October 5. https://motherboard.vice.com/en_us/article/xwgpkq/pepe-copyright-lawsuit-matt-furie-jessica-logsdon.

Givens, Orgie. 2016. Trump, Clinton, and the Deplorable Picture. *The Advocate*, September 14. https://www.advocate.com/election/2016/9/14/trump-clinton-and-deplorable-picture.

Gordon, Rob. 2017. PewDiePie Copyright Strike from Firewatch Dev Accepted. *Game Rant*, September. https://gamerant.com/pewdiepie-copyright-strike-firewatch/.

Halbert, Debora J. 2009. Public Lives and Private Communities: The Terms of Service Agreement and Life in Virtual Worlds. *First Monday* 14 (12): Online.

———. 2017. The Curious Case of Monopoly Rights as Free Trade: The TPP and Intellectual Property and Why It Still Matters. *Journal of Information Policy* 7: 204–227.

Hellekson, Karen, and Kristina Busse. 2006. *Fan Fiction and Fan Communities in the Age of the Internet: New Essays*. Jefferson, NC: McFarland.

Hernandez, Patricia. 2017a. Indie Dev Calls for Copyright Strikes Against Pewdiepie After He Says N-Word on Stream. *Kotaku*, September 10. https://kotaku.com/indie-dev-calls-for-copyright-strikes-against-pewdiepie-1803099736.

———. 2017b. The Pewdiepie Fiasco, One Month Later. *Kotaku*, March 24. Accessed July 14, 2018. https://kotaku.com/the-pewdiepie-fiasco-one-month-later-1793308126.

Herrman, John. 2018. YouTube's Monster: PewDiePie and His Populist Revolt. *The New York Times Magazine*, February 16. https://www.nytimes.

com/2017/02/16/magazine/youtubes-monster-pewdiepie-and-his-populist-revolt.html.

Hills, Megan C. 2018. YouTube Outlines New Official Punishments for 'Egregious Cases.' *Forbes*, February 19. Accessed February 24, 2018. https://www.forbes.com/sites/meganhills1/2018/02/19/new-youtube-rules/.

Hood, Vic. 2017. Firewatch Review-Bombed Following PewDiePie Racism Incident. *Eurogamer* (blog), September 19. https://www.eurogamer.net/articles/2017-09-19-firewatch-steam-review-bomb-pewdiepie-racism-incident.

Ibrahim, Mona. 2017. Firewatch Creators Can Target PewDiePie with DMCA Takedowns, and It's Perfectly Legal – Polygon. *Polygon*, September 12. https://www.polygon.com/2017/9/12/16295412/pewdiepie-campo-santo-firewatch-dmca-legal-abuse.

Kunzelman. 2018. Settlement Resolves Lawsuit over Pepe the Frog Paintings. *The Spokesman-Review*, March 9. Accessed March 20, 2019.

Lange, David, and Jefferson Powell. 2009. *No Law: Intellectual Property in the Image of an Absolute First Amendment*. Stanford, CA: Stanford Law Books.

Lewis, Rebecca. 2018. PewDiePie Challenges T Series to Battle as They Threaten YouTube Crown. *Metro News*, September 3. Accessed October 23, 2018. https://metro.co.uk/2018/09/03/pewdiepie-may-be-about-to-lose-his-crown-as-most-subscribed-youtube-channel-7907515/.

"Matt Furie v. Jessica Logsdon." 2017. Complaint Case 4:17-cv-00828-DW. In the United States District Court for the Western District of Missouri. https://assets.documentcloud.org/documents/4067613/Furie-Complaint.pdf.

Mullin, Joe. 2017. Is the Alt-Right's Use of Pepe the Frog 'Fair Use?' *Ars Technica*, September 24. https://arstechnica.com/tech-policy/2017/09/is-the-alt-rights-use-of-pepe-the-frog-fair-use/.

Nimmer, Melville B. 1969. Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press. *UCLA Law Review* 17: 1180.

Ochoa, Tyler T. 1997. Dr. Seuss, the Juice and Fair Use: How the Grinch Silenced a Parody. *Journal of the Copyright Society of the U.S.A.* 45: 546–633.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge and London: Harvard University Press.

Ray, Siladitya. 2018. Unilever Threatens to Pull Ads from 'Toxic' Online Platforms. *MediaNama* (blog), February 13. https://www.medianama.com/2018/02/223-unilever-online-ads-threat/.

Robertson, Adi. 2017a. Why Was It So Easy to Weaponize Copyright Against PewDiePie? *The Verge*, September 12. https://www.theverge.com/2017/9/12/16287688/pewdiepie-racism-firewatch-campo-santo-dmca-copyright-ban.

———. 2017b. Steam Purges Pepe Emoticons After Copyright Complaint – The Verge. *The Verge*, December 15. https://www.theverge.com/2017/12/15/16781768/steam-pepe-emoticon-banned-matt-furie-copyright-complaint.

Romano, Aja. 2017a. YouTube Start PewDiePie Used the N-Word in a Live Stream, After Months of Denying He's Racist. *Vox* (blog), September 11. https://www.vox.com/culture/2017/9/11/16288826/pewdiepie-n-word-playerunknown-battlegrounds.

———. 2017b. Pepe the Frog vs. Copyright Law Has Troubling Fair Use Implications. *Vox*, September 21. https://www.vox.com/culture/2017/9/21/16333162/pepe-the-frog-alt-right-dmca-takedown-fair-use-matt-furie.

Schwabach, Aaron. 2011. *Fan Fiction and Copyright: Outsider Works and Intellectual Property Protection*. Farnham: Ashgate Publishing, Ltd.

Serwer, Adam. 2016. It's Not Easy Being Meme. *The Atlantic*, September 13. https://www.theatlantic.com/politics/archive/2016/09/its-not-easy-being-green/499892/.

Shapiro, Michael J. 2004. *Methods and Nations: Cultural Governance and the Indigenous Subject*. New York and London: Routledge.

Strange, Susan. 1989. Toward a Theory of Transnational Empire. In *Global Changes and Theoretical Challenges: Approaches to World Politics for the 1990s*, 161–176. Lexington: Lexington Books.

———. 1995. The Defective State. *Daedalus* 124 (2): 55–74.

Suntrust Bank v. Houghton Mifflin Company. 2001. F3d 268 F3d 1257 1257. United States Court of Appeals for the Eleventh Circuit.

Tehranian, John. 2011. *Infringement Nation: Copyright 2.0 and You*. New York: Oxford University Press.

Tushnet, Rebecca. 1997. Legal Fictions: Copyright, Fan Fiction, and a New Common Law. *Loyola of Los Angeles Entertainment Law Journal* 17 (3): 651–686.

———. 2004. Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It. *Yale Law Journal*: 535–590.

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. 1st ed. Oakland, CA: University of California Press.

Weissmueller, Zach. 2017. Who Owns Pepe the Frog? The Alt-Right vs. Cartoonist Matt Furie: New at Reason – Hit & Run. *Reason.Com*, December 4. http://reason.com/blog/2017/12/04/who-owns-pepe-the-frog-the-alt-right-vs.

Winkler, Rolfe, Jack Nicas, and Ben Fritz. 2017. Disney Severs Ties with YouTube Star PewDiePie After Anti-Semitic Posts. *Wall Street Journal*, February 14, sec. Tech. https://www.wsj.com/articles/disney-severs-ties-with-youtube-star-pewdiepie-after-anti-semitic-posts-1487034533.

Wootson, Cleve R., Jr. 2017. An Assistant Principal Wrote a Children's Book About Alt-Right Mascot Pepe the Frog. It Cost Him His Job. *Washington Post*, August 15, sec. Education. https://www.washingtonpost.com/news/education/wp/2017/08/15/an-assistant-principal-wrote-a-childrens-book-about-alt-right-mascot-pepe-the-frog-it-cost-his-job/.

Disinformation and Resistance in the Surveillance of Indigenous Protesters

Jenna Harb and Kathryn Henne

Susan Strange (1994) brings attention to the relationship between knowledge and power—namely, that knowledge is an integral means of maintaining and achieving authority. Although mainstream International Political Economy (IPE) examines the roles of state and non-state actors in its focus on "production, trade, and finance" (Haggart 2017, 176), scholars sometimes lose sight of knowledge. As other contributors to this book have argued, our data-driven world renders the regulation of knowledge as increasingly important, perhaps over and above the other forms of structural power. The state can wield significant power to legitimise and delegitimise knowledge, with notable consequences for peoples who live

J. Harb (✉)
University of Waterloo, Waterloo, ON, Canada
e-mail: jiharb@uwaterloo.ca

K. Henne
University of Waterloo and Balsillie School of International Affairs, Waterloo, ON, Canada

Australian National University, Canberra, ACT, Australia
e-mail: khenne@uwaterloo.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_9

within its territorial bounds. In this chapter, we ask: what are the implications of national tactics of knowledge control for groups historically marginalised by the state?

In particular, we examine how the control of knowledge works to sustain settler colonial states. By settler colonial states, we mean states established through acts of settling upon Indigenous peoples' lands and claiming them as their own (Rowe and Tuck 2017). Through a focus on state surveillance of Indigenous resistance in Canada and the United States (Turtle Island[1]), we consider how information is employed to suppress Indigenous dissent and maintain settler colonial authority. To illustrate specific tactics, we examine these practices as they relate to two cases of Indigenous-led resistance: activism from April 2016 to February 2017 against the construction of the Dakota Access Pipeline (DAPL) that crossed over sacred burial land and contaminated the water supply of the Standing Rock Sioux Tribe in the United States; and Project SITKA, a covert government surveillance programme from January 2014 to January 2015 targeting Indigenous protesters in Canada. We argue that both cases reveal how misinformation (i.e., unintentionally presenting information as truthful) and disinformation (i.e., purposefully false information intended to deceive) (Lewandowsky et al. 2013) operate as interrelated knowledge strategies that use falsities to shift perceptions and responses to events. When applied, they can "overwhelm your critical sensibilities" and "make you doubt the existence of a knowable truth" (Klein 2018). If persuasive enough, they can contribute to widespread and strong beliefs in false and biased information, which can have dire consequences, such as enhancing the population's support for war or armed conflict (Kull et al. 2003; Kaufmann 2004). Further, it is often difficult to disentangle misinformation and disinformation in practice, as actors often employ them in ways that make it harder to detect deception and blatant falsehoods. Here, we examine how misinformation and disinformation, as well as strategies that combine elements of each (hereafter "mis/disinformation"), serve critical roles in securing state power in ongoing battles over Indigenous sovereignty.

The crackdown on contemporary Indigenous-led movements is part of a longer colonial history—a history that is "integral in the formation of the state itself" (Dafnos 2014, 4). As Indigenous peoples' protest has countered settler states' assertion of sovereignty, states have responded by actively working to quell and criminalise them. Knowledge-regulation, we argue, is an overlooked part of these tensions, which reinforces asymmetrical power relations between the state and Indigenous protesters, making

[1] Indigenous peoples often refer to the political and legal jurisdictions of Canada and the United States as Turtle Island (Newcomb 2011).

contemporary colonial practices harder to challenge. As we discuss further, the circumstances around the Standing Rock protests showcase how the state employs information to suppress dissent, promote the construction of pipelines, and conceal the coercive actions of private security firms. In the context of Canada, a country often mythologised as committing less racial violence against and being more inclusive toward Indigenous peoples than the United States (Black 2015; Gilmore 2015), Project SITKA is a coordinated effort to pre-emptively identify and respond to Indigenous persons who are deemed risky or threatening to state interests. Taken together, these examples enable close scrutiny of how information becomes deployed, as well as weaponised, in coordinated state and non-state efforts to suppress Indigenous social movements.

The chapter proceeds as follows. First, we reflect on how scholars acknowledge the important role knowledge plays in terms of states exercising power, particularly in relation to the governance of marginalised groups. In doing so, we draw attention to the role of securitisation and how it supports modes of controlling knowledge to support state interests. We then discuss two cases—that of Standing Rock and Project SITKA—to illustrate how these dynamics play out in relation to critical infrastructure protection and the criminalisation of Indigenous dissent. Indigenous peoples feature centrally in these cases: they have experienced a long history of disproportionate state scrutiny and are often impacted by natural resource extraction operations (e.g., tar sands, deforestation, oil or gas pipelines). Accordingly, forms of Indigenous-led resistance have openly contested capitalism, environmental degradation, and settler colonial claims. After attending to these constitutive conditions, we reflect on how Strange's insights regarding knowledge and structural power aid in understanding how misinformation and disinformation sustain the settler colonial dynamics illuminated in this case. We conclude with a reminder that the regulation of knowledge must be interrogated for its asymmetrical effects, interests, and alliances. These relationships have real-life repercussions in terms of who gets to yield structural power, including violence.

1 Knowledge and Structural Power in Settler-State Governance

Strange (1994, 119, 127) reminds us that the ability to judge what constitutes acceptable versus unacceptable conduct is an exercise of structural power. It is inextricably linked to who can decide the terms of exercising

authority. Recognising that the knowledge structure can be thought of as having both a "*regulatory* aspect (the rules governing the creation, dissemination, and use of knowledge)" and a "*knowledge-legitimation* aspect (the processes by which certain knowledge is deemed legitimate or not)" (Haggart, this volume), their interplay is crucial to understanding the politics of what knowledge becomes valued and normatively embraced. As other chapters in this book explain (e.g., Bannerman and Orasch, Haggart), Strange contends that ideas and beliefs are part of the knowledge structure, which can come to reflect and influence its interrelationships with the other structures of security, production, and finance.

The deployment of mis/disinformation in contemporary settler-state governance offers a site to scrutinise two key concerns related to the knowledge structure: (1) specific tactics employed to legitimate knowledge, and (2) an interplay between knowledge and security that serves state interests—a concern that Strange herself did not explore, but certainly provided a framework for capturing. Strange's insights into authoritative claims made and asserted through knowledge suggest that the ability to influence and shape perspectives of truth is a significant mobilisation of power. Presented in this way, what is accepted as "true" need not correspond with an underlying reality or lived experience; instead, what matters is the belief in a truth—or, as in the case of disinformation, the introduction of doubt regarding other claims of truth or systems of knowledge. As such, Strange's ideas are distinct from Foucauldian notions of power/knowledge, which emphasise the inseparability of power and knowledge as part of the ubiquitous and relational practices that constitute the governance of human subjects (Foucault 1980); however, they share common concerns about the malleability of truth, particularly as it operates in the service of social control.

Knowledge is central to governance. At a foundational level, as Michel Foucault writes, "we are *subjected* to the production of truth through power and we cannot exercise power except through the production of truth" (1980, 93). He also discusses how dominant knowledges often hide or bury subjugated knowledges, which are often disregarded, struck from historical records, or co-opted over time (Foucault 1980, 2003). Knowledge is thus always political, and the insurrection of subjugated knowledge can disrupt and threaten dominant orders. Indigenous protesters taking a stand to protect their lands, such as the Standing Rock protests (Whyte 2017), mark one such an example. We would be remiss, though, not to consider how these tensions are part of longer legacies

rooted in the foundations of states. Foucault (2003), for instance, explains that while war gives way to state formation, the logics of war prevail, becoming embedded in the state and the governance of populations under its jurisdiction. They emerge in the disproportionate treatment of subjects, in which race and racism continue to advance the interests of winners and to institutionally re-inscribe losers as Other (Foucault 2003). According to Ruth Wilson Gilmore, this structural "application of violence—the cause of premature deaths—produces political power in a vicious cycle" (2002, 16). It is often insidious and coercive, not always relying on physical oppression, as the settler state can capitalise on discourse that circulates in the form of justifications, rationalities, and other dominant knowledges to reinforce its interests.

Although Foucault provides guidance in terms of understanding the linkages between war and state racism (and has written extensively on power/knowledge), Strange's observations about structural power and coercion are particularly relevant for thinking through mis/disinformation in relation to Indigenous peoples and how it contributes to the exercise of state power. As Strange (1994) notes, the state does not need to be physically or materially coercive to declare war against threats to its interests; it can harness the power of information to persuade, legitimate, control knowledge, and craft worlds. Structural violence through knowledge is often symbolic rather than openly abusive, and, as Strange explains, "the violent repression of alternative knowledge structures tended to increase whenever the authority became weak or was subject to challenge" (1994, 128). Weaponising information against Indigenous peoples does not always operate in plain sight, which makes its consequences (like the suppression of Indigenous dissent) harder to detect or to identify as problematic. Nevertheless, the presence and effects of weaponised information are no less real or harmful. In fact, the uniquely invisible or ghostly nature of information warfare makes it particularly difficult to identify or challenge.

Securitisation has aided in ensuring that such state practices are veiled. Securitisation, simply put, "is the act of framing an issue as an existential threat requiring extraordinary measures in response" (McKenzie 2018, 9). It is a practice that pervades criminal justice concerns and relies on the regulation of knowledge. In North America, intelligence agencies and their security allies have monopolised discretion over the control of certain kinds of information (Larsen and Walby 2012). These practices exemplify Strange's observations that "the value of the supply to those already holding the knowledge may well be diminished when it is communicated to

others" (Strange 1994, 122). In this case, securitised mechanisms have kept information pertaining to the natural extraction industry from the public's purview because the state has categorised pipelines as critical infrastructure. As the protection of critical infrastructure has been deemed "indispensable for the functioning of social and political life" (Aradau 2010, 491), risks to critical infrastructure, which come to include Indigenous protesters, are consequently treated as threats to national security (Boyle and Speed 2018). This strategic framing reflects a clear deployment of structural power, one that simultaneously bolsters the need for extensive intelligence collection on critical infrastructure vulnerabilities (Monaghan and Walby 2017) and justifies the government's largely unchecked authority to set rules governing this information.

While the connections between knowledge and security are linked, Strange would remind us not to lose sight of their relationships with the other structures of finance and production. Economic and security interests, though conceptually distinct, become blurred under the banner of critical infrastructure. As we discuss further in the next two sections, corporate actors are a key part of the public-private nexus through which threats to critical infrastructure, including forms of Indigenous resistance, are identified and defined. As stated by freelance writer and activist Matthew Behrens (2016, 3), "Indigenous peoples and their lands remain national sacrifice zones in the interests of corporate capital." Their challenges threaten the stability of settler colonialism and impede the capitalist imperative of profit accumulation (Pasternak and Dafnos 2017). Put in Foucauldian terms, these tensions are yet another manifestation of the state's embedded logics of racist violence. Taking these combined observations seriously means we cannot separate securitised techniques from the state's continued commitments to advancing settler interests through various modalities of governance. The deployment of mis/disinformation concerning Indigenous resistance to pipelines and other critical infrastructure assets illuminates these complicated tensions and showcases the centrality of knowledge in settler colonial state maintenance.

2 Settler-Industrial Surveillance in the Information Battle at Standing Rock

In April 2016, local Indigenous communities initiated forms of resistance that led to blocking construction of the DAPL, the establishment of a major protest camp in North Dakota, and non-Indigenous allies joined the struggle locally and globally (Ohlheiser 2016). Their efforts drew public attention

to the DAPL as part of a longer colonial legacy in which the state has failed to meet responsibilities outlined in treaties, exploited and polluted treaty lands, and threatened the survival of Indigenous communities (Estes 2019).[2] At the same time, a range of actors worked to ensure the pipeline project continued uninterrupted, using physical, economic, and penal tactics, as well as strategies for controlling protestor mobility, against the NoDAPL movement.[3] These efforts relied on private-sector actors (Energy Transfer Partners, public relations firms, and conservative media commentators), public agencies (local and federal law enforcement, the U.S. Attorney General's Office, Joint Terrorism Taskforce, National Guard, Federal Bureau of Investigation [FBI], North Dakota Emergency Services), and hybrid actors (private security firms, such as TigerSwan and Silverton, performing government functions) (Brown et al. 2017e; Horn and Waltman 2017). These dynamics are not new; there is a long history of private actor involvement and surveillance practices in the policing of activists and protesters (Lubbers 2015). These integrated efforts are particularly prevalent in cases of defense against environmentalist protesters (Button et al. 2002).

While militarised tactics employed against protesters at Standing Rock have garnered attention, the control of information also stands out as an offensive tactical strategy at Standing Rock: the FBI and TigerSwan infiltrated the activist circles, sometimes using FBI informants posing as protesters to collect private internal information and to turn protesters against one another (Brown et al. 2017d; Hagen 2018). In fact, "TigerSwan agents using false names and identities regularly sought to obtain the trust of protesters, which they used to gather information they reported back to their employer," Energy Transfer Partners (ETP), which owns the DAPL (Brown et al. 2017e, 13). They also monitored protesters' social media and scraped for data while recruiting local residents to share anything that could be perceived as suspicious (Brown et al. 2017c, e). Analysis of surveillance information led to the identification of persons of interest, including the development of a "Be On the Lookout" List, and the mapping of protest networks comprised of mostly Indigenous persons (Parrish 2017).

[2] In accordance with the Treaty of 1851, the DAPL crosses through Sioux territory (d'Errico 2017). In 2017 alone, the DAPL leaked five times (Brown 2018).

[3] Actors employed non-lethal weapons, including rubber bullets and water cannons, as well as militarised weapons and personnel typically used in counterinsurgency operations (Brown et al. 2017b, d). ETP also launched a US$300-million racketeering and defamation lawsuit against pipeline resistance groups, alleging that they intentionally enflamed protests to increase viewer interest (Brown et al. 2017c).

This state-private network deployed and controlled information to cover up law enforcement and private security's actions, withholding key information about their operations, spreading false information about protesters' violence and criminality. Further, it enlisted people to develop and shape the messaging around DAPL and protests in order to influence public perceptions (Brown et al. 2017e; Horn and Waltman 2017). For instance, TigerSwan concealed its role as a private security and investigation firm by claiming that they instead provided "management consulting and IT consulting for our client and doing no security work" (Brown et al. 2017e, 8). Using disinformation, the company disguised their operations because it had been denied an investigation and security licence (Brown et al. 2017a). Federal government, state prosecutors, and judges restricted the release of information related to the far-reaching surveillance activities of public and private law enforcement involved in Standing Rock. Despite persistent and public pleas from defence lawyers representing protesters, such as Red Fawn Fallis who was arrested and charged thanks to information provided by an undercover FBI informant disguised as a protester, government-generated records of these activities were delayed for upwards of a year and were heavily redacted upon release (Parrish 2018).

Public relations (PR) firms, including Delve and Off the Record Strategies, crafted misleading information in the form of professionally crafted talking points, opposition research, and communication strategies, that portrayed the NoDAPL movement as having "nothing less than a desire to occupy, threaten and intimidate" rather than as justifiable protest (Horn and Waltman 2017, 3). They also trained law enforcement on how to strategically speak about DAPL opponents, with the aim of discrediting the NoDAPL movement. For instance, a PR firm advised the National Sheriffs Association and North Dakota Association of Counties to proactively influence the wider narrative, saying "to make sure we are pushing the primary message before the actual press conference begins" (Horn and Waltman 2017, 3). Popular conservative media outlets, including right-wing internet bloggers and radio hosts in North Dakota were sought out to spread calculated pro-DAPL messages, which law enforcement and their allies then distributed via their own platforms (Horn and Waltman 2017). For example, a conservative radio show host of the North Dakota radio programme *What's On Your Mind?* invited a local police officer to discuss DAPL and broadcast talking points supportive of the pipeline and its policing efforts. The host also shared the NSA's memo on his personal Facebook page, which included strategic

dis/misinformation that protesters had ties to Palestinian activists, were in possession of illegal weapons and drugs, and engaged in persistent acts of physical violence, vandalism, and theft that angered the neighbouring community and law enforcement; the post was subsequently shared by the NSA on their own Facebook page (Horn and Waltman 2017, 5).

Various organisations, including the U.S. Department of Homeland Security (DHS) and Bureau of Indian Affairs, TigerSwan, the FBI, and conservative media, contributed to mis/disinformation campaigns that supported the construction of the pipeline by framing anti-DAPL representatives, rather than ETP and its allies, as threats to safety and security. Consider a widely publicised night raid where police deployed various less-than-lethal weaponry against nonviolent protesters, resulting in hundreds of injuries, including the near dismemberment of DAPL protester, Sophia Wilansky's arm (Hagen 2017). Various law enforcement, security, and media groups supportive of ETP disseminated claims that Wilansky's injury was the "product of dumbass 'direct action' protesters" throwing a self-fashioned propane tank transformed into an improvised explosive device (IED) at law enforcement, as evidenced in cross-departmental communications, police press releases, and right-wing news outlets. In fact, some cross-departmental communications, including emails sent by the Attorney's Office National Security Intelligence Specialist Terry Van Horn, contend that Wilansky threw the IED herself (Brown et al. 2017d).

On the whole, mis/disinformation tactics operated to delegitimise dissent and resistance to the pipeline, mobilising both knowledge and law to accuse activists of illegal activities and to shape public perceptions of protesters. In line with Strange (1994, 119), they exercised power through the "negative capacity" to deny knowledge—to repudiate, contradict, or exclude the acceptance, and therefore legitimacy of other knowledges and groups. These practices not only reinforced truth claims supportive of ETP, but they also cast doubt on the validity of protesters' claims. For example, TigerSwan, local police, the National Sheriffs' Association and the DHS Office of Intelligence disseminated information around alleged drug and weapon use among protesters (Brown et al. 2017a, d; Parrish 2017), but not about TigerSwan failing to obtain a license in North Dakota, which, in turn, made their ongoing private security and investigative operations illegal (Brown et al. 2017a). In doing so, disinformation activities supported a culture of fear against activist groups, preventing civilians from knowing about state-private wrongdoing. These collaborations thus have distinct

capabilities in terms of defining who was perceived as engaging in acceptable and unacceptable actions, what circulated as the truth regarding the events at Standing Rock, and played up the importance of DAPL to local and national security. Protesters, for example, were framed as threatening the safety and security of nearby communities and preventing "American citizens and businesses the energy they need to produce jobs and build a vital and healthy economy" (Dakota Access Pipeline Facts 2017). In doing so, these narratives not only reiterated economic and national energy security claims as inherent goods, but they also presented protestors who supported Indigenous sovereignty as standing against U.S. citizens and interests. In fact, a survey of jury-eligible residents in North Dakota, where many protesters were being charged with Standing Rock-related offences, "found that 82 per cent to 94 per cent had prejudged protesters as guilty or were biased against them," thereby potentially impeding their right to a fair trial (Levin 2018, 3).

Resistance groups countered these narratives by constructing their own narratives about the policing of Standing Rock protests and ETP's pipeline construction, as well as by generating counter-information to bolster on-the-ground protesters' awareness of law enforcement tactics and the movement's perceived legitimacy within society. They collected and shared intelligence about police and private security's locations and suppression activities (Brown et al. 2017a) so that they could identify and respond to their coordinated plans (AJ+ 2016). Protester-generated information provided evidence of environmental harm, public-private collusion, police violence, including middle-of-the-night raids, and the resilience of protesters on site (Brown et al. 2017e). A "Facebook check-in" effort grew as remote protesters and average citizens around the world used the social media platform's geolocation tagging to thwart law enforcement efforts to track who was physically present at the North Dakota protest camp (Massie 2016). They also used Facebook to provide wider coverage about protesters' plights in the face of violence (Torchin 2016). For protesters, diverse forms of information collection—drones, patrols on horseback, on-the-ground recordings, and personal narratives—emerged as a form of "protect[ion] … against the legal and constitutional violations [they were] witnessing and going through" (Brown et al. 2017a; AJ+ 2016). Withholding and falsifying information was another tool of resistance, concealing the involvement of some activists in petty crimes, such as vandalism, after exhausting a range

of lawful lobbying tactics.[4] Two anti-DAPL activists, when contacted by journalists concerning allegations that they were involved in pipeline sabotage, initially denied that they were. Later confessing to this disinformation, the pair "[e]xplained the timing of their confession … as an opportunity to encourage public discourse surrounding nonviolent direct action" (Brown et al. 2017c).

Beyond the militarised logics, tactics, personnel, and organised counter-intelligence campaigns centred around the DAPL, Standing Rock represents an information battle linked to the exercise of structural power, exemplifying scholarly observations about how information is integral to structuring battle spaces (Waltzman 2017). Informational warfare, according to technological warfare specialist David Stupples (2015), encompasses electronic (e.g., jamming), cyber-warfare (hacking), and cognitive (propaganda) warfare operations. Otherwise known as psychological-operations (psy-ops) (Stupples 2015) and influence operations (Waltzman 2017), adversaries target the cognitive processes, biases, and errors of different populations by leveraging tactics of "deception, persuasion, creation of fear, shaping available information, or even shaping the information environment" (King 2011, 17). The aim of this specific type of information warfare is to secure a competitive advantage over the adversary by controlling public opinion and coercing mass persuasion (ibid.). Considering these insights, information-related tactics relevant to Standing Rock amount to the weaponisation of knowledge. The distinction in a settler colonial context, though, is that they are part of longer legacies tactics, which Foucault (2003) explains as being rooted in the state. War does not end; it becomes part of governance.

3 State-Sponsored Surveillance of Indigenous Peoples in Canada

In 2016, when researchers Crosby and Monaghan submitted Access to Information and Privacy requests, they obtained the report, "Project SITKA: Serious Criminality Associated to Large Public Order Events with National Implications," which outlined a classified "quasi-criminal investigation" (2018, 1) and surveillance operation that provided a detailed

[4] Nonviolent activities included attending public commentary hearings, gathering signatures for valid requests for environmental impact statements, participating in civil disobedience, hunger strikes, marches and rallies, boycotts, and encampments (Brown et al. 2017c).

overview of individually posed threats to public order events from 2010 through 2015. Though the RCMP routinely issues intelligence reports and conducts surveillance on citizens, central to this case is that it surveilled lawfully acting protesters because the nature of their protests (which are aimed at oil infrastructure) and because they are Indigenous.

Project SITKA was launched in response to a National Tactical Intelligence Priority that was to address the "increase … in Aboriginal protests"[5] and their potential for "unlawful tactics" (Project SITKA 2015, 4). To meet the mandate, the National Intelligence Coordination Centre (NICC), operated by Canada's national police force, the Royal Canadian Mounted Police (RCMP), established a coordinated investigatory effort with Community and Aboriginal Policing, local law enforcement departments, and RCMP divisions throughout the country (Project SITKA 2015, 6–7).[6] Though controversial, these formal and multi-agency intelligence collaborations are not unusual. They are, in fact, legal, and benefit from security networks, alliances, and information-sharing channels that have become institutionalised and normalised (Crosby and Monaghan 2018). Using various surveillance tactics to deliver detailed portraits of resistance efforts, the state's pursuit of knowledge extended beyond prominent activists and overtly criminal behaviour, enabling a much wider picture of Indigenous resistance in terms of scope. Specifically, they developed detailed overviews of individual activists, organisations, and networks; the level of their connectedness across Canada; protesters' social media usage; demographic breakdowns; and attendance at protest events (Livesey 2017a).

The data collected yielded 313 subjects of interest who had their personal information calculated and assessed, using actuarial scoring and risk taxonomies to determine the level of criminal threat these individuals posed in terms of "Aboriginal occupations and protests" (Project SITKA 2015, x). Criteria assessing protesters' personalities, motivations, and protest strategies served as the basis for classifying individuals as "Suspects,

[5] Project SITKA was organised after two extensively publicised Indigenous-led social movements in Canada: Idle No More (November 2012 to April 2013) and Missing and Murdered Aboriginal Women (early 2014 to the present).

[6] The report was compiled by gathering information from tracking individual persons, "all RCMP divisions, data contained within law enforcement data bank holdings, and open [publicly available] information" like social media (Project SITKA 2015, 7, 11). It focused on protests, "speaking tours, disruption of political proceedings, and direct action training camps" (2015, 10).

Persons of Interest, and Associates" (Project SITKA, viii). A "Public Order Profile Scale" also weighted activist group characteristics and behaviours—including their "impacts upon public values" and how "strongly [they are] committed to their cause"—and offered an overall "POPS risk rating" (Project SITKA 2015, xi–xii). To build and populate these profiles required surveillance, which has been standard practice among law enforcement agencies, often for the purpose of pre-emptively detecting criminal people and areas (Woodworth and Porter 1999).

More recently, risk-prediction instruments have become part of a broader expansion of actuarial justice. Their use is intended to streamline decision-making by displacing human discretion in determinations of threat attributes with the use of quantitative and systematised formulas (Moffat et al. 2009). Project SITKA's protester threat assessments can be thought of as more than computational assessments of risk; they actually reorganise and shift the exercise of power, in this case in favour of settler colonial authorities. That is, as both a form of discourse and criminal justice technology, risk assessments rearticulate and mobilise settler-state power along seemingly neutral standards of "professional evaluations" and "evidence". These actions, in turn, can shield the settler state (and its authority) against critiques of discrimination, bias, and unfair judgment. As such, the individuals identified in the report emerge as "risk objects": "that is, not only are they subject to risk management strategies, they are also cast as the source of risk" (Henne and Troshynski 2013, 101). In keeping with Henne and Troshynski's (2013) observations, Project SITKA's analysis identified 89 of the 313 persons as meeting "criteria for serious criminality" (2015, 18) in terms of their likelihood of becoming a future criminal threat. This appraisal prompted the creation and dissemination of their individualised surveillance profiles,[7] which were to be kept up-to-date for future law enforcement use and disseminated to front-line police officers, RCMP divisional analysts, and other law enforcement partners through two national databases.

Of note is the finding that some persons of interest who had their profiles circulated stood in opposition to corporate interests, "particularly pipeline and shale gas expansion" (Project SITKA 2015, 12). These findings are not unexpected considering the long-standing and close

[7] Threat profiles included information on their height, age, weight, phone number, personalities, tactics, vehicles, mobility, "category of protester," "notable files," etc. (Project SITKA 2015, xiv, xv).

relationship between the energy sector and national security agencies, which Monaghan and Walby (2017) argue has been further cemented through critical infrastructure protection and the defence of pipelines. As extractive projects such as DAPL often operate on or directly impact Indigenous peoples' lands, they emerge as sites in which we can observe contestations over land that are at the heart of settler colonialism (Estes 2019; Rowe and Tuck 2017). Project SITKA, although relatively new, is part of a longer struggle between Indigenous peoples and settler colonial projects. In fact, these tensions gained greater public attention in late 2018, when RCMP officials began to dismantle two camps on unceded Wet'suwet'en territory, both of which were protesting the construction of a natural gas pipeline.

Looking more closely at the Project SITKA report reveals how the control of information, alongside misinformation and disinformation strategies, serves settler interests. In terms of the control of securitised knowledge, Project SITKA's threat assessments were classified as protected information that, "if compromised, could cause injury to an individual, organization, or government" (Government of Canada 2017). As such, the vast majority of information about the Project SITKA was not accessible, nor was it required to be shared. Similar to information related to the policing and surveillance of Standing Rock protesters, information was not easily accessible to the public and only some was available via Freedom of Information requests and, in the case of Standing Rock, some information leaked by employees or ex-employees who had access to protected information. In controlling access to securitised knowledge, the surveillance, profiling, and categorisation of lawful protesters as risky remains insulated from public knowledge (and therefore away from public contestation).

Beyond the control of information, some disinformation is apparent. The report on Project SITKA revealed misinformation in the misrepresentation of Indigenous activism. For instance, even though the report acknowledges that "systemic issues … might lead Aboriginal people to mount protests or occupations in the first place" (Project SITKA 2015, 8), it goes on to characterise their reasons for protest as complex but ultimately unknown. This position is asserted even though many Indigenous activists have used a myriad of forums (e.g., public statements, social media, news reports) to openly and frequently share their personal aims, experiences, and histories (see Sium and Ritskes 2013). Thus, the report's characterisation of Indigenous protesters' reasons as vague, especially when considered alongside strong assertions about risk and the need to

surveil them, undermines Indigenous people's claims to sovereignty by presenting them as not substantiated.

To legitimate the activities, motivations, and consequences of this multi-organisational surveillance operation, Project SITKA draws selectively on forms of expertise to support its stated commitments to "maintain[ing] public order while ensuring public safety" (2015, 4) through the use information-based strategies. For example, the report presents classificatory schemes developed by an independent public-order policing expert, Dr. Eli Sopow. These socio-psychological profiles lend to different kinds of suspect categories, which are Volatile, Disruptive, and Passive, in order to engage in ongoing or future criminal activity (Project SITKA 2015, 7). Further, Sopow currently works for the RCMP, providing "training and advice" on public-order events. In the past, he has worked for both public (e.g., U.S. DHS, Government of British Columbia) and private organisations, most notably "many resource corporations" (Project SITKA 2015, iii). Presenting these categories as "accurate, comprehensive list[s]" (Project SITKA 2015, ii) substantiates the report's identification and categorisation of "criminal" protesters as an entirely "objective means to demonstrate criminal and violent intentions" (Livesey 2017a, 8). Although put forth as a sound methodology devoid of bias, Sopow and the RCMP's protester risk assessment reflect the shortcomings of actuarial and risk-based approaches, which have been critiqued for being entrenched with personal, cultural, and racial assumptions (Moffat et al. 2009) and for often being retrofitted to advance institutional agendas (Maurutto and Hannah-Moffat 2006). In this case, the report's risk assessments promoted actuarial kinds of knowledge about Indigenous peoples, which legitimate racially targeted policing and surveillance while contributing to the social control of broadly defined public-order threats. Although framed in objective terms, it relies on settler-constructed categorisations, which frame Indigenous assertions of self-determination and environmental degradation as "irrational and hostile threats to settler common sense" (Crosby and Monaghan 2018, 174).

At the same time, official statements comments made by representatives of the Canadian government officials about the Project SITKA perpetuate settler-supportive narratives, even though they appear to promote civility and safety. In a 2016 meeting with oil sector business leaders, Canadian Natural Resources Minister Jim Carr justified the use of military and police force to combat civil disobedience blocking pipelines to protect those working on natural resource projects (Livesey 2017b; Voices-Voix 2017), thereby marketing safety as something the state will ensure for its settler

subjects, not its Indigenous residents. Canadian Prime Minister Justin Trudeau took a different approach, maintaining that "Canada's national police force respects the right to peaceful demonstrations by Indigenous activists" (Craig 2016). His words implied a distinction between the "good" and law-biding Indigenous citizen from the "bad" and criminalistic subject, implicitly positioning the settler state as acting legitimately even though it is built on long-standing violence.

Overall, revelations around Project SITKA reveal how articulations of incomplete or skewed reporting—a blurring of mis/disinformation—are key to the Canadian state's justification of its activities targeting Indigenous activists. The report and related state discourse mostly manipulate information through the disregard of historical and present-day contexts—what Mohawk anthropologist Audra Simpson (2017) emphasises as continuous colonial disavowal and amnesia. The contorting of surveillance evidence through the logics of risk assessments enables speculation of protesters' motivations, tactics, and future behaviours, but not of the settler state. These forms of strategic disavowal contribute to enduring formations of settler governance and control (see Fullenwieder and Molnar 2018), and in doing so, they make it harder to challenge deployments of structural power.

The Canadian government's use of mis/disinformation reflects manoeuvres to legitimate Project SITKA's intrusive surveillance and threat categorisations as the outcomes of good intentions and sound policy. By doing so, the report promotes a settler-centric agenda that has two key implications: On the one hand, it frames the promotion of pipeline projects and resources extraction as in the national interest; on the other, its targeting of Indigenous protesters' legitimacy exacerbates an already deep suspicion of Indigenous peoples in general—of peoples who challenge the settler state's (see Simpson 2017). The use of information therefore contributes to a revolving door of mistrust that strengthens the monitoring of populations that already experience notable levels of disenfranchisement, which (as discussed below) is further perpetuated by the securitisation of information.

4 Securitising and Weaponising Information

Contemporary cases of states mobilising against Indigenous-led resistance to natural resource development showcase the surfacing of war logics embedded in the state. They reflect a longer tradition in which settler colonial states have used law and policy as tools to secure their

interests—for example, the use of contracts to remove Indigenous peoples from their lands (Simpson 2016). The particular role of knowledge, however, is distinct. While Standing Rock showcases how information can be weaponised through public discourse, Project SITKA demonstrates how the securitisation of critical infrastructure protection enables a form of information-based regulation that not only manages how, when, and to whom information is disseminated, but also who it targets. Policy aids in centralising the Canadian government's control over information—specifically, the channels by which it is communicated and accessed—about the surveillance and policing of Indigenous peoples. It can therefore be thought of as a key apparatus of knowledge-regulation.

Additionally, collaborations between state-private sector strategies of mis/disinformation and knowledge gatekeeping, reinforced by securitisation, supports the exercise of state power through the knowledge structure (Strange 1994). Without access to information collected through operations targeting legal social movements or knowledge of how it was corroborated, it is difficult to verify or contest security claims (Crosby and Monaghan 2018). The resulting *unknowability* of this knowledge to populations beyond a covert surveillance network makes it much harder to challenge state claims, including: which protesters are classified as risks to critical infrastructure; why, and how they are being accounted for; reasons behind expanding state powers and authority through critical infrastructure protection; how policing decisions are made; and, whose interests are represented under the banner of national security (Monaghan and Walby 2017). Securitisation thus enables and authorises black-box decision-making about vaguely defined threats.

Strange's insights can help us understand information-based tactics employed by settler colonial states. While the cases of Standing Rock and Project SITKA are not the same, they show how states manipulate and weaponise information. In both cases, the strategic use and protection of knowledge supports the ongoing dispossession of Indigenous peoples' land to make way for critical infrastructure. Moreover, the rendering of Indigenous protesters as suspect or criminalistic in both cases is rooted in a longer genealogy of the state. While Standing Rock highlights overt tactics of mis/disinformation, Project SITKA illustrates a mode of exercising power that is not as visible as the tactics deployed in relation to protesters at Standing Rock. Without transparency to identify these practices

or meaningful ways to counter governmental knowledge, the settler colonial state leverages power through opacity. Even when Project SITKA became known, it did not receive the same amount of public scrutiny or mainstream media reporting, particularly when compared to the visibility of activities surround Standing Rock protests. While mainstream Canadian news outlets (the National Post, CBC News, and the Globe and Mail) acknowledged the report, it was Indigenous news outlets (APTN News, Warrior Publications), and social justice groups (Council of Canadians, Voices-Voix, Canadian Journalists for Free Expression) that commented extensively. These tactics, though not scrutinised like the state-private tactics of coercion observed in relation to Standing Rock, nonetheless reaffirm CIP and counter-protest networks enabled by both state and private actors, which continue to wield power over historically marginalised groups like Indigenous peoples.

Despite the apparent strength of the state, its exercise of power is not as all encompassing as we may assume. We would be remiss not to acknowledge that Indigenous resistance narratives have long responded to and resisted settler colonial dispossession and violence (Rowe and Tuck 2017). Protesters, for instance, used technologies, such as drones to collect information as a way to legitimate their claims through visual evidence, supporting a larger project that asserts their sovereignty and autonomy. Power asymmetries prevail, however, and are fortified by entrenched settler beliefs and ideologies—dominant knowledges that both Foucault (2003) and Strange (1994) acknowledge. If we consider negative perceptions of Indigenous peoples and protesters alongside weaponised information that aligns with, and actually reinforces, long-standing discriminatory beliefs, we can see that claims shaped by mis/disinformation are often influential because they are "compatible with other things the recipient assumes to be true" (Lewandowsky et al. 2013, 490). They exploit an already-prevalent bias against Indigenous peoples. For instance, many Canadians do not empathise with or understand the historical and contemporary settler colonial abuses endured by Indigenous peoples, as evidenced by a recent Canadian survey in which most respondents indicated that they believed the state had overly apologised for the residential school system and that Indigenous peoples should assimilate into society (Palmater 2018). In short, the *knowledge-legitimation* aspect of structural power has clear hegemonic dimensions that surpass the direct actions of the settler state.

5 Conclusion

Though securitisation is important to understanding how states wield authority and exercise structural power, we recognise that most analyses of these dynamics fail to attend to embedded settler colonial dynamics. This chapter marks an attempt at remedying this gap by illustrating how a focus on knowledge reveals that securitisation is only one dimension of structural power. In doing so, we have endeavoured to illustrate that it would be a misnomer to think of the deployment of mis/disinformation as peripheral activities. Efforts to craft and legitimate narratives that advance both settler state and corporate interests reveal how knowledge has been central to the suppression of Indigenous protesters. However, mis/disinformation must be considered in relation to other constitutive relations, as it does not operate alone. It is inextricably linked to overt efforts to collect, hide, and deploy information strategically, as well as knowledge relationships. Dominant knowledges have a hegemonic quality that not only reflects the state's monopoly over legitimised violence, but also perpetuates and normalises its exercise through more coercive modes. We see this perhaps most clearly in the Canadian case: The Canadian government has shifted from its earlier attempts to portray Canadian energy corporations as "ethical oil" (Foster 2010) to rendering Indigenous protest as a criminal threat (Crosby and Monaghan 2018). Once the government and law enforcement share intelligence about Indigenous protesters, the assertions of a threat retain a more permanent place within the knowledge structure, thereby contributing to a longer trajectory of settler colonial governance.

Specific tactics that target, surveil, and criminalise Indigenous peoples are but one dimension of the knowledge structure's place in settler colonial governance. More generally, manoeuvres, such as misinformation and disinformation, that direct focus and attention onto Indigenous protesters are a larger misdirection from ongoing colonial practices, which, in turn, contribute to the re-inscription of subjugated knowledges and peoples. Intrusions onto Indigenous lands through the justification of critical infrastructure are but one grounded example of larger processes, and the fight over pipelines and critical infrastructure has never operated on level-playing grounds. Although Indigenous land protectors have used information to both unearth and counter entangled state-corporate interests, the pipelines at the heart of the Standing Rock protests have not been halted, and Project SITKA never underwent strong public scrutiny—and both developments received limited critical media attention (Levin

2018; Torchin 2016). Thus, as Strange (1994, 119) writes, "there are asymmetries in networks of information" and "divergences in perceptions," but the analysis of knowledge and the exercise of structural power should not end there. It requires further examination of not only its interrelationships with structures of security, finance, and production, but also of longer legacies that have indoctrinated dominant knowledges that operate in the service of inequitable governance.

References

AJ+. 2016. #NoDAPL Drones Monitor North Dakota Police. Video. Published December 2, 2016. https://www.youtube.com/watch?v=uXWw0y44xaM.

Aradau, Claudia. 2010. Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* 41 (5): 491–514.

Behrens, Matthew. 2016. Trudeau's Trumpishness Bulldozes Indigenous Rights. *Rabble.ca*, November 23. Accessed December 30, 2018. http://rabble.ca/columnists/2016/11/trudeaus-trumpishness-bulldozes-indigenous-rights.

Black, Conrad. 2015. Conrad Black: Canada's Treatment of Aboriginals Was Shameful, But It Was Not Genocide. *National Post*, June 7. https://nationalpost.com/opinion/conrad-black-canadas-treatment-of-aboriginals-was-shameful-but-it-was-not-genocide.

Boyle, Philip J., and Shannon T. Speed. 2018. From Protection to Coordinated Preparedness: A Genealogy of Critical Infrastructure in Canada. *Security Dialogue* 49 (3): 217–231.

Brown, Alleen. 2018. Five Spills, Six Months in Operation: Dakota Access Track Record Highlights Unavoidable Reality—Pipelines Leak. *The Intercept*, January 9. https://theintercept.com/2018/01/09/dakota-access-pipeline-leak-energy-transfer-partners/.

Brown, Alleen, Will Parrish, and Alice Speri. 2017a. The Battle of Treaty Camp. *The Intercept*, October 27. https://theintercept.com/2017/10/27/law-enforcement-descended-on-standing-rock-a-year-ago-and-changed-the-dapl-fight-forever/.

———. 2017b. Police Used Private Security Aircraft for Surveillance in Standing Rock No-Fly Zone. *The Intercept*, September 29. https://theintercept.com/2017/09/29/standing-rock-dakota-access-pipeline-dapl-no-fly-zone-drones-tigerswan/.

———. 2017c. TigerSwan Responded to Pipeline Vandalism by Launching Multistate Dragnet. *The Intercept*, August 26. https://theintercept.com/2017/08/26/dapl-security-firm-tigerswan-responded-to-pipeline-vandalism-by-launching-multistate-dragnet/.

———. 2017d. Standing Rock Documents Expose Inner Workings of 'Surveillance-Industrial Complex'. *The Intercept*, June 3. https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex/.

———. 2017e. Leaked Documents Reveal Counterterrorism Tactics Used at Standing Rock to "Defeat Pipeline Insurgencies. *The Intercept*, May 27. https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/.

Button, Mark, Tim John, and Nigel Brearley. 2002. New Challenges in Public Order Policing: The Professionalisation of Environmental Protest and the Emergence of the Militant Environmental Activist. *International Journal of the Sociology of Law* 30 (1): 17–32.

Craig, Sean. 2016. RCMP Tracked 89 Indigenous Activists Considered 'Threats' for Participating in Protests. *National Post*, November 13. https://nationalpost.com/news/canada/rcmp-tracked-89-indigenous-activists-considered-threats-for-participating-in-protests.

Crosby, Andrew, and Jeffrey Monaghan. 2018. *Policing Indigenous Movements: Dissent and the Security State*. Halifax: Fernwood Publishing.

d'Errico, Peter. 2017. The U.S. Claim of Domination Over Standing Rock Violates the Treaty of 1851. *Indian Country Today*, February 7. https://newsmaven.io/indiancountrytoday/archive/the-u-s-claim-of-domination-over-standing-rock-violates-the-treaty-of-1851-mbhIlIuFEkOp_y9S9P4Xag/.

Dafnos, Democrati. 2014. *Negotiating Colonial Encounters: (Un)Mapping the Policing of Indigenous Peoples' Protests in Canada*. PhD Dissertation, York University.

Dakota Access Pipeline Facts. 2017. The Dakota Access Pipeline Is the Best Way to Move Bakken Crude Oil to Market. Accessed December 30, 2018. https://daplpipelinefacts.com/.

Estes, Nick. 2019. *Standing Rock Versus the Dakota Access Pipeline, and the Long Tradition of Indigenous Resistance*. New York: Verso.

Foster, Peter. 2010. Peter Foster: Ethical Oil. *Financial Post*, September 21, 2010. https://business.financialpost.com/opinion/peter-foster-ethical-oil.

Foucault, Michel. 1980. *Power/Knowledge: Selected Interviews and Other Writings 1972–1977*. Rome: Pantheon.

———. 2003. *Society Must Be Defended: Lectures at the Collège De France, 1975–76*. New York: Picador.

Fullenwieder, Lara, and Adam Molnar. 2018. Settler Governance and Privacy: Canada's Indian Residential School Settlement Agreement and the Mediation of State-Based Violence. *International Journal of Communication* 12: 1332–1349.

Gilmore, Ruth Wilson. 2002. Fatal Couplings of Power and Difference: Notes on Racism and Geography. *The Professional Geographer* 54 (1): 15–24.

Gilmore, Scott. 2015. Canada's Race Problem? It's Even Worse than America's. *Maclean's*, January 22. https://www.macleans.ca/news/canada/out-of-sight-out-of-mind-2/.

Government of Canada. 2017. *Levels of Security*. Accessed August 25, 2017. https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html.

Hagen, C.S. 2017. TigerSwan and Government Twist Narrative Over Dakota Access Pipeline. *High Plains Reader*, June 6. http://hpr1.com/index.php/feature/news/tigerswan-and-government-twist-narrative-over-dakota-access-pipeline/.

———. 2018. Infiltrated: No-DAPL Activist Hoodwinked by Paid FBI Informant, Defense Says. *High Plains Reader*, January 11. http://hpr1.com/index.php/feature/news/infiltrated-no-dapl-activist-hoodwinked-by-paid-fbi-informant-defense-says/.

Haggart, Blayne. 2017. Incorporating the Study of Knowledge into the IPE Mainstream, or, When Does a Trade Agreement Stop Being a Trade Agreement? *Journal of Information Policy* 7: 176–203.

Henne, Kathryn, and Emily Troshynski. 2013. Suspect Subjects: Affects of Bodily Regulation. *International Journal of Crime, Justice and Social Democracy* 2 (2): 100–112.

Horn, Steve, and Curtis Waltman. 2017. Emails Show Iraq War PR Alumni Guided Government Response to Standing Rock Protests. *MuckRock*, July 20. Accessed December 30, 2018. https://www.muckrock.com/news/archives/2017/jul/20/DAPL-pr-iraq-war/.

Kaufmann, Chaim. 2004. Threat Inflation and the Failure of the Marketplace of Ideas. *International Security* 29 (1): 5–48.

King, Sara B. 2011. Military Social Influence in the Global Information Environment: A Civilian Primer. *Analyses of Social Issues and Public Policy* 11 (1): 1–26.

Klein, Ezra. 2018. Donald Trump, Fox News, and the Logic of Alternative Facts. *Vox*, February 9. https://www.vox.com/policy-and-politics/2018/2/9/16991410/trump-fox-nunes-fbi-warner-texts.

Kull, Steven, Clay Ramsay, and Evan Lewis. 2003/2004. Misperceptions, the Media, and the Iraq War. *Political Science Quarterly* 118 (4): 569–598.

Larsen, Mike, and Kevin Walby. 2012. Introduction: On the Politics of Access to Information. In *Brokering Access: Power, Politics and Freedom of Information Process in Canada*, ed. Mike Larsen and Kevin Walby, 1–32. Vancouver: UBC Press.

Levin, Sam. 2018. 'He's a Political Prisoner': Standing Rock Activists Face Years in Jail. *The Guardian*, June 22. https://www.theguardian.com/us-news/2018/jun/22/standing-rock-jailed-activists-water-protectors.

Lewandowsky, Stephan, Werner G.K. Stritzke, Alexandra M. Freund, Klaus Oberauer, and Joachim I. Krueger. 2013. Misinformation, Disinformation, and Violent Conflict: From Iraq and the 'War on Terror' to Future Threats to Peace. *American Psychologist* 68 (7): 487–501.

Livesey, Bruce. 2017a. Spies in Our Midst: RCMP and CSIS Snoop on Green Activists. *National Observer*, May 5. https://www.nationalobserver.com/2017/05/05/news/spies-our-midst-rcmp-and-csis-snoop-green-activists.

———. 2017b. Canada's Spies Collude with the Energy Sector. *National Observer*, May 18. https://www.nationalobserver.com/2017/05/18/news/canadas-spies-collude-energy-sector.

Lubbers, Eveline. 2015. Undercover Research: Corporate and Police Spying on Activists. An Introduction to Activist Intelligence as a New Field of Study. *Surveillance & Society* 13 (3/4): 338–353.

Massie, Victoria M. 2016. What the Viral Facebook Check-In at Standing Rock Says About Activist Surveillance. *Vox*, November 1. https://www.vox.com/identities/2016/11/1/13486242/facebook-standing-rock.

Maurutto, Paula, and Kelly Hannah-Moffat. 2006. Assembling Risk and the Restructuring of Penal Control. *British Journal of Criminology* 46 (3): 438–454.

McKenzie, Michael. 2018. *Common Enemies: Crime, Policy, and Politics in Australia-Indonesia Relations*. Oxford: Oxford University Press.

Moffat, Kelly, Paula Maurutto, and Sarah Turnbull. 2009. Negotiated Risk: Actuarial Illusions and Discretion in Probation. *Canadian Journal of Law and Society* 24 (3): 391–409.

Monaghan, Jeffrey, and Kevin Walby. 2017. Surveillance of Environmental Movements in Canada: Critical Infrastructure Protection and the Petro-Security Apparatus. *Contemporary Justice Review* 20 (1): 51–70.

Newcomb, Steven. 2011. 'Canada' and the 'United States' Are in Turtle Island. *Indian Country Today*, September 30. Accessed December 30, 2018. https://newsmaven.io/indiancountrytoday/archive/canada-and-the-united-states-are-in-turtle-island-BuMvxVSitEG766jBQ2WplA/.

Ohlheiser, Abby. 2016. Why Facebook Users Are 'Checking In' at Standing Rock. *The Washington Post*, October 31. https://www.washingtonpost.com/news/the-intersect/wp/2016/10/31/why-facebook-users-are-checking-in-at-standing-rock/?utm_term=.1abd60807620.

Palmater, Pam. 2018. Indigenous Rights Are Not Conditional on Public Opinion. *Macleans*, June 8. https://www.macleans.ca/opinion/indigenous-rights-are-not-conditional-on-public-opinion/.

Parrish, Will. 2017. An Activist Stands Accused of Firing a Gun at Standing Rock. It Belonged to Her Lover—An FBI Informant. *The Intercept*, December 11. https://theintercept.com/2017/12/11/standing-rock-dakota-access-pipeline-fbi-informant-red-fawn-fallis/.

———. 2018. A Native American Activist Followed Her Mother's Footsteps to Standing Rock. Now She Faces Years in Prison. *The Intercept*, January 30. https://theintercept.com/2018/01/30/standing-rock-red-fawn-fallis-plea-deal/.

Pasternak, Shiri, and Tia Dafnos. 2017. How Does a Settler State Secure the Circuitry of Capital? *Environment and Planning D: Society and Space* 36 (4): 739–757.

Project SITKA. 2015. *Project SITKA: Serious Criminality Associated to Large Public Order Events with National Implications* [Report]. National Intelligence Coordination Centre, March 16.

Rowe, Aimee Carrillo, and Eve Tuck. 2017. Settler Colonialism and Cultural Studies: Ongoing Settlement, Cultural Production, and Resistance. *Cultural Studies: Critical Methodologies* 17 (1): 3–13.

Simpson, Audra. 2016. The State Is a Man: Theresa Spence, Loretta Saunders and the Gender of Settler Sovereignty. *Theory & Event* 19 (4): 1–16. https://muse.jhu.edu/article/633280.

———. 2017. The Ruse of Consent and the Anatomy of 'Refusal': Cases from Indigenous North America and Australia. *Postcolonial Studies* 20 (1): 18–33.

Sium, Aman, and Eric Ritskes. 2013. Speaking Truth to Power: Indigenous Storytelling as an Act of Living Resistance. *Decolonization: Indigeneity, Education & Society* 2 (1): i–x.

Strange, Susan. 1994. *States and Markets*. 2nd ed. London: Bloomsbury Publishing.

Stupples, David. 2015. What Is Information Warfare? *World Economic Forum*, December 3. Accessed December 30, 2018. https://www.weforum.org/agenda/2015/12/what-is-information-warfare/.

Torchin, Leshu. 2016. What Can the Mass 'Check-In' at Standing Rock Tell Us About Online Advocacy? *The Conversation*, November 4. https://theconversation.com/what-can-the-mass-check-in-at-standing-rock-tell-us-about-online-advocacy-68276.

Voices-Voix. 2017. Criminalization of Indigenous Communities. *Voices-Voix*, August 1. Accessed December 30, 2018. http://voices-voix.ca/en/facts/profile/criminalization-indigenous-communities.

Waltzman, Rand. 2017. *The Weaponization of Information: The Need for Cognitive Security*. Testimony Before the United States Senate Armed Services Committee, Subcommittee on Cybersecurity, April 27. The RAND Corporation. Accessed December 30, 2018. https://www.rand.org/pubs/testimonies/CT473.html.

Whyte, Kyle. 2017. The Dakota Access Pipeline, Environmental Injustice, and U.S. Colonialism. *Red Ink: An International Journal of Indigenous Literature, Arts, & Humanities* 19 (1): 154–169.

Woodworth, Mike, and Stephen Porter. 1999. Historical Foundations and Current Applications of Criminal Profiling in Violent Crime Investigations. *Expert Evidence* 7 (4): 241–264.

Reflection III

Blayne Haggart

The two chapters discussed here, by Debora Halbert, and by Jenna Harb and Kathryn Henne, are a little unsettling. Halbert's chapter on the weaponisation of copyright forces us to consider whether censorship is sometimes legitimate and politically justifiable. And beyond that, she argues that we routinely engage in de facto censorship via copyright but often do not recognise it as such because it is seen as a legitimate exercise of a copyright owner's rights. Harb and Henne, meanwhile, tackle the state use of disinformation and misinformation to securitise and delegitimise marginalised groups and their concerns, in this case Indigenous peoples and groups protesting infrastructure projects in Canada and the United States.

The uneasiness that emerges from these chapters comes from the reality that the regulation of knowledge (as through copyright) *necessarily* involves censorship, which does not fit well with liberal-democratic sensibilities. Similarly, thinking about misinformation and disinformation as forms of knowledge seems like a misnomer—shouldn't they be considered

Thank you to Brad Sherman, who served as the discussant for the chapter by Halbert and whose comments informed this reflection.

B. Haggart (✉)
Brock University, St. Catharines, ON, Canada
e-mail: bhaggart@brocku.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_10

to be something like "anti-knowledge"? In confronting these issues, we are not just thinking about who profits from strong copyright law, or how surveillance can be used to oppress marginalised groups in the name of state security, although these are key components of copyright law and state surveillance, respectively. Rather, we are engaging with deep, fundamental questions about how we perceive reality. From a Strangean perspective, these chapters are both about the creation and construction of legitimacy in deciding what counts as knowledge. Even more troubling, they suggest the extent to which what we consider to be truth, beliefs and reality is contingent and subject to the exercise of (structural) power.

In Harb and Henne's case, the ability of the state to control the narrative and spread misinformation and disinformation about the less-powerful clearly fits within Susan Strange's knowledge structure, namely, the power to influence "what is believed (and the moral conclusions and principles derived from those beliefs); [and] what is known and perceived as understood" (1994, 119). To use Bannerman and Orasch's terminology (this volume), it addresses the power to construct ideas and beliefs. It's telling that the frameworks proposed by Strange, and elaborated upon by Bannerman and Orasch, can be read in a way that does not require that there be a "truthful" correspondence between knowledge/ideas/beliefs and an underlying "reality." Rather, perceptions of truth are the outcome of power relations. Harb and Henne explain how power shapes perceptions of reality, and how more powerful actors (such as the state) have the ability effectively to shape what we accept as reality. They are illustrating how legitimacy is socially contested even as it works in the service of social control. While the state's vast resources give it a relative advantage in framing marginalised groups' intentions, these same groups can and have challenged this authority, including by appealing to "information" to combat "disinformation."

The question of legitimacy also weighs heavily over Halbert's consideration of copyright's far-reaching effects as a regulator of culture and society, and her contribution could not be more timely. Around the world, governments and societies are confronting the scourge of "fake news" (which we can also think of, in a nod to Harb and Henne, as disinformation) and violent racist and misogynistic speech online that many see as a threat to society (such as how the anti-vaxxer movement has led to the re-emergence of previously controlled deadly diseases (Smith and Graham 2017; Dubé et al. 2015)), and liberal democracy itself (The Economist 2017), to say nothing of the negative personal toll such attacks often have on individuals.

Copyright, in Halbert's telling, brings us into direct contact with the dilemmas posed by the spread of disinformation and hate speech. In particular, she draws an unsettling equivalence between copyright's effects on creative expression and its potential to fight hate speech. In doing so, she confronts a tension, not only within the law, but within her own beliefs regarding freedom of speech. Halbert has long been concerned with copyright's stifling effect on free expression (e.g., David and Halbert 2015; Halbert 2014). She is not alone in this perspective: there is a veritable cottage industry of scholars and activists who have challenged the push for ever-stronger copyright protection on the grounds that it impedes freedom of expression.[1] As Halbert is American, it is worth pointing out that her perspective is very much in line with the premium placed by the U.S. Constitution on freedom of expression via the First Amendment. Even though we tend to think of censorship as something that governments do to political speech, it is relatively easy to see copyright as a form of cultural censorship if we start from the perspective that emphasises copyright's stifling effects on the spread of knowledge and culture.

This normative (and commendable) commitment to free speech and opposition to laws that stifle creativity explains why thinking through copyright's politically censorious use in the Pepe and PewDiePie cases are so troubling for Halbert and others. Confronting the ways in which using copyright (legitimately, or at least legally) to shut off certain forms of cultural expression is similar to how it has been used in these cases (to stifle socially destructive hate speech) requires considering the possibility that censorship (cultural? political? both?) can be legitimate and politically justifiable. And if this is so, then where should we draw the line? This is a hard question, for which there is no easy answer.

In the United States, as Halbert notes, the use of Pepe the Frog for racist purposes can be seen, from a copyright perspective, through the lens of whether its use is "transformative" and thus likely acceptable under American copyright law. If one is in favour of encouraging creativity and weakening copyright law, does this require supporting *all* transformative uses? Even those undertaken in the service of a hateful ideology (the alt-right) that is closely allied, if it doesn't overlap completely with, a white supremacism that perpetuated centuries of slavery in the United States and today still continues to oppress millions of African-Americans? And beyond these stark moral questions, it is worth noting that the question of

[1] As this page of "Anti-copyright resources" suggests: http://praxeology.net/anticopyright.htm, accessed November 30, 2018.

transformative use as a defence against copyright infringement here is being made in a particular national context: other countries draw different lines around these issues, as well as those regarding hate speech, reflecting (as Strange would likely note) their particular power configurations and views of what knowledge and beliefs are considered to be legitimate.

In thinking through the questions of regulating speech (and culture), in this case one must also address the fact that copyright, at least in the U.S. context in which it is primarily a form of economic regulation, was never intended to settle such moral questions. Even this mismatch is revealing. As has been mentioned several times in this volume, the regulation of knowledge is a fundamental form of structural power. In that light, the fact that U.S. law very tightly regulates commercial speech (through intellectual property law) while leaving hate speech, even with its attendant ills (Calvert 1997), largely unregulated reveals a great deal about the relative importance to U.S. society of commercial speech and the relative lack of concern with the effects of hate speech (which tends to target marginalised groups).

However, simply arguing that copyright is a commercial law that should not be applied to deal with moral issues does not get us very far. By highlighting how copyright shapes culture, Halbert brings us back to copyright's de facto role as a tool that by its very nature censors culture. Copyright itself may not be the appropriate legal tool in this particular hate speech situation, but again, if we're fine with censoring in one context (online hate speech), should we be okay with it in another (culture)?

By highlighting the fact that copyright rules shape cultural expression, and that not all forms of expression are socially advantageous, Halbert forces us to consider that "free speech" may not be a foundational value to which we can turn when thinking about these issues, or at the very least it cannot function as a moral absolute. We need rules to govern forms of expression. These do not have to take the form of hard law: prior to World War II, many such issues regarding copyright were settled by groups outside of the legal system, such as the U.S. 1935 *The Gentlemen's Agreement*, which was a voluntary agreement that set guidelines for the limits of acceptable reproduction of copyrighted materials on behalf of scholars (Hirtle 2006). But as Strange would remind us, rules governing the legitimation, creation, use and diffusion of knowledge are inescapable—the only question is who is going to make them, and in whose interest.

In the end, this is where Halbert leaves us (and, one senses, herself). If unrestricted speech is not a morally absolute value, and if censorship—

rules restricting creativity and speech—can be socially and politically legitimate in some cases, what should we do? Halbert leaves us not with answers, but with a starting point for future debates: That we see copyright as speech regulation, that free speech and cultural expression are vital but that some speech should be legitimately censored.

The question of power is never far from the surface of Halbert's chapter—the power to censor a YouTube channel, to undertake an expensive lawsuit that expands copyright to include the "feel" of a song, and of course to set copyright law itself. The state here stands in the background, exerting structural power in the form of copyright law itself, and as the entity to which people appeal to regulate the online platforms upon which disinformation, hate speech and copyright infringement proliferate. Yet while Halbert's argument suggests that the power of the state can be used to legitimise knowledge to promote a social good, such as by banning hate speech, Harb and Henne provide a forceful reminder that this same knowledge-legitimising power can be used to set the context through which people see the world, including to perpetuate the marginalisation of specific groups, in this case Indigenous peoples living in Canada and the United States.

Most of the other chapters in this volume focus on knowledge-regulation and knowledge itself (including systems of communication, as in Winseck's chapter). Harb and Henne, for their part, examine the use of knowledge to govern, with a particular focus on its mobilisation—and even arguably weaponisation—against the stated interests of marginalised group identities. They thus build upon the constitutive or beliefs aspect of Strange's knowledge structure (Haggart, and Bannerman and Orasch, this volume). The power to shape identities—to shape how one knows other individuals and groups—is about as pure an example of structural power (in Strange's use of the term) as one can imagine. In their contribution to this volume, Harb and Henne explore how the Canadian and U.S. states used their power to shape the identities of Indigenous groups protesting the implementation of natural-resource projects on and passing over their lands.

What stands out in their account is the state's interest in and effectiveness at identifying Indigenous protesters as categorically suspect, presenting them as a security threat to the state. The state's success in promoting this perspective depends on the ability to control access to the information gathered by the state (via surveillance) about the protesters. If the state is surveilling a group and making claims about the group that are unverifiable

because they are treated as national-security secrets, it becomes much easier for the state to monopolise a society's view of that group. This control of the means of surveillance and over the mechanisms by which knowledge is diffused (in this case access to information requests blocked on national-security grounds) means that the group becomes effectively knowable by others only through those who dominate the knowledge structure: in this case, the state, which is also working to protect corporate interests.

Harb and Henne point out how the supposed national-security threat posed by Indigenous protesters is grounded in what they call disinformation about their actual objectives, which they note are rooted in concerns about their sovereignty, and which the protesters, unlike the police, would almost certainly not characterise as vague. Because of the state's key role in society, this disinformation (which might also be understood as aggressive or motivated misunderstandings) has the effect of "maintaining a longer trajectory of settler colonial governance of Indigenous peoples: their continuance of sanctioned monitoring and ongoing discrimination" (Harb and Henne, this volume). As with hate speech leading to violence, control over the knowledge structure affects the lives of actual people in very real ways. Importantly, they argue that these tactics, while seemingly new and enabled by surveillance technologies, are part of and continue longer settler colonial traditions of this type of domination.

Phrased in this way, this form of control can appear to be unbearable and inescapable. However, despite their analysis, Harb and Henne do not end up in such a bleak place. Like Halbert, they note that the strategic construction of legitimacy in knowledge—of group identities or of what knowledge is considered to be "appropriate"—is inextricably wrapped up in power relations exercised with particular historical contexts.

Although asymmetrical power relations are shaping the construction of legitimacy, the state is not the only actor that has agency in this story. Harb and Henne point to Indigenous protesters' use of technologies, such as drones and social media, to challenge the state's assertions via their own strategic use of surveillance and information. Even more importantly, while the perception of particular ends as legitimate is itself the outcome of power relations (as in the state's appeals to national security in dealing with Indigenous protesters): this legitimacy is also open to political contestation. Halbert makes this point by highlighting the political nature of copyright law; Harb and Henne embody it by in essence challenging the legitimacy of the Canadian and U.S. states' securitisation play.

However, while Harb and Henne frame their chapter in terms of injustices done to Indigenous peoples (and it is hard for us to object to this framing), Halbert's normative question remains unanswered. Where do we draw the line between speech and censorship? What makes for a "legitimate" identity? And, given the complexity of these issues, how do we decide? Certainly, understanding that these issues are grounded in power relations is important, but it is only a starting point. Strange's structural-power approach tells us *how* power works, while leaving unresolved the choice of ends, and the question of what constitutes justice. In their case studies, Harb and Henne convincingly argue that the Canadian and American governments are acting unjustly in their attempts to define Indigenous peoples. However, as Halbert's discussion of hate speech suggests, sometimes it is perfectly just for the larger society to describe a group in negative terms: sometimes you have to call a Nazi a Nazi, regardless of how they attempt to justify their particular hatred. Taken in this way, the right to self-identify, as with the right to free speech, emerge not as a guiding absolute, but as issues subject to normative and political contestation. The value in these two chapters is that they make us aware of this omnipresent debate and thus allow us to add another layer to our own research: where the norms underlying particular legal frameworks come from, the relative power of state and non-state actors[2] in setting these norms (and the often-unbalanced resources they hold to do so), and in whose benefit they operate.

References

Calvert, Clay. 1997. Hate Speech and Its Harms: A Communication Theory Perspective. *Journal of Communication* 47 (1): 4–19. https://doi.org/10.1111/j.1460-2466.1997.tb02690.x.

David, Matthew, and Debora Halbert. 2015. *Owning the World of Ideas: Intellectual Property and Global Network Capitalism*. Thousand Oaks, CA: SAGE Publications Ltd.

Dubé, Eve, Maryline Vivion, and Noni E. MacDonald. 2015. Vaccine Hesitancy, Vaccine Refusal and the Anti-Vaccine Movement: Influence, Impact and

[2] Specifically, they ask us to consider the balancing-act relationship between the state and non-state actors when it comes to exercising structural power, with Harb and Henne paying particular attention as to how the state's monopoly over the legitimate use of violence fits into this balance.

Implications. *Expert Review of Vaccines* 14 (1): 99–117. https://doi.org/10.1586/14760584.2015.964212.

Halbert, Debora. 2014. *The State of Copyright: The Complex Relationships of Cultural Creation in a Globalised World*. Oxford and New York: Routledge.

Hirtle, Peter. 2006. Research, Libraries and Fair Use: The Gentlemen's Agreement of 1935. *Journal of the Copyright Society of the U.S.A* 53: 545–546.

Smith, Naomi, and Tim Graham. 2017. Mapping the Anti-Vaccination Movement on Facebook. *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2017.1418406.

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

The Economist. 2017. Does Social Media Threaten Democracy? *The Economist*, November 4. https://www.economist.com/leaders/2017/11/04/do-social-media-threaten-democracy.

PART IV

Surveillance and Knowledge and/as Control

Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India

Kathryn Henne

As other chapters in this book attest, knowledge is often central to the mobilisation of structural power. In focusing on knowledge, it is important to consider *what* and *who* can exercise such power and *how*. Structural power, according to Susan Strange (1998), sits with actors who can influence and exert control over people's livelihoods and security, including the modes of accessing essential services. Here, I examine how two key features of structural power—that is, knowledge and authority—coalesce in the context of social assistance provision. State-supported welfare systems hinge on the collection of significant amounts of personal information, using data to monitor beneficiaries' behaviour and to assess their compliance with the conditions of receiving assistance (Eubanks 2018). Accordingly, they rely on a wide range of technologies and techniques to manage and administer benefits and payments. In short, it depends on surveillance—that is, "the focused, systematic, and routine attention to

K. Henne (✉)
University of Waterloo and Balsillie School of International Affairs, Waterloo, ON, Canada

Australian National University, Canberra, ACT, Australia
e-mail: khenne@uwaterloo.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_11

personal details for purposes of influence, management, protection or direction" (Lyon 2007, 14). Social assistance offers a domain of governance where we can observe, document, and trace both striking and mundane aspects of leveraging knowledge in the exercise of structural power. In this context, governance relies on knowledge about subjects, but it is not complete knowledge of their lived conditions; rather, governance here relies on isolated forms of data that can be extracted through biometric technologies. As this chapter illustrates, surveillance becomes a key mode through which authorities come to know subjects, shaping how they are treated.

While the targeted surveillance of marginalised populations is not new (see Gilliom 2001), the proliferation of monitoring techniques and verification mechanisms in the context of welfare provision has received greater attention in recent years. A number of countries have expanded—and are continuing to expand—their practices of tracking and authenticating social assistance recipients, using a range of technologies to do so. For example, in the United States, mechanisms for discerning welfare recipients' bought goods, tracking their employment opportunities, and sharing data across administrative agencies are commonplace, as are risk-analysis and predictive tools for assessing their current and future circumstances. The Australian government has proposed expanding trials for welfare card programmes to limit individual purchases and has sought to mandate drug testing as a condition of social assistance. South Africa has added biometric authentication to its social benefits cards, 19 million of which have been supplied to welfare recipients since 2012, with a range of countries—including Ireland, Trinidad and Tobago, and the Philippines—following suit. The Unique Identification Authority of India (UIDAI), established in 2010, has issued over one billion unique identifier numbers (or "Aadhaar") for use across several government assistance programmes. Although distinct jurisdictions, authorities evoke similar justifications, such as fraud prevention and cost savings, for introducing new monitoring and authentication technologies in the context of social assistance. In doing so, the disproportionate surveillance of citizens who are often poor, vulnerable, and sometimes multiply marginalised becomes enabled through narratives of transparency, accountability, and good governance.

Developments in social assistance, I argue, demonstrate Zeynep Tufekci's claim that the engineering of social life is "a political process involving questions of power, transparency, and surveillance" (2014, 1). To illustrate how socio-technical entanglements emerge in the form of surveillance and convey structural power, this chapter focuses on the making and maintenance of data-intensive infrastructure to support state social

assistance systems, using India as its central case. Its analysis of Aadhaar examines how surveillance enabled through unique identification numbers constitutes a distinct mode of governance, one that depends on the pursuit of particular kinds of knowledge. After doing so, I consider how these practices evince broader shifts in which state actors, as well as non-state actors working in the service of state interests, create and sustain the conditions for regulating subjects.

Although its focus is on India, the chapter illuminates potential issues with and limitations of these hybridised formations of governance more generally. Hybridity, at least in relation to law and regulation, typically refers to "synergies between binding and non-binding mechanisms" that support governance functions (Trubek and Trubek 2005, 344). In this case, UIDAI is part of an amalgamated machinery that is supposed to streamline service delivery through data collection and verification; however, as elaborated upon in later sections of this chapter, India's biometric management system has had notable failings. As a networked assemblage, it has the capacity to short-circuit. I use "assemblage" here to flag that although Aadhaar can be thought of as infrastructure, it is actually constituted as a "multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they work together as a functional entity" (Patton 1994, 158). Assemblages can materialise through events, but they are not fixed or stable; they can fluctuate along different registers that cross time and space. Thus, in addition to concerns of technocratic utility, the scrutiny of Aadhaar offers a space in which we can glean insight into how nationalist agendas and inequalities inform the terms and conditions of biometric surveillance systems and how they materialise in citizens' lives in differential ways.

In particular, this chapter discusses how UIDAI's one-way expectation of transparency, which is aimed at recipients of social assistance, illustrates how knowledge and authority coalesce in the contemporary expression of structural power. It shares Strange's appreciation of granular analyses, as Germain elaborated earlier in this book, as a necessary mode of interrogating the details of a concern in order to understand its material effects. Here, I consider some of the intricacies through which power is being fashioned while retaining critical focus on the "big picture" as Strange would. However, and distinct from Strange, I do so in a way that accounts for entanglements of technologies, bodies, and social categories of difference, which are reflective of interlocking systems of inequality and oppression that are part of the Indian state. The argument put forth here departs

from traditional Strangean analyses found in International Political Economy. Unlike Strangean analyses' tendency to overlook questions of gendered inequality, I embrace feminist calls to look at how "surveillance is integral to many of our foundational structural systems, ones that breed disenfranchisement, and that continue to be institutionalized" and to critically attend to how "underlying structures of domination" inform surveillance activities (Dubrofsky and Magnet 2015, 7). This chapter therefore attends to a wider range of structural formations of difference, including race and racism as well as gender and sexuality, as it examines the exercise of state power.

The remainder of the chapter proceeds in four parts. The first section discusses the longer trajectory of states using knowledge about its residents as a central method of governing populations within its jurisdiction. A reflection on specific contours and features of India's national identification initiative follows. The next section considers the specifics of Aadhaar in relation to insights gleaned through the literatures on surveillance, transparency, and governance, explaining specific contributions from the Indian example. I conclude by contemplating this case study's implications for how we think of knowledge, particularly its role in the growing range of practices that can be understood as *biogovernance*, which generally speaking, is the governance of populations and individual humans through science and technology.

1 How States Come to Know and Govern Citizens

Nation-states have longstanding practices of identifying, monitoring, and sorting their residents, employing various mechanisms to do so. Their strategies have involved individual identification and authentication techniques, such as biometric-based technologies, as well as population-based approaches. For example, reflecting on the United States, David Theo Goldberg (1997, 33) explains that "the national census is as old as the republic itself" and that delineating different groups within the population is central to governing apparatuses, particularly "the distribution of federal resources." Goldberg (1997) emphasises that while these practices are often framed as being for the benefit of the nation, they often reaffirm difference, particularly racial difference, among subjects. Simone Browne (2015) elaborates upon this observation in relation to historical and contemporary modes of surveillance. Specifically, she states, surveillance operates as a "technology of social control" that "exercise[s] a 'power to define

what is in or out of place'" (Browne 2015, 16). In other words, population governance through surveillance can be thought of as an articulation of structural power, one that can reproduce and perpetuate inequalities. On the surface, this foundational form of biogovernance may appear objective and apolitical; however, upon further reflection, it demonstrates the shaping of the agendas and institutional terms through which states, peoples, and other actors can relate to each other. It ultimately reflects the ability to "decide how things shall be done" (Strange 1998, 24–25).

The expansion of national identification systems offers an opportunity to further explore the tensions that emerge in the push to collect and analyse data about individual members of the population. Today, many states maintain elaborate identification systems to track and distinguish citizens and non-citizens, with widely accepted documents, such as passports, serving as longstanding tools of authentication (Torpey 2009). To buttress these systems, many jurisdictions have embarked on "modernising" them by including practices of biometric authentication (Lyon 2013), which use data collected to document a person's unique physiological characteristics—most commonly, fingerprints, facial features, irises, and retinal veins—to verify identity. The enthusiasm for new national systems of biometric identification across jurisdictions, according to David Lyon (2013), has enabled new approaches to population management, many of which rely on unprecedented levels of digitised data generation. Part of a broader post-9/11 trend in which governments are expanding the biometric verification of both foreign- and native-born residents (Gates 2011), this shift has led to greater private, corporate, and non-state involvement in the creation and sharing of information about individuals. In doing so, writes Btihaj Ajana (2010, 237), "bio-digital samples" of human beings have become the basis for evaluating subjects, their identities, and their relationship to the state. The enhancement of identification systems may promise more stable modes of population management through claims of accuracy and objectivity; however, they come with risks that are especially relevant to groups who occupy marginalised social positions—even though such risks are not always evident in everyday life. With the expansion of surveillance, we need to cultivate a "critical biometric consciousness" that is attentive to the unintended effects of these technologies (Browne 2010, 132). This issue is particularly important as such technologies posit truth-claims about bodies and identities in ways that may direct attention away from larger issues of inequality.

Concerns of inequality are especially relevant to the surveillance of social assistance recipients and arguably the poor more generally. Many people who receive welfare are subject to multiple regulatory systems that collect and triangulate data on their individual needs, consumption patterns, access to resources, and compliance with the rules and conditions of receiving social assistance benefits. These arrangements, according to Torin Monahan (2017, 193), can "regulate the practices and subjectivities of the various 'clients' they serve," often making moral assessments that can underscore "the stigma of being on welfare" and "suspicion of deficiencies with one's character." With the collection and tabulation of data, suspicion can become embedded in ways that can have problematic outcomes for those who are subject to multiple forms of surveillance. For example, Virginia Eubanks (2018) has documented how governments' embrace of automated systems can result in judgments based on errors in data collection and analysis, with life-threatening implications for those who are dependent upon social services. Social assistance recipients in particular are entangled within the fabric of these networked schemes, which Eubanks (2018, 175–190) describes as constituting a "digital poorhouse" that is woven together by fibre-optic strands. By this, she means the surveillance of those most in need of services prompts the threads to wrap more closely—and potentially more tightly—around them. Just as importantly, while individual circumstances may change or there may be errors in the data collected, the data do not necessarily change or disappear accordingly. The imprint may remain hardwired in the network. Representations of social assistance recipients can render them hypervisible to authorities, especially compared to other citizens who do not have their data harvested and cross-checked by other surveillance systems on a regular basis. It therefore increases the likelihood of losing support for noncompliance or becoming subject to other forms of state control.

Browne (2015), Monahan (2017), and Eubanks (2018), like many other scholars of surveillance (e.g., Magnet 2011; Staples 2014; Guzik 2017), stress the potentially dangerous consequences of data-driven population governance, emphasising how their reliance on monitoring individuals often perpetuates structural inequalities. In contrast, advocates for Aadhaar, the unique identification number (UID) for residents of India, argue the opposite point: that the tracking and verifying of residents can help to counteract and alleviate persistent inequalities by ensuring they receive essential services. Specifically, the introduction of Aadhaar responds to failures in social assistance delivery and allegations of identity fraud. The programme assigns

a 12-digital UID to collect demographic and biometric data, including iris scans, facial pictures, and fingerprints, which can be linked to access services, such as food rations, subsidies, pensions, and other financial services. International observers have praised the programme's sophistication, attributing Aadhaar with making "it simpler and more secure for poor people to do business with banks" (Bill and Melinda Gates Foundation 2017) and for supporting cost savings of up to US$11 billion per year (World Bank 2016, 195). In fact, experts, such as Paul Romer, a former World Bank Chief Economist, have promoted it as a model for other countries to adopt (Doshi 2018). With widespread support and seemingly evident need, does Aadhaar—a programme introduced in a country where some speculate that only half of births are registered—overcome the critiques that scholars have levied at data-driven governance? The next section of this chapter outlines some of the purported strengths and limitations of Aadhaar by considering its establishment, its expansion, and its technocratic malfunctions.

2 The Aspirations and Shortfalls of National Identification Systems in India

When the Congress Party-led government launched Aadhaar in 2009, it promoted biometric identification, verification, and authentication as a voluntary option, one that would benefit those seeking welfare benefits and food subsidies. Previously, the other major party, the Bharatiya Janata Party (BJP), had criticised the programme when it was in opposition. Since coming to power after the 2014 election, the BJP has actually expanded Aadhaar and its use. In fact, verifiable UIDs became a requirement for accessing various public services and for conducting many private financial transactions. Authorised under the *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016* ("*Aadhaar Act 2016*"), UIDAI, the statutory authority tasked with the programme's oversight, has a mandate to issue UIDs to all residents of India; to eliminate duplicate, false, or otherwise inaccurate forms of identification; and to ensure that cost-effective and user-friendly modes of authentication are in place (Government of India 2016). An ambitious project, Aadhaar covers 1.12 billion people, nearly 99 per cent of the adult population in India (Digital Dawn 2017), making it the largest biometric identification programme in the world. It is also a visible, and arguably foundational, component of the Indian government's "Digital India" initiative to

enhance the nation's online infrastructure and to expand internet access across the country. To understand how Aadhaar is an expression of structural power therefore requires considering its place within and alongside state agendas.

2.1 Establishing a National Identification Authority in India

Recognising that a large number of people in need of services were either not registered at birth or lacked basic identity documents, the Indian government opted for a biometric system to establish verifiable identities. The programme was meant to be a comprehensive response to a widespread problem often referred to as "leakage," meaning that funds did not reach the correct beneficiaries, with some being taken by someone acting on their behalf (Singh 2017). In fact, one estimate suggested that only 27 per cent of funding went to the correct recipients. The incentive for individuals to enrol in Aadhaar was the promise that it would ensure the streamlined and guaranteed delivery of welfare provisions while also removing fraudulent information and go-betweens who may take a cut of funds intended for the recipient. Critics of Aadhaar, including noted Hindu nationalist Narendra Modi before he became prime minister in 2014, characterised it as a "political gimmick" at worst (Narendramodi 2014) and too expensive to be practical at best (Singh 2017). Despite these challenges, the programme proceeded with Nandan Nilekani, an entrepreneur who co-founded and co-chaired Infosys Technologies, as the chairman of UIDAI.

The choice of Nilekani to lead the UIDAI is interesting, but not necessarily surprising. In his 2009 book, *Imagining India*, Nilekani discusses the benefits of UIDs, characterising them as a foundational reminder of citizens' "rights, entitlements, and duties" and the state's obligations to provide them. He also frames them as the potential way to enable more Indians to open bank accounts and participate in more economic activities. His presentation of UIDs is a direct response to earlier government ideas that promoted an identification programme in the interests of border security.

The development of Aadhaar—which means "foundation" in Hindi—embraced Nilekani's more liberal envisioning, which became reflected in its branding: a fingerprint logo in the shape of the sun. Distinct from other welfare-delivery programmes, it did not advance overt or "new paternalist" platforms observed elsewhere (e.g., Australia, the United States), which often use surveillance to monitor and enforce conditions on social assis-

tance recipients under the guise of encouraging more responsible behaviours among them (see Dee 2013). In contrast, Aadhaar was not so much about monitoring or scrutinising the actions of the poor, but instead, ensuring the validation of identities so that all Indians could receive their allotted entitlements. Those allowances were—and still are—far from generous, though, as India only spends 1.7 per cent of its GDP on social support, which is much lower than its lower-middle income neighbouring countries (3.4 per cent) and China (5.4 per cent) (Drèze 2014).

Aadhaar, as a large-scale digital infrastructure project, required both technical and political labour. With the establishment of the agency in Delhi and the technological branch in Bangalore, Nilekani's team included bureaucrats as well as engineers with experience working in Silicon Valley and for major multinational technology companies, such as Google and Intel (Parker 2011). In order to verify biometric information, the design of the system relies on the ability to millions of comparative alignments, which requires the use of algorithmic assessment enabled through partnerships with Accenture, L1, and Morpho (ibid.). At its core, Aadhaar is a hybrid. Even though it is led by UIDAI, a state authority promoting state interests, it draws heavily from private-sector expertise and tools.

2.2 Implementing and Expanding Aadhaar

The rollout of the national identification scheme was a notable success in terms of its reach, with authorities registering participants at a rate much faster than anticipated in initial targets (Sathe 2014). The issuing of the first Aadhaar number in September 2010 to a woman living in rural Maharashtra received much publicity, even though she later reportedly stated that her UID had little value if the provisions it ensured were not enough to end one's hunger (Parker 2011). By mid-2013, the government had issued UIDs to 350 million people and established 500 operational service centres, with plans for doubling the number of centres nationwide before the year's end (Kumar 2013). By March 2014, the average authentication rate was 300,000 identities per day (Sathe 2014). Additionally, authorities expanded verification through mobile-based password services and business authorisation services (ibid.). There were, however, stated concerns about whether Aadhaar would actually undermine the Public Distribution System (PDS), which provides subsidised goods to the poor. As the biometric system requires delivering money into bank accounts rather than providing foodstuffs directly, it placed new demands on banks that had

previously not had to service a wide range of customers, and many recipients had to start paying market prices (Parker 2011). In hindsight, these shifts in service provision were only the beginning of the changes enabled by Aadhaar.

Although designed to support social assistance delivery, the use of Aadhaar has expanded significantly in recent years. By early 2017, the BJP-led government had mandated its use for various programmes and schemes, including for tax compliance, bank account usage, educational scholarship awards, public Wi-Fi access, pension payments, and maternity benefits (Ghoshal 2017). Prime Minister Modi, previously a vocal opponent of the UID system, has shifted his stance to actively promote efforts to make Aadhaar mandatory for accessing most government services. In fact, Aadhaar has emerged as a foundational component of the BJP's governance plans, which include the wider digitisation of services, particularly through its suite of software applications, which are bundled as together as India Stack, a digital application project interface intended, according to its website, to enable "governments, businesses, startups and developers to utilise an unique digital infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery" (India Stack 2018).

With the stated aim of bringing more Indians into the formal economy, India Stack is supposed to remove barriers and "friction" they may face in terms of access. It entails four layers, the first of which is the "presenceless layer," which is facilitated through the achievement of a "universal biometric digital identity" enabled by Aadhaar, the foundation that would enable verification of anyone so that they can access a service from any location in the country (India Stack 2018). The second layer is "paperless," which is intended to remove challenges associated with the storage and reliance on physical paper for documentation and verification, while the third layer is "cashless," a measure to broaden access to bank accounts—a move framed as "democratizing payments" (ibid.). The fourth layer, "consent," is to ensure to the free and secure movement of data, including personal biometric information and other relevant linked information.

Critics have described Aadhaar, particularly its role within the wider digital architecture, as the foundation of a surveillance state (e.g., Ganesh 2018; Khera 2018). They have been quick to cite research indicating that Aadhaar has not fixed problems of social assistance delivery; rather, in some areas, it has exacerbated food insecurity (see Khera 2018). In contrast, within two years of implementation, government reports indicate a

cost savings of US$8 billion, which reportedly far surpass the US$1 billion cost of Aadhaar (Digital Dawn 2017). Regardless of outcomes, it is clear that the use of UIDs now extends well beyond their originally stated purpose. This development fits scholarly assertions that surveillance measures targeting the poor are often the precursor for future practices targeting the public more generally (Eubanks 2018).

As Aadhaar becomes linked to more databases through the delivery of public services, the completion of private transactions, and increased digital interconnectivity, the likelihood of other entities accessing identifying information too increases. The 2016 *Aadhaar Act* permits this practice, as a "requesting entity" (any "agency or person" willing to pay the required fee) can ask for demographic information related to one's identity as long as it is not the actual biometric data collected (UIDAI 2016). Given the embeddedness of Aadhaar, few Indians can refrain from using it—certainly not the poor who need access to essential services and rations.

Although many residents must use Aadhaar, it does not mean doing so is always easy. As Reetika Khera (2018) observes, the fact that one has to have a UID and ensure that it was linked correctly to different accounts can be an obstacle when trying to obtain social assistance. There are multiple reports of services being denied, including food, medical services, and education, because the intended recipient cannot authenticate their identity, which can be the result of administrative errors, failed biometric verification, inconsistent internet connections, or simply an individual's inability to link accounts. Khera (2018), for instance, recounts the death of an 11-year-old girl after being removed from the subsidies registrar due to the government's failure to link her Aadhaar to her ration card. Others cite the case of the man who was able to get an Aadhaar for his dog (e.g., Dixit 2017a). Further, older and disabled populations can no longer rely on someone else to obtain their rations, since verification now requires their physical presence.

There are also positive stories associated with the expanded use of UIDs, such as reports that poor residents felt that Aadhaar had an equalising influence: since more affluent residents had to sign up on their own (as servants cannot complete the enrolment process for them), they were forced to do so alongside Indians of different backgrounds and social status (see Sathe 2014, 86). In a country that still has rigid social divisions, some of which are solidified through caste, the notion that all residents would have Aadhaar and that it would be a means for giving the poor greater access to financial institutions had symbolic meaning for some. It

offered a seemingly more "open" approach to a historically closed society (ibid.). Further, more residents can have bank accounts and thus access income through direct and confirmable deposits. Regardless, while some reports emphasise these benefits alongside claims of cost savings and successful anti-corruption reforms, Aadhaar has come with unforeseen and undesirable trade-offs, which the next section describes.

2.3 Short-Circuits in the National Identification Infrastructure

The widespread implementation of UIDs has faced both legal and technical obstacles. On three separate occasions between 2013 and 2015, the Supreme Court of India reaffirmed that Aadhaar was to remain a voluntary programme (Ghoshal 2017). Thus, the ruling countered the BJP-led government's efforts to mandate UID verification for many services. Unfortunately, though, it followed the widespread practice of doing so. More recently, in August 2017, a ruling by the Supreme Court took a stronger stance relevant to Aadhaar: it asserted for the first time that privacy is "an intrinsic part of Article 21 that protects life and liberty."[1] In doing so, the Court overturned two previous rulings that aligned with government assertions that privacy is not a fundamental right—and thus not a relevant concern for the current or expanded use of Aadhaar. In contrast, the recent decision, which was a unanimous ruling by a nine-judge panel, framed privacy as an expansive protection that applies to one's home life and domestic relationships, sexual orientation, and bodily integrity (Guruswamy 2017). It not only may have bearing on the 30 ongoing challenges specific to Aadhaar, but it also enshrines a legal right that may provide a defence against other government actions, now and in the future, given the current political climate in India. The BJP, which has been in power since 2014, has sought to regulate—and arguably control—various intimate and embodied practices related to gender and sexuality, marriage, religion, and food (ibid.). While the full implications of this ruling are not yet realised, it paves the way for various constitutional challenges, including the successful overturning of Section 377 of the Indian Penal Code in 2018, which decriminalised homosexuality across India, and prohibitions on alcohol and beef consumption in some parts of the country.

[1] *Justice K. S. Puttaswamy (Retd.) and Anr.* vs *Union of India and Ors* (2017) 10 SCC 1. Specifically, it holds that the right to privacy is protected under Articles 14, 19, and 21 of the Constitutions.

Beyond legal contestations around Aadhaar, technical issues have given rise to other concerns, with more recent developments fuelling worries about access, privacy, and the security of personal data. For example, in terms of access, when it became mandatory for Aadhaar to be linked with PAN (the Permanent Account Number given to each taxpayer in India), complications emerged for citizens who do not fit in binary gender categories. Whereas Aadhaar captured transgender identities, the PAN application form only allowed for "male" and "female" options (Sharma 2018). As such, an entire group of citizens[2]—those whose have registered their identity as transgender with Aadhaar—could not comply with the new requirement. Additionally, in 2017, researchers discovered a website that contained the UIDs and demographic information of more than 500,000 minors enrolled in Aadhaar (Dixit 2017a). In the same year, reports revealed that more than 200 government websites shared personal details about millions of citizens, some of which was accessible through a basic internet search (Goel 2018). In response to these unauthorised disclosures, sceptics drew attention to a critical point about the *Aadhaar Act* (2016): that it enables levying sanctions for "illegal access" but does not contain adequate provisions for preventing breaches (Dixit 2018). The leaking of data thus drew attention to fundamental flaws in a system that was presented to the public as foolproof.

Security problems persisted into 2018. An investigative report by journalist Rachna Khaira, published in the Indian newspaper, *The Tribune*, documented how she was able to access personal information collected by UIDAI through an agent for merely Rs 500 (approximately US$8) (Khaira 2018). Government representatives denied claims that Aadhaar data was not protected or secure, with the BJP initially characterising the report as "fake news" and UIDAI officials stating her actions were "illegal" and a "major national security breach" (Dixit 2018). Further, the UIDAI's deputy director filed a criminal complaint that implicated Khaira and the newspaper, asserting offences that included forgery and cheating (Safi 2018). The move attracted notable criticism from onlookers who framed it as an attack on independent journalism and freedom of the press, claims to which officials later responded, stating that UIDAI named multiple parties in the complaint, which primarily targeted the unidentified actors who purportedly accessed and sold the data (ibid.).

[2] According to the 2011 Census, 488,000 Indians are transgender.

Authorities such as Ajay Panday, Nilekani's successor as head of UIDAI, have framed system breaches as "inevitable" problems that the agency can fix, while others have reduced their reliance on Aadhaar. For instance, in Delhi, the government has removed Aadhaar as a requirement for food rations (Goel 2018). Irrespective of these responses, the accessibility of private data seemingly confirms privacy advocates' fears. Moreover, they have been exacerbated as companies reportedly planned to follow Microsoft's lead by implementing plans to access demographic information through Aadhaar as part of the conditions of their service provision (Dixit 2017b). These developments have prompted speculation over the nature of Aadhaar's future, even though the national government has yet to step back from plans for its intended expansion of the programme. However, a September 2018 ruling by the Indian Supreme Court[3] suggests that Aadhaar may be here to stay, but likely with some qualifications and possible limits: upholding the constitutionality of the *Aadhaar Act*, including the requirement of a UID as a condition for receiving public benefits and filing taxes, the Court did put limits on how private companies use Aadhaar by striking down Section 57 of the *Act*.

In practice, the 2018 Supreme Court decision means services, such as mobile phone service or banking, cannot be denied on grounds that a customer does not provide a UID, nor can companies and schools disclose UIDs (Bhattacharya and Anand 2018). There are, however, no prescribed remedies provided for those who have already enrolled and submitted UIDs for various public- and private-provided amenities and have had their data shared. Notably, a dissenting judgment,[4] written by Justice D.Y. Chandrachud, addressed data retention, stating that data should be kept for no more than six months, especially in the absence of mechanisms to hold UIDAI accountable for leaking data and ensuring its security. Further, Justice Chandrachud took issue with the majority holding that Aadhaar gives dignity to marginalised citizens, asserting, "One right cannot take away another. Dignity to the marginalised cannot do away with right of a person to bodily autonomy." The 2018 ruling, particularly the

[3] Reports by *The Hindu* and *The Indian Express* include the full text of the ruling, which is available at https://indianexpress.com/article/india/aadhaar-verdict-full-text-judgment-supreme-court-order-5374794/.

[4] Justice Chandrachud stated that the Section 7 of the *Aadhaar Act* is unconstitutional on the grounds that it makes Aadhaar mandatory for state subsidies. Also referring to it as a "fraud on the Constitution," he acknowledged that enshrined guidelines for a Money Bill, indicating that the *Aadhaar Act* exceeds the limits they put forth.

dissenting judgement, highlights that concerns around Aadhaar are still linked to fundamental questions of personhood, citizenship, and bodily integrity, even though its focus on persons are socio-technical and abstracted as data.

3 Insights About Surveillance as/and Governance

In less than a decade, Aadhaar has surpassed its original mandate as a fix for a leaky social assistance system. Instead, it has become a central piece within a larger push to modernise India's digital infrastructure and service delivery—one that builds in knowledge about and verification of Indian identities as the foundation for governance. It fits into a longer pattern of states identifying and delineating subjects in the name of providing for them. Even though the deployment of technologies, be they Aadhaar or other ways of distinguishing subjects, emerges as logical and even productive and beneficial, it is nonetheless an exercise of state power. These practices are not simply about *knowing* subjects, but also about *laying claim* to subjects. They are, according to Allen Feldman (1991, 115, emphasis in original), central to state maintenance: "*(m)other bodies in order to engender itself. The production of bodies—political subjects—is the self-production of the state*." Although employing newer technologies of regulation, Aadhaar continues longer, biopolitical processes of state (co)production. Modi's popularised narratives about Aadhaar, for instance, are quite explicit about the centrality of the biopolitical management to state preservation: it emerges as a foundational aspect of the articulations *and* infrastructure of "Digital India." Biogovernance is a core feature of the state apparatus. In this case, the Indian government purports technological innovation as a key component of its continued development, suggesting it supports a growth-oriented and sustainable trajectory of governance.

While the observation of states using techniques to know and document their subjects is not new, the socio-technical assemblage that constitutes India's changing approach to population governance—of which Aadhaar is a part—is distinct and worth unpacking. Consider, for instance, as Strange would suggest, the materiality of the digital infrastructure involved, including its implications. Recent developments reveal that Aadhaar, as a fix, is itself actually leaky—a feature that is not something that a technical adjustment can remedy. Instead, its problems stem from its materiality, which is, at its core, digital. This digital materiality makes Aadhaar more of a "thing" than an "object": that is, as others have

reflected on in relation to data from self-tracking technologies (Pink et al. 2017, 9), a process that is "always incomplete" and ongoing, something that is open, not closed, a set of relationships that are in process and are being processed. Aadhaar is more than giving UIDs to residents and using data collected about them for verification purposes; it is also more than a national ID initiative. As explained by Maya Indira Ganesh (2018), it "is also a public-private partnership and a government project, critical public infrastructure, a complex socio-technical system, a biometric database, a contested legal subject, and now, a flagrant security risk." In other words, Aadhaar, as a thing, is multiple—and thus so is its leakiness, as it spills into other spaces through verification and sharing, with the prospect of implicating multiple domains of everyday life. The infrastructure itself might be framed as a technically sound whole with tiered layers, but it, including its shortcomings and vulnerabilities, is more diffuse in practice.

The multiplicity of Aadhaar cannot be separated from its entanglements. Harvesting and using knowledge about individual residents takes shape in and becomes part of a larger ecosystem that includes embedded inequalities, such as India's caste system and its reinforcement through endogamy and social exclusion. For example, Right to Food researchers have reportedly tried to track deaths from starvation that could be linked to the denial of food rations following the introduction of Aadhaar (Bhatia 2018). While specific reasons may vary, due either to technical or authentication errors or the inability to be verified in person, a notable pattern emerges, one in which marginalised members of Indian society, "including Muslims, Dalits, and members of remote tribes," are more likely to be among the dead (Bhatia 2018). Such cases reveal what Ganesh (2018) warns about: the "untidy, imperfect interconnections between digital technology, privacy, and the contestations and manipulations of identity" can position Aadhaar as "a tool to perpetuate long-standing and deep-rooted forms of discrimination." Even if well intended, Aadhaar can still be used to serve pernicious agendas, such as the misrecognition of gender minorities or the BJP's promotion of Hindu nationalist beliefs and its enabling of religious fundamentalism. The broader implications are important: that the introduction of technological tools does not necessarily ensure objective or even outcomes. In fact, their implementation alone cannot escape or overcome inequality.

Understanding Aadhaar as leaky and inseparable from historical and contemporary tensions that have shaped the Indian state aids in understanding this particular form of surveillance as an approach to governance.

The embrace of surveillance accompanies a broader shift in governance, which others have described as the rise of the "regulatory state" (Braithwaite 2000). This term captures the increasing tendency of states to exercise power "through a regulatory framework, rather than through the monopolization of violence or the provision of welfare" (Walby 1999, 123). While Aadhaar may challenge this distinction drawn by scholars (since its introduction comes through social assistance provision, not a regulatory framework as such), its wider deployment demonstrates how regulatory frameworks emerge as the formations through which states wield power. As mentioned previously, this case of biogovernance reveals that the preoccupation with authenticating identities is about more than about delivering services; it is about marking political subjects. Knowledge about subjects is a foundation for governance; however, it is not complete knowledge. Rather, as scholars of surveillance have long observed (e.g., Haggerty and Ericson 2000), surveillance enables flows of data, which must be assembled and re-assembled for analysis and intervention. More surveillance, monitoring, and data triangulation may assist those processes, but analysis and intervention rely on representational findings that cannot fully capture human experience in context. In short, the state comes to know its subjects through mediated means, from data that are both extracted and abstracted through technical means. As a result, the nature of state knowledge is incomplete.

Perhaps what is striking about Aadhaar is the state's openness in terms of framing it as a nationalist project. Other studies of state surveillance highlight how a regulatory focus on individualised bodies often draws public attention away from the machinery that continues or perpetuates inequalities, stigmatisation, or oppression (see Lyon 2013; Browne 2015; Dubrofsky and Magnet 2015). Citizens are expected to be transparent, yet the systems making them as such, as well as their beneficiaries, are rarely rendered fully visible. The short-circuiting of Aadhaar—through breaches exposing its technical vulnerabilities and pushback from legal and civil-society actors—shines a particularly critical light on this nationalised architecture. This power imbalance, combined with the aforementioned disparities of Aadhaar experienced in everyday life illustrates that it, as a socio-technical assemblage, maps onto the state's existing "geographies of belonging and exclusion" that "privilege particular subjects' positioning while simultaneously rendering other bodies vulnerable" (Moore et al. 2003, 14). This observation is an important reminder that contemporary articulations of structural power cannot be separated from their socio-technical conditions and interlocking systems of marginalisation.

4 Conclusion

So, what does an analysis of Aadhaar tell us about the relationships between knowledge, governance, and state power? On the one hand, it showcases how the pursuit of knowledge about subjects is central to exercising structural power. On the other, it enables scrutiny of how these practices are part of state maintenance. More importantly, though, it demonstrates how the two concerns are inextricably linked, with surveillance working in the service of both. Strange's theorising helps us to see that knowledge is foundational, but it does not provide the appropriate lens for tracing the relationships that shape the terrains of governance in which Aadhaar is enrolled and deployed. In contrast, poststructural insights, which Strange expressed scepticism about, aid in correcting how to focus on structural power; they have long been attuned to how biogovernance, inequality, and state authority coalesce in ways that are not limited to political economy's traditional areas of emphasis. As Paul Langley (2009, 128) acknowledges, Strange may have disrupted "previously settled conceptions of power[,] … raising questions about the significance of knowledge in the materialization of the global political economy," but she also "contributed to the insulation or estrangement of the field from debates about power taking place across the social sciences, debates in which poststructuralism and Michel Foucault's (1980) work on 'power-knowledge' loomed large." Poststructural insights have since brought attention to how nation-state biopolitics bring about diverse material effects, including human experience, into stark relief, to which Strange does not attend.

A remaining challenge is how to account for the shifting techniques of biogovernance that Aadhaar reveals, especially as an assemblage of state, non-state, and hybrid entities operate—and will continue to operate—in ways that extract and utilise data on Indian subjects. While recent Indian Supreme Court rulings may weigh in on the appropriate use of UIDs, they may have little bearing in terms of influencing the nature of the architecture already in place. In fact, they explicitly stop short of doing so, drawing boundaries around the existence of privacy rights and whether companies can compel citizens to disclose their UIDs in the future. Thus, rather than reflect on what government actors have or have not done to check the exercise of structural power in this context, this chapter concludes with a reflection on how the fashioning of Aadhaar reflects a shift in how regulatory webs are woven.

As Eubanks (2018) writes in relation to the role that new technologies have played in welfare provision in the United States, the increased reliance on tools for monitoring compliance and for assessing and predicting risk has meant that already marginalised people are not only more likely to be surveilled more closely than other citizens, but they are also more prone to becoming ensnared by webs weaved by the socio-technical systems. That is, instead of technologies ensuring beneficiaries receive necessary provisions, they render already vulnerable subjects more susceptible to punitive measures. Although greater transparency before the state may promise better service delivery, it does not necessarily ensure it. It does, however, mean such subjects are exposed—and thereby become easier targets—for different facets of structural power. This observation is a reminder that state power is a violent force, even when it is not asserted through blunt measures. Be it within or beyond the borders of India, the United States, or elsewhere, the digital materiality of social assistance interventions, such as Aadhaar, means that knowledge about citizens passes through data-sharing webs that blur private and public domains. In doing so, it facilitates flows of structural power, which can concentrate around, target, and even fixate on subjects who are made more visible through these practices. Further, as the India case illustrates, its materiality facilitates the expansion of regulatory webs to encompass a wider range of residents—and rapidly so.

As argued here, Aadhaar as a fix for a leaking social assistance system has actually led to the institutionalisation of leakiness. Through the embrace of digital data for the purposes of regulation, leakiness is becoming a structural feature of governance. Although Strange passed away before the information society came fully into its own, her work nonetheless gives us a starting point for thinking through the foundational relationship between state power and knowledge, particularly in this current digital moment. In fact, further analysis in relation to other dimensions of Strange's framework could aid in eliciting how other structures come to bear on the case at hand. In order to make sense of how these entanglements operate, we cannot rely on Strange's ideas around structural power alone. We must look to scholarship that Strange herself did not appreciate, particularly as feminist and critical race scholarship has been central to illuminating how interlocking systems of oppression and social categories of difference work in tandem to make some subjects more vulnerable to the punitive aspects of state power than others. Moreover, by sharing Strange's commitment to granularity, we do not lose sight of the embodied aspects and effects of governance.

References

Ajana, Btihaj. 2010. Recombinant Identities: Biometrics and Narrative Bioethics. *Journal of Bioethical Inquiry* 7 (2): 237–258.

Bhatia, Rahul. 2018. How India's Welfare Revolution Is Starving Citizens. *The New Yorker*, May 16. https://www.newyorker.com/news/dispatch/how-indias-welfare-revolution-is-starving-citizens.

Bhattacharya, Ananya, and Nupur Anand. 2018. Aadhaar Is Voluntary—But Millions of Indians Are Already Trapped. *Quartz*, September 25. https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/.

Bill and Melinda Gates Foundation. 2017. *Financial Services for the Poor: India*. Accessed December 29, 2018. http://stash.globalgoals.org/goalkeepers/datareport/case-studies/financial-services-for-the-poor-india/.

Braithwaite, John. 2000. The New Regulatory State and the Transformation of Criminology. *British Journal of Criminology* 40 (2): 222–238.

Browne, Simone. 2010. Digital Epidermalization: Race, Identity, and Biometrics. *Critical Sociology* 36 (1): 131–150.

———. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham. NC: Duke University Press.

Dee, Mike. 2013. Welfare Surveillance, Income Management, and New Paternalism in Australia. *Surveillance & Society* 11 (3): 272–286.

Dixit, Pranav. 2017a. India's National ID Program May Be Turning the Country into a Surveillance State. *Buzzfeed News*, April 4. https://www.buzzfeed.com/pranavdixit/one-id-to-rule-them-all-controversy-plagues-indias-aadhaar.

———. 2017b. Airbnb, Uber, and Ola Are Considering Using India's Creepy National ID Database. *Buzzfeed News*, July 19. https://www.buzzfeed.com/pranavdixit/airbnb-uber-and-ola-may-start-using-aadhaar-indias?utm_term=.sxVVwn0xMV#.bhGZwNmx0Z.

———. 2018. India's National ID Database with Private Information of Nearly 1.2 Billion People Was Reportedly Breached. *Buzzfeed News*, January 4. https://www.buzzfeed.com/amphtml/pranavdixit/indias-national-id-database-with-private-information-of.

Doshi, Vidhi. 2018. India's Biometric ID Program Was Supposed to End Welfare Corruption. But the Neediest May Be Hit Hardest. *Washington Post*, March 25. https://www.washingtonpost.com/world/asia_pacific/indias-vast-biometric-program-was-supposed-to-end-corruption-but-the-neediest-may-be-hit-hardest/2018/03/24/bb212a86-289c-11e8-a227-fd2b009466bc_story.html?utm_term=.79f45c7dc264.

Drèze, Jean. 2014. On the Mythology of Social Policy. *The Hindu*, July 8. http://www.thehindu.com/opinion/lead/on-the-mythology-of-social-policy/article6186895.ece.

Dubrofsky, Rachel E., and Shoshana Amielle Magnet. 2015. Feminist Surveillance Studies: Critical Interventions. In *Feminist Surveillance Studies*, ed. Rachel E. Dubrofsky and Shoshana Amielle Magnet, 1–17. Durham, NC: Duke University Press.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Feldman, Allen. 1991. *Formations of Violence: The Narrative of the Body and Political Terror in Northern Ireland*. Chicago: University of Chicago Press.

Foucault, Michel. 1980. *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*. New York: Pantheon Books.

Ganesh, Maya Indira. 2018. Data and Discrimination: Fintech, Biometrics, and Identity in India. *Cyborgology*, January 25. https://thesocietypages.org/cyborgology/2018/01/25/fintech-aadhaar-and-identity-in-india/.

Gates, Kelly A. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: NYU Press.

Ghoshal, Devjyost. 2017. The World's Largest Biometric ID Programme Is a Privacy Nightmare Waiting to Happen. *Quartz India*, March 28. https://qz.com/943102/aadhaar-for-dummies-why-right-thinking-indians-should-be-worried-over-the-slow-death-of-privacy/.

Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.

Goel, Vindu. 2018. 'Big Brother' in India Requires Fingerprint Scans for Food, Phones, and Finances. *New York Times*, April 7. https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html.

Goldberg, David Theo. 1997. *Racial Subjects: Writing on Race in America*. New York: Routledge.

Government of India. 2016. Your Aadhaar. *Unique Identification Authority of India*, 2016. Accessed December 29, 2018. https://uidai.gov.in/your-aadhaar/about-aadhaar.html.

Guruswamy, Menaka. 2017. India's Supreme Court Expands Freedom. *New York Times*, September 10. https://www.nytimes.com/2017/09/10/opinion/indias-supreme-court-expands-freedom.html.

Guzik, Keith. 2017. *Making Things Stick: Surveillance Technologies and Mexico's War on Crime*. Berkeley: University of California Press.

Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622.

India Stack. 2018. *What Is India Stack?* Accessed December 29, 2018. http://indiastack.org/about/.

Khaira, Rachna. 2018. Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details. *The Tribune*, January 3. http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

Khera, Rachna. 2018. Why India's Big Fix Is a Big Flub. *New York Times*, January 21. https://www.nytimes.com/2018/01/21/opinion/india-aadhaar-biometric-id.html.

Kumar, Hari. 2013. Unique ID Program Introduces Instant Verification Services. *The New York Times*, May 24. https://india.blogs.nytimes.com/2013/05/24/aadhar-program-introduces-instant-verification-services/.

Langley, Paul. 2009. Power-Knowledge Estranged: From Susan Strange to Poststructuralism in British IPE. In *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*, ed. Mark Blyth, 126–139. New York: Routledge.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.

———. 2013. *Identifying Citizens: ID Cards as Surveillance*. Cambridge: Polity Press.

Magnet, Shoshana A. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham: Duke University Press.

Monahan, Torin. 2017. Regulating Belonging: Surveillance, Inequality, and the Cultural Production of Abjection. *Journal of Cultural Economy* 10 (2): 191–205.

Moore, Donald S., Anand Pandian, and Jake Kosak. 2003. The Cultural Politics of Race and Nature: Terrains of Power and Practice. In *Race, Nature, and the Politics of Difference*, ed. Donald S. Moore, Jake Kosak, and Anand Pandian, 1–70. Durham, NC: Duke University Press.

Narendramodi. 2014. On Aadhaar, Neither the Team That I Met Nor PM Could Answer My Qs on Security Threat It Can Pose. There Is No Vision, Only Political Gimmick. *Twitter Post*, April 8. Accessed December 29, 2018. https://twitter.com/narendramodi/status/453543852175925248.

Nilekani, Nandan. 2009. *Imagining India: The Idea of a Renewed Nation*. New York: Penguin.

Parker, Ian. 2011. The I.D. Man. *The New Yorker*, October 3. https://www.newyorker.com/magazine/2011/10/03/the-i-d-man.

Patton, Paul. 1994. Metamorpho-Logic: Bodies and Powers in *A Thousand Plateaus*. *Journal of the British Society of Phenomenology* 25 (2): 157–169.

Pink, Sarah, Shanti Sumartojo, Deborah Lupton, and Christine Heyes La Bond. 2017. Mundane Data: The Routines, Contingencies, and Accomplishments of Digital Living. *Big Data & Society*, Online First. https://doi.org/10.1177/2053951717700924.

Safi, Michael. 2018. Reporter Who Exposed India Data Breach Named in Criminal Complaint. *The Guardian*, January 8. https://amp.theguardian.com/world/2018/jan/08/reporter-who-exposed-huge-indian-data-breach-rachna-khaira-named-in-government-criminal-complaint.

Sathe, Vijay. 2014. Managing Massive Change: India's Aadhaar, the World's Most Ambitious ID Project. *Innovations* 9 (1/2): 85–111.

Sharma, Pankul. 2018. Only Male or Female Can Get PAN Card, Transgender Told. *Times of India*, March 15. https://timesofindia.indiatimes.com/india/only-male-or-female-can-get-pan-card-transgender-told/articleshow/63321785.cms.

Singh, Manish. 2017. Is India's Central Database with Biometric Details of Its Billion Citizens a Privacy Nightmare? *Mashable*, February 14. https://mashable.com/2017/02/14/india-aadhaar-uidai-privacy-security-debate/#ZgQ0T5iIwOqc.

Staples, William G. 2014. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. 2nd ed. Lanham, MD: Rowman & Littlefield.

Strange, Susan. 1998. *States and Markets*. London: Pinter.

Targeted Delivery of Financial and Other Subsidies, Benefits and Services (Aadhaar) Act, 2016. https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.

The Economist. 2017. Digital Dawn. *The Economist*, April 15, 32–33.

Torpey, John. 2009. *The Invention of the Passport: Surveillance, Citizenship, and the State*. Cambridge: Cambridge University Press.

Trubek, David M., and Louise G. Trubek. 2005. Hard and Soft Law in the Construction of Social Europe: The Roles of the Open Method of Co-ordination. *European Law Journal* 11 (3): 343–364.

Tufekci, Zeynep. 2014. Engineering the Public: Big Data, Surveillance, and Computational Politics. *First Monday* 19 (7). https://doi.org/10.5210/fm.v19i7.4901.

Walby, Sylvia. 1999. The New Regulatory State: The Social Powers of the European Union. *British Journal of Sociology* 50 (1): 118–138.

World Bank. 2016. Enabling Digital Development: Digital Identity. *World Development Report 2016*. http://pubdocs.worldbank.org/en/822821519686607466/9781464806711-WDR2016-Spot4-Rev-Oct2017.pdf.

A Border Seeping in All Directions: Technologies of Separation Along the U.S.-Mexico Border in Ambos Nogales

Allison Fish

Today, more than 90 per cent of all goods consumed in North America are involved, in one way or another, in international trade. In other words, the vast majority of commodities that we consume are produced, at least in part, in another country and must travel across national borders in order to reach their final point of sale.[1] This simple fact embodies the key reality that almost every object consumed in modern daily life, from the ubiquitous computing technologies we use to organise our work and social lives to the clothing that we wear, to many of the things we eat have been produced, at least in part, in another country. Moreover, this figure is constantly increasing, with the volume of international commerce swelling more than fourfold between 1970 and 2005 (George 2013). While many factors have contributed to this growth, a key and often overlooked one

[1] This is true for most countries, as there are few locations that remain outside of the global economy. Additionally, in some countries, such as Australia, the percentage of internationally traded commodities is higher than 90 per cent.

A. Fish (✉)
University of Queensland, Brisbane, QLD, Australia
e-mail: a.fish@law.uq.edu.au

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_12

has been the standardisation of a range of technologies[2] used in international transport, from metal containers that can be seamlessly transitioned from truck to rail to boat to the software capable of coordinating complex commodity chains (George 2013; Levinson 2016; Martin 2016).

In order for internationally traded goods to find their way from point of production through to point of consumption, they must be physically moved along routes that pass through national borders. Legitimate physical passageways of cargo from one nation-state to another are generally restricted to a limited set of narrow geographic spaces—border ports-of-entry—that tend to function as checkpoints and chokepoints for international commercial flows. It is in and around these narrow spaces that commodities, as well as the people involved in their transportation, are judged as *trustworthy* or *untrustworthy*. Those shipments and people meriting trust are then eligible for legal passage and have the opportunity to participate in the global economy. In contrast, those that cannot demonstrate they are worthy of trust are restricted from entry, an outcome that can have knock-on effects up and down that particular commodity chain.

While most international commodities complete the bulk of their journey via ocean freight, a substantial portion moves by land via rail and/or road (Donovan and Bonney 2006; Levinson 2016). This chapter focuses on commercial movements that cross land border ports-of-entry as goods move northwards from Mexico into the United States. As points of passage between neighbouring nation-states, land-border ports-of-entry represent a key site for the on-the-ground interpretation of laws that are intended to reconcile and balance numerous social, political, and economic interests. In the case of the U.S.-Mexico border these interests include: national security, road safety concerns, trade protection, customs and tariffs, anti-counterfeiting measures, quarantine, migration, and environmental protection measures. The argument of this chapter is that the determination of a commercial shipment's trustworthiness and eligibility for cross-border passage requires the reconciliation and balancing of these numerous legal concerns. Further, determining such trustworthiness is a process that is increasingly monitored, enacted, and enforced via a complex system of technologies deployed at and around border ports-of-entry.

In many ways the passage of commercial goods across international borders and through ports-of-entry is a material place where law and

[2] This chapter defines "technology" broadly to refer to any systematised processes, machinery, or devices, as well as computational technologies.

technology increasingly intersect and become entangled. These technologies, then, can be thought of as promoting certain ways of "knowing" the border and are significant points where law is enacted and interpreted. As such, these technologies are important regulatory instances of the knowledge structure (see Strange 1994; Haggart this volume) and those who control their configuration and implementation are vested with the authority to determine what constitutes trustworthiness and, by implication, lawful and legitimate cross-border traffic. In the case of land ports-of-entry along the U.S.-Mexico border, such authority rests upon a unique surveillance assemblage with its own peculiar configuration and processes.

Organising this movement, navigating these narrow chokepoints, and responding to legal requirements in a manner that addresses the specific technological infrastructures at border ports is the role of the international shipping and transport logistics industry, an industry that is either mostly invisible or, quite literally, off limits to the general public. The average person doesn't think about the practicalities of logistics nor do they see logistical processes and actors in motion. In essence, logistics is a service industry with an almost imperceptible profile, despite being the major backbone supporting the global market's interdependence and interconnectivity.[3] The fact that the regulation of such a core aspect of the global economy operates almost entirely out of the public view functions to veil and naturalise the power dynamics at play in this space. This chapter investigates the historical emergence of the unique matrix of law and technology at a specific land border port-of-entry between the United States and Mexico—the Mariposa Port of Entry located at Ambos Nogales. Specifically, attention is paid to how laws and technologies are brought to bear in determining the trustworthiness of Mexican-origin shipments and peoples, a powerful decision that determines who can participate in the global economy and the conditions governing such participation.

Ambos Nogales, a small town straddling the border with one side in the U.S. state of Arizona and another in the Mexican state of Sonora, has been the primary "hub" for northbound winter produce for more than a century. During this time frame, the volume and value of trade moving through Ambos Nogales has increased substantially. In sync with this

[3] There is an emerging but limited body of scholarship that tends to focus primarily on freight moving through seaports, which represents the vast bulk of international commercial freight. In contrast, there is a relatively limited understanding of freight crossing over land border ports-of-entry, moving either by rail or truck.

increase, the complexity of the legal and technological matrix regulating movement along the border has also grown.[4] For example, technologies of separation (from open spaces to guardhouses to fences and walls) and technologies of monitoring (from border agents to X-rays to electronic logging and sensor technologies) have gradually accumulated at the border. At times this accumulation of technologies appears to proceed in a coordinated effort to ensure immigration, food safety, national security, road safety, and environmental standards are met. However, at other times, the accumulation of technologies appears discordant and unrelated.

Each variation of this growing intersection between law and technology, which taken together I refer to as a *techno-legal system*, potentially impacts the social, economic, and political configuration of the local logistics industry in Ambos Nogales. In exploring these inter-related impacts, the chapter traces how:

- the development of contemporary techno-legal systems at border ports-of-entry should be examined holistically and placed in their socio-historical context;
- varied technologies, both old and new, are brought together at specific sites in a manner that increasingly aims to make visible, spatially constrict, and digitally monitor the *trustworthy* movements of goods and people; and
- in contrast, all other movements that take place across national borders are increasingly implicated as *untrustworthy*, illicit, or illegal and become policed as such.

The techno-legal systems used to regulate cross-border movements in Ambos Nogales have gone through roughly three temporal stages in logic since the late 1800s. The three stages, described in detail below, are *visualisation of movement* (1880s to 1910s), *spatialisation* or *spatial constriction of entry* (1910s to 1990s), and finally *digital monitoring* (2000s to present). It is important to note that techno-legal systems, as well as the underlying logics that animate them, tend to be additive. As a result, these

[4] Heritage laws and technologies have tended to accrete and layer over time, rather than replace one another as new requirements are added. This is in keeping with the idea that elements of infrastructural systems, once stabilised, are difficult to dislodge (Bowker and Star 1999).

systems tend to become increasingly complex over time as they accrue multiple, and often conflicting, technologies and regulatory objectives. Thus, when taken together, an analysis of the techno-legal system regulating movement through the Mariposa Port of Entry has the capacity to not only illuminate how trust, authority, and control are unequally distributed within the contemporary knowledge infrastructure, but is also able to tell a story of the way these relationships came to be.

1 Logistics as an Integral Aspect of Commodity Chain Analysis

The following account draws on historical and ethnographic materials to discern the way in which surveillance technologies and law create a certain way of knowing and controlling the commercial activity that moves through the U.S.-Mexico border in Ambos Nogales.[5] In doing so, the following account extends critical commentary that holistically examines the relationship between technology, law, and society. Significantly, in doing so, the analysis adds to the field of technology studies by turning away from the question of how contemporary information technologies shape access to intangible resources and affect participation in the knowledge economy. Instead, I would like to focus on how technological systems factor into and shape access to tangible resources for different actors across the commodity chain. This move is predicated, in part, on my belief that, despite entering the Information Age, *materiality* and *material conditions* continue to matter and are integral aspects of an individual's ability to lead a secure life.

In doing so, the chapter draws from critical social science and humanistic literature on the trans-border movements of people and goods, especially those implicated in global commodity chains (Appadurai 1986; Beckert 2014; Coutin 2000; Holmes 2013; Mezzadra and Neilson 2013; Mintz 1986). Work in this area tends to highlight the otherwise opaque and seemingly indirect relationships between *consumers*, often located at the centre, and *producers*, often located at the periphery. By making these relationships explicit, scholarship in this domain focuses on the unequal distributions of wealth and political power that have characterised such international flows since the colonial period through to the present.

[5] Since the 1980s, Marxist scholars have analysed commodity chains as important social sites reflecting and reinforcing socio-economic and political structural inequalities.

Including logistics in this analysis will add the integral, but often overlooked, component of how producers connect to consumers and who is involved in forging this connection.

While logistics has not been a traditional focus of commodity chain analysis, in recent years there has been an increasing interest in the cargo container. This research focuses on the role that such a seemingly simple innovation—the standardisation of how commodities materially move—has shaped not only the logistics industry, but also the functioning of the global economy (Bonacich and Wilson 2008; Cudahy 2006; Easterling 2014; Klose 2015; Levinson 2016). However, this research has focused on ocean-going freight and tended to overlook that which travels by road. As such, these studies tend to either be quantitative in nature and/or global in scope. By focusing on Ambos Nogales, a small road port that plays a significant role in connecting regional North American produce markets, this study extends the type of granular analysis advocated by Susan Strange.

The following discussion is additionally interested in exploring the relationship between law, policy, and surveillance technologies (Chan 2013; Coleman 2013; Henne 2015; Jasanoff 2011; Kelty 2008; Medina 2011; Rankin 2016). To do this I examine how varied technologies are being used to identify *trusted* logistics providers and "control" the physical flow of goods involved in legitimate commercial trade. In this sense, the design and deployment of socio-technical assemblages can be understood as a site in which law is interpreted, enacted, or performed on a daily basis in a manner that reaches into the lives of everyday citizens in both the United States and Mexico.

2 Ambos Nogales: A Key Hub for Northbound Mexican Produce

At first glance, Nogales appears to be a sleepy and isolated town spanning both sides of the border. With a population of 240,000 people (21,000 in Arizona and 220,000 in Sonora) the impression of rural idyllic is reinforced by the physical geography, which tucks the sparse population into the crevices of rolling hills at an elevation of 4,000 feet—keeping the town several degrees cooler than the surrounding Sonoran Desert. To the north, the major road linking Nogales, Arizona, to the rest of the United States is Interstate 19, a narrow and winding corridor that stretches for 65 miles

(105 kilometres) before ending in Tucson, Arizona. Here I-19 empties into Interstate 10, the major east-west highway connecting the southernmost portion of the United States. The isolated and disconnected atmosphere of Nogales, Arizona, belies the enormous role that this town plays as the northbound hub for the Mexican fresh produce bound for various U.S. and Canadian markets, as well as the town's role as an experimental high-tech port-of-entry into the United States.

The significance of the Mariposa Port of Entry lies just across the international border as the gateway to (and from) Nogales, Sonora, the northernmost terminus of *Carretera Federal* 15, MX 15.[6] MX 15 is one of the largest and best maintained roadways connecting the western half of the country from Mexico City in the south through Guadalajara, Hermosillo, and, finally, Nogales. It is along this corridor, from Mexico's MX-15 to United States' I-19 and on to I-10, that the majority of Mexican produce consumed by Canadians and Americans passes each year.

Passage across the U.S.-Mexico border in Ambos Nogales takes place at two major ports-of-entry; the Dennis Deconcini Port of Entry located in the downtown area, and the Mariposa Port of Entry located in an industrial district two miles to the west.[7] While both service pedestrian and vehicular traffic, only the Mariposa Port deals with truck-related commercial freight. As the fourth-largest port-of-entry along the United States-Mexico border, in 2017 the Mariposa Port was the gateway for more than 330,000 northbound trucks[8] carrying more than US$15 billion worth of trade per year.[9] The vast majority of commercial trade moving through the Mariposa Port, both in terms of value and volume, is northbound—

[6] The Mexican Federal Highway 15 (*Carretera Federal 15*) connects most large cities in the western half of the country. In 1991, MX 15 was incorporated into the CANAMEX corridor, a series of pre-existing set of interconnected motorways connecting Mexico, the United States and Canada. In 1995 improvements along the CANAMEX corridor became an important element of the North American Free Trade Agreement allowing the improved flow of commercial traffic between the three countries.

[7] There is a third port-of-entry, the Morley Gate. However, this pedestrian gate is located next to the Deconcini port and for the purposes of this chapter these two ports are treated as one.

[8] Figures from the U.S. Bureau of Transportation Statistics webpage "Border Crossing/Entry Data" (https://www.bts.gov/content/border-crossingentry-data) accessed on April 3, 2018. Data on southbound trucks unavailable.

[9] Figures from U.S. Trade Numbers webpage for "Nogales, Border Crossing, Arizona," https://www.ustradenumbers.com/port/nogales-border-crossing-ariz/, accessed November 16, 2018. The report by Landes (2016) indicates a higher figure, but is non-specific as to actual value.

originating in western Mexico and travelling to consumers in the United States or Canada (Pavlakovich-Kochi and Thompson 2013).[10]

Of the 330,000 northbound trucks annually passing through the Mariposa Port, approximately 40 per cent, or 140,000, carry perishables, primarily vegetables, but also other agricultural products such as fruits and grains. The total value of the perishable agricultural commodities passing through the Mariposa Port is estimated to be approximately US$2.85 billion per year (a little less than 20 per cent of the total value of northbound commodities). The northbound produce accounts for one-quarter to one-third of the total Mexican produce sold to United States and Canadian markets (Hufbauer and Jung 2017; Pavlakovich-Kochi and Thompson 2013). Furthermore, the business of importing produce from Mexico into the United States via Ambos Nogales is rapidly expanding with customs-recorded value growing by more than 150 per cent between 1996 and 2011. During this 15-year period the value of produce moving through the Mariposa Port soared from US$1 billion in 1996 to US$2.54 billion in 2011 (Pavlakovich-Kochi and Thompson 2013).

Movements across the border tend to be seasonal, with the height of activity occurring in the winter months when Mexican agriculture remains productive, while the majority of Canadian and U.S. fields are not due to inclement weather. In this busy season, which begins in October, continues through May and is most intense from January to March, up to 80 per cent of all north-bound Mexican agricultural produce moves through the Mariposa Port on more than 4,000 trucks a day (Landes 2016). In the summer months, however, this figure drops precipitously leading to high seasonal unemployment on both sides of the border (Landes 2016). Another factor putting pressure on the local logistics industry is that the Mariposa Port is increasingly facing competition from McAllen, Texas, as a destination hub for the movement of northbound Mexican produce. This increase is the result of various factors including improved road and port infrastructures on both sides of the border near McAllen, as well as an increased demand in Canadian and U.S. markets for high-value fruits and specialty vegetables that grow primarily in eastern or southern Mexico,

[10] Most northbound goods originating in Central and South America are transported to the United States.by ocean-going freight and enter the country at the Long Beach, Los Angeles, or Miami seaports. Most western Mexican commodities bound for consumers outside of North America move by other means.

such as avocadoes and bitter melon.[11] These two pressures, when coupled with the renegotiation of the North American Free Trade Agreement and introduction of the United States-Mexico-Canada Agreement,[12] have led to numerous concerns for Nogales' economic and social stability in the future (FPAA 2018).

Concerns over regional welfare are directly linked to the stability of the local logistics industry in Ambos Nogales, which includes far more than simply northbound trucks filled with pallets of fruits and vegetables. The industry also connects a wide cast of characters including customs inspectors and border officials, wholesalers, warehouses, and cold storage operators, as well as freight forwarding personnel and customs brokerage firms—all of which must be located close to the border to ensure the fast and efficient processing of the northbound perishable commodities. This commercial complex, along with all the associated business of fuel providers and federal agencies on the border, generated about US$437 million in 2013 for Santa Cruz County (the county in which Nogales, Arizona, is located)—or 22 per cent of all jobs, 25 per cent of total wages, and one-third of total direct and indirect revenue for the county. In short, logistics is big business in Nogales and quite literally the economic life-blood of this community.

The complex economic network underlying the local logistics industry did not spring up overnight, nor are local providers merely disconnected representatives employed and relocated to this border-town by multinational firms. Instead, the Nogales logistics industry has developed over more than a century and, until recently, has been dominated by social networks with close ties on both sides of the border. However, over the years, as border technologies of separation and tracking have changed, the strength of these social connections to economic livelihood has also fluctuated.

[11] Examples include the increasing demand for avocados, papayas, and mangos throughout North America, as well as the increasing demand by U.S. and Canadian immigrant communities for specialty items that fit home-country menus such as bitter melon or kombucha squash.

[12] The United States announced a new trade agreement with Mexico that would replace NAFTA in August 2018 and then extended this to Canada in October 2018. As of May 2019, ratification and implementation of the USMCA is still pending.

3 Early Technologies Separating Borders and Shaping Trade: Spaces, Fences, and Walls

Nogales has been an important border crossing not only for produce, but also for other types of social, economic, and political exchange between the United States and Mexico for over 150 years. Established initially via a land grant by the Mexican government in 1841, Nogales was transferred to the United States via the Gadsden Purchase in 1853 and an international trading post was established on the northern side of the border in 1880. At around this time, the two towns of Nogales, Sonora, and Nogales, Arizona, were formally separated by international agreement by a space of 60 feet on both sides of the border (Fig. 1). Physical checkpoints manned by state officials charged with monitoring international movements were built on both sides of the border around the turn of the century (see Fig. 2). Beginning in 1915, however, both the United States and Mexican governments built and removed temporary fences of hay or

Fig. 1 Open border between Nogales, Sonora, (*left*) and Nogales, Arizona, (*right*) circa 1898–99. At this time the countries were separated by 120 feet of space that was monitored by permanent checkpoints. Photo by WI Neumann. Available at the U.S. National Archives and Records Administration

Fig. 2 Photo from the 1920s showing national guardhouse structures, built in the late 1800s, and the earliest permanent border fence, built around 1918. Photo by unknown author. Available at the University of Arizona Library's Special Collections

wire for various reasons (see Fig. 3).[13] In fact, the earliest fence along the U.S.-Mexico border appeared in Nogales in 1915 at the behest of the Mexican governor at the time, Jose M. Matoreyna. However, it wasn't until 1918, after nearly a decade of tensions resulting in the Battle of Ambos Nogales (between Mexican and U.S. military and civilian militia forces) that the first permanent fence separating the two towns was constructed (see Fig. 2) (Knight 1986). Significantly, this two-mile-long, six-foot-tall barbed wire fence in Nogales was the first permanent structure separating the United States and Mexico erected anywhere along border (Knight 1986; Parra 2010).

For nearly a century the international border at Ambos Nogales has had a permanent structure of some kind that has taken on an increasingly solid form over time. Initially this permanent separation was produced via a

[13] For Mexico, one primary concern was Mexican revolutionaries crossing the border into the United States to evade detection and capture by the Mexican government. The U.S. government, in contrast, was concerned that these same revolutionaries would steal or rustle livestock. One example of such a revolutionary in the Nogales area is Francisco "Pancho" Villa, who escaped into Arizona multiple times in 1912.

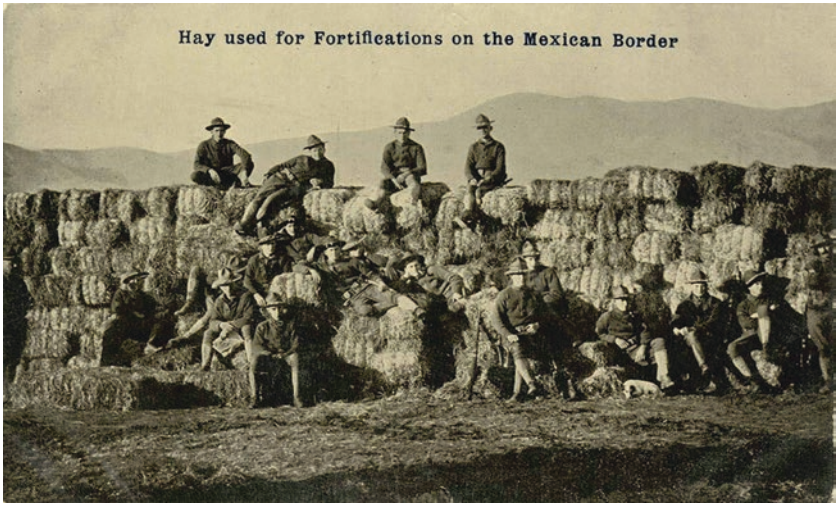

Fig. 3 Photo from the 1910s showing an early temporary border fence made out of hay near Douglas, Arizona. Photo by unknown author. Available at the University of Arizona Library's Special Collections

wire fence with concrete posts. This was later converted to a chain-link fence that spanned the length of the city. In 1994, however, the fence became a wall that stretched much further. In that year, Operations Gatekeeper, Safeguard, and Hold-the-Line, all measures instituted by the U.S. federal government aimed at deterring illegal immigration, mandated the construction of a solid wall built from steel sheeting and barbed wire across California, Arizona, and Texas. In Arizona, which was covered by Operation Safeguard, this wall was in addition to and ran side-by-side with the existing chain link fence.[14] The result was a 14-foot-high structure that ran for 62 miles and cost US$374 million (see Fig. 4). In the years immediately following Operation Gatekeeper other technologies and processes were funded by the U.S. federal government and placed along the wall in an effort to buttress the objective of preventing illegal movement—forcing transnational circulation through specific ports-of-entry. These efforts included doubling the number of armed border patrol guards, as well as

[14] Operation Gatekeeper was implemented in the San Diego area at about the same time and also included the building of a permanent wall between the two countries.

Fig. 4 Contemporary border wall at Ambos Nogales. Photo by the author

the use of infrared night-scope vision devices, low-light cameras, ground sensors, all-terrain vehicles, and floodlights along the wall (Nevins 2002).

As the Ambos Nogales community grew throughout the 1900s, the two countries experimented with various technologies in an attempt to satisfy an ever-changing set of social, political, and legal objectives that manifested at the border. The first set of technologies, from 1880 to 1900, appear to have focused almost solely on enabling the *visualisation* of the border in order that movements, commercial and otherwise, could be seen and tracked. In these earliest years, visibility appears to have been purely a matter of the general public's unencumbered view of the 120 feet of open space surrounding the border. Sometime during the 1890s it appears that effective visualisation required both the sight of border guards able to monitor the legitimate movement of goods, as well as checkpoints where these officials were located. In this sense, effective visualisation required monitoring by state agents, extensions of the government, who also required housing at particular locations.

By the 1910s, however, visualisation alone was deemed to be insufficient to police the national border—ushering in a second era where technologies were oriented towards the *spatial constriction* of movement. This transition appears to have been motivated by both economic and political concerns relating to the unpredictable movements of livestock, on the one hand, and Mexican guerrilla revolutionaries, on the other. During this period, technologies such as fences and walls of various durability and size were constructed to ensure that movements took place through official checkpoints that quickly transitioned to become border ports-of-entry and customs houses. In the following decades, these technologies were further enhanced by the addition of various devices designed to illuminate the unsanctioned and illegal crossings of people and objects at other points (e.g., lights, night-vision goggles).

4 The Physical and Virtual Expansion of Border Technologies

During the last century technologies of border visualisation and spatialisation were designed around the presumption that legitimate movements could and should be funnelled through official geographically constrained checkpoints, the border port-of-entry. Furthermore, if movements were routed through these ports, then a fairly stable suite of technologies (e.g., X-rays, K-9 units, random changing of border guards, and hand-held mirrors) were sufficient for policing illegal movements that passed through them. Other legitimate movements, both commercial and private, in contrast, could be managed via face-to-face interactions and tracked through paper-based mediums. Over time, however, these presumptions proved to be simplistic and by the 1990s the international border began to seep in multiple directions around Ambos Nogales, moving

- from east to west as the fences themselves have spread beyond individual towns and cities and across the southern U.S. border through Operations Gatekeeper, Safeguard, and Hold-the-Line;
- upwards and downwards as surveillance teams employed robots, ground-sensing radar, drones, and satellite technologies to monitor aerial and subterranean movements (Sorrensen 2014); and

Fig. 5 Approaching the Amado, Arizona, border checkpoint. Photos by the author

- from north to south as domestic U.S. and Mexican inspection checkpoints were established miles from the actual border line in both the United States (Amado, Arizona) and Mexico (Querobabi, Sonora) (Fig. 5).

This seepage was enabled primarily through the introduction of sophisticated computational technologies that aimed not only to visualise and spatially constrict border movements, but also *digitally monitor* these movements via *networked sensors* that allowed for the communication of information over long distances.

In the late 1990s, the U.S. federal agencies tasked with monitoring international commercial logistics began to incorporate many of the same computational and networked technologies used to monitor illegitimate movements. As a result, the local logistics industry in Ambos Nogales also began to adopt numerous new technologies in order to communicate and comply with U.S. federal agency directives. In this sense, these new networked technologies quickly became sites through which important legal requirements pertaining to road safety, anti-counterfeiting measures, customs and tariffs, and immigration were monitored and enforced. As these technologies accumulated, they began to transform the local logistics industry by allowing the online processing of customs duties, the monitoring of individual vehicles via automated driver and maintenance

logs, and the electronic sealing of containers. The physical inspection and surveillance of commercial traffic at the Mariposa border port-of-entry, however, continued to retain more simplistic heritage technologies, such as concrete barriers, X-rays, K-9 units, and hand-held mirrors for the purposes of visualising and spatial constricting northbound movements. In short, though the logics of managing the physical space of the border changed minimally over this 80-year period, the logistics industry was beginning to communicate in new ways through online exchanges on office desktops, mobile telephones, and electronic logs—activities that take place, primarily, at a substantial distance from the border.[15]

In the early 2000s, this change further accelerated with the introduction and increased affordability of mobile information and communication technologies, such as sensors. During this period of time, the Mariposa Port entered a third phase, in which digital monitoring has become a key aspect of the regulation of commercial border movements. While the early generations of these new technologies and their embedded legal processes were first conceptualised in the mid-2000s, they were not integrated into the local logistics industry until recently. This integration, though currently only partial, has been accomplished in step with the redesign of the Mariposa Port, a process that took place between 2010 and 2015. The end result is that the Mariposa Port has become a techno-legal space that incorporates a multi-layered logic of visualisation, spatial constriction, and digital monitoring that seeps in many directions.

5 The Mariposa Port of Entry as High-Tech Passageway: 1973 to Present[16]

Since the early twentieth century the volume of northbound international trade through Ambos Nogales has increased exponentially and, by the late 1960s, had become difficult for existing facilities to accommodate. In

[15] Within just a few years, local logistics providers moved from being a completely paper-based industry to one where significant office work took place online. For example, in 2001 Nogales brokerage firms still employed "runners" at the Mariposa Port. Runners took customs paperwork from queuing drivers, delivered these and proof of payment to officials at the border, then "ran back" approvals before drivers before were able to cross into Arizona (personal communication). By 2004 this job had been phased out as these communications and payments are now all handled online.

[16] The bulk of information for this section comes from personal communications with members of the Nogales logistics industry, as well as newsletters and policy briefs issued by local public and non-governmental organisations.

order to accommodate the increased demand for international commodities, as well as the increased capacity of local infrastructure, the Mariposa Port of Entry opened in 1973. For the first 40 years of its existence, the Mariposa Port was an international gateway known for its narrow connecting roadways, poor infrastructure, and long wait times. Of the four lanes of traffic flowing northward through the port, only two were dedicated to commercial transport.

Originally designed to handle 750 trucks per day, by the late 1990s the Mariposa Port was overwhelmed, with 2,000 trucks queuing up for entry into the United States on some days. This resulted in lines of trucks that regularly spread for more than five miles south of the border, with an average wait time of six hours. Accidents, and in some cases public protests,[17] were capable of shutting down the port and, as a result, international commercial trade. During the busy winter season, border wait times increased resulting in high costs for numerous sectors of the logistics industry; carriers lost nearly a day moving cargo a short distance, drivers spent increasing amounts of money on petrol while idling, exhaust fumes from waiting trucks degraded local air quality, and shippers faced the potential financial disaster of an entire container of perishables spoiling (Landes 2016).[18]

Border wait times, when combined with U.S. regulations requiring drivers to rest every 11 hours, further shaped the tempo and structure of the local logistics industry as under these conditions it was economically unsound for long-haul trucks to cross the border in either direction. As a result, most goods actually crossed the border on drayage, or short-haul, trucks that would pick up a shipment at a warehouse in Nogales, Sonora, and transport the container the five to ten miles to a warehouse in Nogales, Arizona. This meant that many short-haul drivers were local Nogales residents who, despite working 16-hour days in some cases, might only take one container across the border per day. Drayage drivers were well known to one another, the customs and border agents, as well as the warehouse

[17] In 2001, Mexican truckers, protesting unequal implementation of provisions in the North American Free Trade Agreement, managed to shut down the Mariposa Port for several days using a comparatively small number of vehicles to block the road. Mexican trucking licenses, by and large, effectively are still not treated by U.S. authorities as being sufficient for driving on U.S. roadways (Kitroeff 2018).

[18] Each type of perishable commodity is stored at a particular temperature to prevent spoilage (e.g., bananas are stored at 13 degrees Celsius). Climate-controlled containers often fail if a truck is stalled too long, leading to spoilage and a complete loss of cargo even during winter months.

operators on both sides of the border. Under these conditions, the local logistics industry maintained a fairly familiar tone that was connected via multi-generational family businesses.

By 2004 many of the private businesses in the local logistics industry had been forced to scale-up technologically. In large part this was due to requirements from the U.S. Customs and Border Protections that all paperwork and payments pertaining to cross-border shipments needed to be electronically filed. Given the insufficient infrastructure, over the next few years the Nogales Brokerage Association, along with organisations like the Fresh Produce Association of the Americas, lobbied for the expansion of the Mariposa Port as the first cyberport in the United States.[19] Eventually this redesign was funded by a grant from the *American Reinvestment and Recovery Act*.[20] The project was an ambitious plan that cost more than US$244 million and took almost five years, beginning in early 2010 and ending in late 2014. The expanded Mariposa Port was designed not only to expand the physical infrastructure for processing international movements, but also included the networked sensorisation and tracking capabilities that paved the way for digital monitoring.

Under the new infrastructure, as of 2018 the Mariposa Port boasts dedicated 8 lanes and 56 inspection booths for northbound commercial traffic that can handle 4,000 trucks per day. Wait times to cross the border plummeted and, according to a 2016 study, processing times for trucks averaged one hour, making the Mariposa port the fastest passage point for northbound traffic along the U.S.-Mexico border.[21] This result, when combined with recent decisions—first, the U.S. Department of Transportation's (a regulatory agency) acceptance of Mexican safety inspections and certifications as sufficient for the operation of Mexican trucks on U.S. roadways, and second, a recent 9th Circuit federal appellate court case summary

[19] It is the unique needs of transport relating to produce—the fact that these perishable commodities must move rapidly or will spoil, resulting in economic loss—that have made Nogales the focal point for trialling the Mariposa Port as the United States' first land-based cyberport. The cyberport is composed of two programmes; the Customs Trade Partnership Against Terrorism (C-TPAT) and the Free and Secure Trade clearance program (FAST).

[20] The ARRA was the Obama administration's stimulus package aimed at infrastructural investment and initiated in the wake of the 2008 Global Financial Crisis.

[21] It is important to note that the Mariposa port is still connected to poor infrastructure on both sides of the border, including narrow roads and off ramps from Mexico's I-15 and on ramps onto U.S.I-19. Even with the new port, traffic can back up for several miles and experience significant delays during the high season.

knocking back claims by the International Brotherhood of Teamsters that Mexican carriers enjoy unfair competitive advantages[22]—means that Mexican truckers are, for the first time, legally able to drive through to destinations north of the border.[23]

In order for Mexican drivers to work throughout the United States, Mexican shippers and others on the supply chain must qualify and adhere to the technological and legal standards of the FAST (Free and Secure Trade) programme. This programme allows registered cargo containers carrying approved Mexican commodities to travel through the border without stopping using a FAST lane at the Mariposa Port—potentially saving hours of waiting time. For cargo to qualify for the FAST lane, sensorised devices must be attached to containers to make them "intelligent." This ensures that U.S. Customs and Border Protection authorities will be able to recognise whether the container has remained sealed since it was originally loaded or whether it has been subject to tampering. This seal is checked three times during the cargo's passage over the border into the United States: at the Querobabi Inspection Station approximately 100 miles south of the U.S.-Mexico border by Mexican federal authorities; at the Mariposa Port of Entry; and finally about 30 miles north of the border on US I-19. At each stop, customs brokers assess the container's information and send this information ahead to requisite U.S. and Mexican agencies via internet platforms. Through these online registries, officials at border inspection points are able to see what the truck is carrying, verify who is driving the truck, approve it as legitimate international cargo, and assess any fees or duties. If there is any doubt, these officials retain a suite of non-invasive and invasive visualisation technologies (e.g., drive-through cargo container size X-rays) they can use to inspect trucks and containers.

To participate in this programme a driver must have a specialised FAST license, which requires both a background check and the registration of additional biometric features. Additionally, both the carrier and the importer must be registered with C-TPAT (Customs Trade Partnership against Terrorism). C-TPAT is a programme that brings together Customs

[22] *International Brotherhood of Teamsters v. U.S. Department of Transportation* (2017).

[23] This will present economic opportunities for Mexican carriers since they will now be able to move through to distribution hubs in the United States, such as Phoenix and Los Angeles. It will allow Mexican truckers pick up a haul so they will not have to return home empty, a situation called "deadheading."

and Border Protection and the private logistics industry to "safeguard the world's vibrant trade industry from terrorists, maintaining the economic health of the U.S. and its neighbours. The partnership develops and adopts measures that add security but do not have a chilling effect on trade, a difficult balancing act."[24]

In order to "add security, but not have a chilling effect on trade" every node along the logistics chain must successfully register for C-TPAT. In the case of perishable commodities passing through Nogales, this includes any third-party logistics provider, the customs brokers in Nogales, Arizona, and Nogales, Sonora, the trucking company, and, in cases where the producer loads and seals their own cargo container, the seller. Participation in this programme is a privilege and is predicated primarily upon being able to demonstrate "good character" via background investigations of the business in question, the owner, and the employees. Any red flags, including employing an ex-felon or a business's poor finances, may result in withdrawal of a C-TPAT license. The award of a C-TPAT license is completely discretionary and not subject to appeal by the applicant.

Most individuals involved in local Nogales logistics-related occupations speak about participation in the cyberport, and therefore successful application to the FAST and C-TPAT programs, as essential to the continuation of their livelihood. However, ensuring that everyone in a supply chain is able to obtain and maintain participation in both FAST and C-TPAT programmes is difficult and causes anxiety for many in the Nogales logistics industry. As the legislative liaison for the Fresh Produce Association of the Americas mentioned during an interview with the author, while the process can be seamless if implemented accurately, it is a challenge to obtain and maintain *trusted* partner status. Moreover, as supply chains grow, so too does the cast of characters requiring C-TPAT registration. In order to minimise the uncertainty of these extra links, many Mexican carriers are worried that shippers will increasingly contract with multinational corporations. Finally, in order to use the two dedicated FAST/C-TPAT lanes at the Mariposa Port, a driver must be able to accurately predict his arrival time. This is difficult because wait times at Mexican checkpoints, such as those in Querobabi, fluctuate greatly, as arrival estimates are highly unreliable.

[24] See https://web.archive.org/web/20160304194123/ http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism#. Accessed March 20, 2019. Concerns that Islamic terrorists might enter the southern land borders of the United States quickly gained speed in the post-9/11 era with regular unfounded reports of Muslim prayer rugs found in the desert amongst the detritus left behind by Latin American immigrants entering the country illegally (MacNamara 2004).

6 The Impacts of Techno-Regulation on the Nogales Logistics Industry and Community

When discussing the FAST and C-TPAT programmes with local logistics providers, different people voiced concerns about their own position in relation to the law via digital monitoring, as well as their relationship within the logistics industry. For example, customs brokers in Nogales, Arizona, discussed concerns that carriers could be stopped by Mexican police and that the driver would be unable to stop a container being searched. This would result in the intelligent seals being broken and the shipment being disqualified from the FAST/C-TPAT programme. Another concern among customs brokers in Nogales was how to ensure C-TPAT licensing requirements among their supply chain partners as many contracts, and the related liabilities for failure to complete schedules, were negotiated ahead of time. As both the Mexican agricultural sector and Mexican warehouses tended to hire short-term labour that changed rapidly, the idea that every node of the supply chain will be able to meet the C-TPAT requirements to hire only employees capable of passing the required background checks seemed unlikely. In both these situations, logistics providers on the U.S. side of the border voiced concern over what they perceived as their Mexican counterparts' inability to meet and maintain the techno-legal requirements of the FAST/C-TPAT program—a factor that belies an underlying notion of Mexico as a space incapable of complying with law, at best, and illegitimate or illegal at worst.

Mexican truckers also relayed similar stories highlighting concerns over police harassment. Some drivers were worried that police were beginning to use the concern of "security"—particularly the carriage of illicit cargo such as guns or drugs—as a way of harassing those who refused to pay bribes. Such harassment usually meant that truck containers were searched and intelligent seals broken to disqualify shipment from FAST entry at the border. Two truck drivers specifically said they were concerned that their employer or supervisor might blame them for not handling the situation well (i.e., discreetly paying the bribe to the officer) and, as a result, they could be docked pay or lose their job.

By lengthening official surveillance throughout the supply chain and by locating the assessment of *trusted* carrier capable of safely crossing the border into the United States, the FAST/C-TPAT programmes have the power to alter the tight-knit, family-oriented local logistics industry in Ambos Nogales. Throughout the nineteenth and twentieth century *trust* in the

Nogales logistics industry was built and maintained through social and familial networks, repeated face-to-face interactions, and assessed by individuals located at the border port. With the advent of digital monitoring, such assessments of trust are now linked to an actor's willingness and ability to subject themselves to particular forms of surveillance. The surveillance demanded by the FAST/C-TPAT programmes extend past the individual applicant to all points in the logistics chain and require the use of expensive mobile sensorised technologies. International logistics providers, as compared to local Nogales businesses, are much better positioned to meet these requirements, as well as the associated costs. As a result, the last decade has seen many local Nogales providers either go out of business or transform into franchisees of national or international logistics companies. In addition, many of these national and international companies bring in external managers and siphon off money; jobs that would have otherwise gone towards local Nogales residents and money that would have otherwise been spent in the local economy.

Adding to this, individual border officials in both Mexico and the United States still have the capacity to renegotiate this assessment of trust during face-to-face interactions. In this sense, *digital monitoring* technologies, rather than replacing, are added to the suite of heritage mechanisms for *visualisation* and *spatial constriction*. However, whether and how this dimension of *digital monitoring* is eventually integrated into logistics processes in a dependable manner that effectively and efficiently meets contemporary regulatory objectives still remains to be fully determined. In particular, Nogales logistics providers are concerned that as the requirements of the techno-legal assemblage at the border grow, both in complexity and cost, there is also a corresponding uncertainty as to the actual outcome. For these local business owners the assumption of such increasing risk is a difficult cost to bear and they may fear that their livelihoods and family businesses are being sacrificed in order to satisfy the increasing speed demanded by the global economy.

7 Conclusion

In international commerce, accelerated passage through border ports-of-entry is highly desirable as a cost saving mechanism that is particularly important for perishable commodities subject to spoilage (e.g., agricultural products, seafood, etc.)—the types of commodities that compose the majority of goods moving through Ambos Nogales. This chapter has been

a preliminary investigation aimed at elucidating how the tension between national security, the policing of contraband, and environmental concerns, on the one hand, and the need for speedy passage to accommodate commercial interests on the other, has been navigated in the design and adoption of the varied techno-legal assemblages selected and tested at the Mariposa Port in Ambos Nogales.

Nogales' history of border-related techno-legal experimentation and testing stretches back in time with early attempts to *visualise* and *spatially constrict* the border beginning in the 1890s, moving on to the building of the first permanent fences in 1918, and on to contemporary attempts to employ *digital monitoring* technologies as part of the Mariposa cyberport project. These efforts have historically been oriented around monitoring, identifying, and policing what moves across the international border. As the balance of legal and regulatory concerns have shifted, changed, or expanded over time, so too have the technologies used for the visualisation, spatialisation, and digital monitoring the border.

What has remained constant over time is that concepts of trust have factored heavily into the construction and maintenance of techno-legal systems over all periods. What has changed, however, is that *trust* is manifested in different ways. This directly shapes *control* over the physical movement of goods. Specifically, the authority to determine trustworthiness of shippers and goods was located in different places, had unique regulatory objectives, and functioned according to slightly different logics for each techno-legal assemblage reviewed (in local family relationships, in public views of open space, in the individual judgment of official border guards, and in different visualisation and tracking technologies). Each of these assemblages reflects a particular perception of the role of varied actors at the international border as a means of regulating, containing, and monitoring movements—primarily northbound movements. In many ways the commercial border ports-of-entry at Nogales have always been experimental hubs where both countries have trialled an assemblage of technology and law to strike a balance vis-a-vis competing legal, regulatory, and political concerns. As an experiment in constant motion these techno-legal assemblages also double as reflections of the deeper socio-historical relationships that mark and separate the communities and people inhabiting the border region.

The larger project underlying this chapter attempts to elucidate how the port is conceptualised as a gateway to the nation-state, as well as the role that law and technology play in controlling who and what is allowed

to pass through and into the country. In doing this, I hope to demonstrate that the border is constructed as a constantly shifting social experiment that balances, shapes, and interprets *trust* as a mechanism for *controlling* the physical flow of goods and people involved in legitimate commercial trade. In this sense, the design and deployment of socio-technical assemblages can be understood as one site in which law is interpreted, enacted, or performed on a daily basis in a manner that reaches into the lives of everyday citizens in both the United States and Mexico. While the everyday tempos of Nogales logistics industry appear to be somewhat unaffected by recent U.S. politics, activities of the Trump Administration, including the new United States-Mexico-Canada Agreement, may present another major point of departure through which the techno-legal assemblage at Ambos Nogales shifts. This shift, as with the ones in the past, will probably function to further separate the social, economic, and political linkages that have bound rural border regions with twin cities such as Ambos Nogales.

References

Appadurai, Arjun. 1986. *The Social Life of Things: Commodities in Cultural Perspective*. New York: Cambridge University Press.

Beckert, Sven. 2014. *Empire of Cotton: A Global History*. New York: Alfred A. Knopf.

Bonacich, Edna, and Jake B. Wilson. 2008. *Getting the Goods: Ports, Labor, and the Logistics Revolution*. Ithaca, NY: Cornell University Press.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out: Classification and Its Consequences*. Boston, MA: MIT Press.

Chan, Anita. 2013. *Networking Peripheries: Technological Futures and the Myth of Digital Universalism*. Cambridge, MA: MIT Press.

Coleman, E. Gabriella. 2013. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

Coutin, Susan Bibler. 2000. *Legalizing Moves: Salvadoran Immigrants' Struggle for U.S. Residency*. Ann Arbor: University of Michigan Press.

Cudahy, Brian J. 2006. *Box Boats: How Container Ships Changed the World*. New York: Fordham University Press.

Donovan, Arthur, and Joseph Bonney. 2006. *The Box that Changed the World: Fifty Years of Container Shipping – An Illustrated History*. East Windsor: Commonwealth Business Media.

Easterling, Keller. 2014. *Extrastatecraft: The Power of Infrastructure Space*. New York: Verso.

Fresh Produce Association of the Americas. 2018. Fresh Produce Association of the Americas Annual Report 2017–2018. Accessed March 21, 2019. https://cdn.freshfrommexico.com/wp-content/uploads/2018/05/10223204/Annual-Report-2017-18.pdf.

George, Rose. 2013. *Ninety Percent of Everything: Inside Shipping, the Invisible Industry That Puts Clothes on Your Back, Gas in Your Car, and Food on Your Plate*. New York: Metropolitan Books.

Henne, Kathryn. 2015. *Testing for Athlete Citizenship: Regulating Doping and Sex in Sport*. New Brunswick, NJ: Rutgers University Press.

Holmes, Seth M. 2013. *Fresh Fruit, Broken Bodies: Migrant Farmworkers in the United States*. Berkeley: University of California Press.

Hufbauer, Gary C., and Euijin Jung. 2017. NAFTA Mischief in Fruits and Vegetables. Trade and Investment Watch: A *Journal of the Peterson Institute for International Economics*. Accessed April 7, 2018. https://piie.com/blogs/trade-investment-policy-watch/nafta-mischief-fruits-and-vegetables.

Jasanoff, Sheila. 2011. *Reframing Rights: Bioconstitutionalism in the Genetic Age*. Cambridge, MA: MIT Press.

Kelty, Christopher M. 2008. *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press.

Kitroeff, Natalie. 2018. From Mexico to the U.S., a Nafta Tale of Two Truckers. *New York Times*, January 6. Accessed March 20, 2019. https://www.nytimes.com/2018/01/06/business/economy/nafta-border-truckers.html.

Klose, Alexander. 2015. *The Container Principle: How a Box Changes the Way We Think*. Cambridge, MA: The MIT Press.

Knight, Alan. 1986. *The Mexican Revolution: Counter-Revolution and Reconstruction*. Cambridge, UK: Cambridge University Press.

Landes, Amy. 2016, January/February. The Road to Nogales: A Modern Gateway for Mexican Produce. *Blueprints*, pp. 52–64.

Levinson, Marc. 2016. *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*. 2nd ed. Princeton: Princeton University Press.

MacNamara, Tom. 2004. Illegals from Terrorist Nations Are Crossing the Border into Arizona. *Eyewitness News 4 Investigators*, KVOA News 4, August 13.

Martin, Craig. 2016. *Shipping Container*. New York: Bloomsbury.

Medina, Eden. 2011. *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge, MA: MIT Press.

Mezzadra, Sandro, and Brett Neilson. 2013. *Border as Method, or, the Multiplication of Labor*. Durham: Duke University Press.

Mintz, Sidney W. 1986. *Sweetness and Power: The Place of Sugar in Modern History*. New York: Penguin Books.

Nevins, Joseph. 2002. *Operation Gatekeeper: The Rise of the 'Illegal Alien' and the Making of the US-Mexico Boundary*. New York: Routledge Press.

Parra, Carlos F. 2010. Valientes Nogalenses: The 1918 Battle Between the U.S. and Mexico That Transformed Ambos Nogales. *Journal of Arizona History* 51: 1–32.

Pavlakovich-Kochi, Vera, and Gary D. Thompson. 2013. *Foundations and Opportunities for Nogales and Santa Cruz County*. A Report Prepared for Nogales Community Development by the College of Agriculture and Life Sciences at the University of Arizona.

Rankin, William. 2016. *After the Map: Cartography, Navigation, and the Transformation of Territory in the Twentieth Century*. Chicago: University of Chicago Press.

Sorrensen, Cynthia. 2014. Making the Subterranean Visible: Security, Tunnels, and the United States-Mexico Border. *Geographical Review* 104 (3): 328–345.

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

Reflection IV

Jennifer Musto

In reflecting on this section's chapters, I bring my education in structural power, which comes by way of feminist theory. Its animating idea is that in order to understand structural power in all its unwieldy, obfuscating dimensions, attention must be paid to those whose lives are directly shaped by it. Relatedly, a feminist analysis of power demands an understanding of the structural inequalities it invariably produces and a corollary commitment to doing something about it. At core, Strange's theorisation of structural power centres on agenda-setting, "the power to decide how things shall be done" (Strange 1994, 25). Yet before agendas are set and decisions made in the name of political economy or security, a more elemental question arises: Who is invited to sit at the proverbial table of power in the first instance? Whose voices are heard and whose knowledge and experiences privileged as baseline starting points for understanding the multifaceted dimensions of structural power?

That Strange's work effaces consideration of how dominant cultural understandings of race, gender, sexuality, class, and religion—among and other social locations—shape the contours of power is a major blind spot of her work and underscores the limits of theories of structural power—

J. Musto (✉)
Wellesley College, Wellesley, MA, USA
e-mail: jmusto@wellesley.edu

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_13

Strangean or otherwise—that do not interrogate the conceptual starting points and hegemonic frameworks on which such theories hang. Moreover, I question whether Strange's framework is sufficiently equipped to capture the granular workings of structural power or in advancing a paradigm for justice and accountability for those who bear its most enduring effects.

In a volume that tackles knowledge governance from a number of angles, from the infrastructure and inner workings of the internet to the relationship between copyright and censorship, I find it fitting that this book concludes with detailed case studies by Allison Fish and Kathryn Henne. The other chapters in this volume take a macro view of our shared subject, knowledge governance, addressing important issues with far-reaching societal implications. Fish and Henne's chapters, meanwhile, deal with equally weighty issues but from the bottom-up. In particular, they draw attention to the people implicated by and through structural power. Although Strange's conceptualisation of structural power exists quite apart from feminist theories, Fish and Henne's chapters invite a feminist reading through a thoughtful engagement with her work.

Both chapters give us a sense of the geographically bounded and biologically intimate terrain in which knowledge structures manifest. Fish's exploration of the "techno-legal spaces" that have emerged in Ambos Nogales, a geographic borderland, tell us something about current social, political, and economic relationships of life within, beside, and along the U.S.-Mexico border. Henne's discussion of the Unique Identification Authority of India (UIDAI) offers a window through which to explore how a large-scale biometric project has conjoined state aspirations to deliver social assistance to poor and vulnerable residents with tools and expertise drawn from the private sector. Taken together, they help us to think through an essential, yet arguably underdeveloped dimension of structural power: chiefly, that an analysis of the knowledge structure ought to be paired with a robust discussion about the real people and real bodies whose lives are shaped and newly constrained by it.

1 Insights from Situated Approaches to Knowledge Governance

Both chapters prompt a reconsideration of what is gained—and what gets lost—if we myopically focus our attention on structural power without simultaneously asking whether the theories we utilise to describe it don't

explicitly focus on people who become socially relegated by it—that is, women and sexual minorities, racially marginalised people, the poor and economically disadvantaged, and people facing heightened economic vulnerability in these politically contentious times. Asked in a somewhat more pointed way: what's the point of theorising structures of power if the theories on offer do not also prompt us to take seriously the structural inequalities that consolidate it? And, what analytical and imaginative tools have the capacity disrupt it? These questions dovetail with—and draw inspiration from—scholarship by feminist surveillance studies scholars who suggest that feminist analysis ought to centre real people engaged in real activities. Rachel Dubrofsky and Shoshana Magnet state this point clearly:

> Implicit in most understandings of surveillance is the idea of real people being watched, often unknowingly, doing real things …. [F]eminist surveillance studies hails from a critical tradition that has at its core an activist and interventionist agenda, and a questioning of the taken-for-granted, of what is often mundane and seamless, with a profound sense that what goes unquestioned can be dangerous, particularly for disenfranchised bodies. Our critical feminist approach involves a feminist praxis that centers intersectionality. (Dubrofsky and Magnet 2015, 1–3)

As a theory, method, and "analytical strategy," intersectionality links individual experiences of oppression to structural power (Dill and Zambrana 2009, 4). By centring the lived experiences and "subjugated knowledge" of people marginalised by racial, gender, class, ethnic, and class differences—among other social identities—and pushing beyond a "single-axis" account of difference and identity, an intersectional approach to power offers a framework for theorising the processes through which inequalities are structurally produced and institutionally sustained (Dill and Zambrana 2009, 5–8). Dubrofsky and Magent's intersectional approach to surveillance, combined with an action-oriented framework of change to disrupt it, provides a conceptual scaffolding for thinking about knowledge structures, whether with respect to surveillance, biogovernance, or how people are newly subjected to different forms of social-legal control in the labour they perform. If we are to interrogate structural power and its implications, we need to question the taken-for-granted categories and subjectivities that may pass as "givens," not only to diagnose the problem but also to develop specific and targeted interventions to address the inequalities they produce.

The chapters by Fish and Henne make significant inroads through a situated approach to structural power as it plays out in relation to knowledge governance. Whether we are talking about the Mexican truck driver trying to get specialised FAST (Free and Secure Trade) and C-TPAT (Customs Trade Partnership against Terrorism) licences (Fish) or the Aadhaar users denied basic services and foodstuffs when their identity cannot be authenticated (Henne), what is of central importance is that it is real people who are being watched and controlled as they engage in doing everyday real things, an observation that cannot be emphasised enough. The fact that Strange has developed an influential body of work within International Political Economy (IPE) but does not include discussion of gender, patriarchy, or race as animating structures of power is striking. So, too, is it notable that her work excludes any discussion about how an individual's social location shapes their experiences and resistance to structural power.

Take the structural dimensions of race, for instance. The category of race, like gender, is elemental to power, the foundational building blocks on which power is wielded, denied, contested, and reworked. As critical race scholars Michael Omi and Howard Winant importantly point out, race is a "master category" par excellence. Like gender, its social construction belies its omnipresent reach in shaping all facets of history, culture, and economic possibility (Omi and Winant 2014, 106, 114). An exploration of race thus proves essential both in understanding how structural power works and in tracing the links between structural power and the structural inequalities it produces. Structural inequalities include but are not limited to structural racism, class inequality, and patriarchal oppression.

A cursory review of feminist contributions to questions of power vis-à-vis patriarchal structures highlights that inequalities endure due to the persistent gendered divisions of power, power that "dichotomize(s) political and apolitical actions, and separates public and private, reason and emotion" among other bifurcations (Runyan and Peterson 2018, 101). Since as early as the 1960s, these concerns have prompted feminists to pose a straightforward, yet still arguably under-theorised question to scholars in IPE: "Where are the women?" And, where do women fit in our theorisations of power (Runyan and Peterson 2018, 102)? Furthermore, as Kate Bedford and Shirin M. Rai (2010, 2) ask: Why is it the case that "gendered questions at the heart of the international political economy continue to be neglected?" In response, Bedford and Rai illustrate how feminist analyses and theoretical innovations complicate foundational tenets of IPE and provide a fuller account of the gendered,

sexual, and racialised dimensions of the political economy. Feminist critiques have been multifaceted. Among myriad of interventions that have been made in the IPE space, feminist scholars have drawn attention to social reproduction, the gendered ideologies that separate paid and unpaid labour growth, and the rise of "a new international division of labor that has been accompanied by the increasing mobilisation of female workers and the consolidation of a gendered division of labor" (Bedford and Rai 2010, 3; 7–10). What their examples aim to draw attention to—and where I think feminist scholarship in the IPE arena may help us to complicate our discussion about knowledge and power in the global economy—are the taken-for-granted categories that reproduce particular forms of structural power and attendant inequalities. Let us consider some of these insights in relation to the dimensions of structural power revealed through analyses featured in this anthology.

2 Reading Knowledge and IPE Through an Intersectional Lens

In connecting some of these ideas to Fish's chapter, we might reflect on how logistics, technologies, mobile sensors, and databases rework ideas about trust. How is trust leveraged to control the physical flow of goods and people, and don't these shifts stand to disrupt the "tight-knit" and "family-oriented" logistics industry (Fish, this volume)? If so, what are the effects? I would argue a more explicit feminist analysis might help us uncover gendered assumptions about the logistics industry, which might also inform "the range of technologies used in used in international transport" (Fish, this volume). On a cursory level, such a framework would help us to understand how masculinity and ideas about gender, race, nation, and migration intersect in shaping the logistics industry and how, for instance, the rollout of the FAST and C-TPAT programs and enhanced digital monitoring, constructs Mexican men's trucking labour in implicitly gendered ways. Not only does Fish's chapter invite us to ask questions about the uncertainty that drivers face in meeting certain requirements, it also prompts us to reflect on what a feminist analysis might help to further reveal. For example, I can't help but wonder how the techno-legal regulations truckers face on the road also shape the gendered division of labour at home or within some of the tight-knit families she mentions. What about the resulting anxieties? Do they put new kinds of pressures on the

families, the daughters, the wives, the women and girls doing or resisting the feminised (invisible) labour on which men's "productive" logistics and trucking and transport labour relies? In other words, the mechanisms of control and compliance do not simply impinge directly on truckers; they have spillover effects and lasting implications.

Henne's chapter explicitly raises issues of social power regarding questions of social inequality. By situating Aadhaar within the framework of biogovernance, we learn how a seemingly beneficial "voluntary" project to extend social welfare benefits to poor and marginalised communities in India, to provide secure forms of identification, and to reduce fraud nonetheless advances a surveillant agenda. Whereas this hybrid system makes recipients "hypervisible to authorities" (Henne, this volume), authorities are ill-equipped to manage or triage this sociotechnical system when certain details and critically important data are wrong. Moreover, the implications for the most vulnerable or multiply marginalised can be troubling and in expected ways.

As mentioned briefly in Henne's chapter, the linking of Aadhaar and PAN (Permanent Account Number) led to major challenges for many transgender citizens. Because the PAN application form did not include a third gender category, transgender applicants were more likely to miss the deadline for linking their accounts, which meant the cancellation of the PAN card. The story of Reshma Prasad, a transgender woman, serves as a case in point:

> Prasad's Aadhaar card identifies her as a transgender, but her existing PAN card reflects the gender assigned to her at birth, which was male. As a result of the mismatch, the two cannot be linked. To many, this may appear to be a technical error. But its implications are multiple and stand to impact the entire transgender population of the country, which according to the 2011 census, is around 488,000. (Ratnam 2018)

This situation highlights more than a contradiction of a programme pitched as voluntary. It shows ways in which the categories, frameworks, and seemingly mundane drop-down boxes and value neutral methods for collecting information—in this case, one's gender and more specifically, third gender—tie a state-orchestrated, technically augmented project of surveillance together with a gender classification system in which two and only two gender options are available.[1]

[1] Petitions have been filed with the Supreme Court to address this technical error (Express News Service 2018).

These chapters point to the possibilities of making connections to a dynamic literature of feminist, queer, and transgender scholarship that similarly highlights how poor and vulnerable people encounter intensive forms of surveillance and the ways in which surveillance systems reproduce gendered and racialised forms of citizenship that underwrite new forms of punishment (e.g., Spade 2008; Beauchamp 2014). Attention to socio-legal regulations (Fish) and an exploration of how system-linking and the technical settings used to execute it (Henne) signal other possibilities for using IPE questions of knowledge structure and governance as a launch-pad for engaging in a broader transdisciplinary exploration of the invisible labour, default assumptions, and disciplinary mechanisms that underwrite surveillant agendas and sociotechnical innovation more broadly.

3 The Past Informs the Present and Links to Public-Private Partnerships

Both chapters attempt to reconcile how practices of the past and in other contexts can help us to make sense of people and borders are controlled today. For Fish, the techno-legal systems employed to manage and control flows of goods, cargo, and people tell a longer "story" about the way that social, economic, and political relationships in Ambos Nogales "came to be" (Fish, this volume). Within it, we see the importance of how technologies are employed to render certain movements of goods and people and particular kinds of logistical arrangements trustworthy.

This idea of trust and the ways logistics function offers an illustrative site to understand the delicate balancing act between state-market interests and tensions in maintaining national security. In a moment in which a repertoire of technologies, both old and new, are so rigorously leveraged in the service of visualising and monitoring so-called "illegitimate" movements, states have created systems that authorise and "fast track" the movement of agricultural goods from Mexico to the United States in order to meet to meet the latter's teeming demand for prized and high-value agricultural commodities. That the United States would expand and intensify such systems to control and police illegitimate movements, while at the same time developing mechanisms to ship goods, grow markets, and protect capital in ways that save time, cut costs, and ensure a somewhat predictable return on capital investment is in some ways unsurprising. As scholars of borders and borderland theory observe, despite their

seeming opposition, "opening up some borders to allow for the flow movement of goods, capital, and some groups while erecting boundaries to restrict groups deemed undesirable such as unauthorised border crossers and terrorists" are interrelated, constitutive processes (Jones and Johnson 2014, 4).

Against the backdrop of a Mexico-U.S. borderland that has over the course of the past 138 or so years expanded, stretched, and "seeped" in new directions, Fish's exploration of the Mariposa Port of Entry and the development of the logistics industry draws our attention to the nuanced, and at times awkward, balancing act between controlling the flow of goods deemed legitimate and good for capital and flows of people (and goods) deemed illegitimate and a threat to national security. The delicate interplay reminds us that just as borders are "complex human creations perpetually open to question" (Agnew 2008, 8, as cited in Coleman and Streusse 2014, 40) so too does the border get made through public-private partnerships.

Indeed, considering the public-private partner piece helps to illuminate the diffuse ways in which promoting trade becomes a securitised goal. C-TPAT, for instance, brings together U.S. Customs and Border Protection and the private logistics industry in its stated aims to "safeguard the world's vibrant trade industry from terrorism" (Fish, this volume). C-TPAT states openly and explicitly that it allows its partners to "enjoy a variety of benefits, including taking an active role in working closer with the U.S. government in its war against terrorism" (U.S. Customs and Border Protection 2018). While such statements presume that they benefit from helping the U.S. Customs and Border Protection, it is worth noting that the same U.S. government is waging what some would call a war on the border. Indeed, commentators liken what is happening on the border to a war, drawing attention to how violence and murders that have occurred around the border "reflect a decades-long political project that's blurred the line between policing and militarization, between law enforcement and war" (Platt 2018). Donald Trump's order to deploy National Guard service members to the border is but one more recent data point among many that evidence heightened militarisation. The encouragement of private-public partnerships alongside aggressive efforts to secure the border, a situation described as ongoing militarisation and an all-out war, arguably suggests that techno-legal requirements to meet C-TPAT standards are attached to a broader security and military agenda in which Mexican truck drivers are conscripted.

Henne's chapter explores public-private partnerships in ways that show us other dimensions of the intersections between history, nation, and securitisation. Not only is Aadhaar the outgrowth of both technical and political efforts that braid state authority with private-sector technologies, its biopolitical dimensions reveal a kind of scope creep where demographic data can be mined—and I would say plundered—to benefit companies like Microsoft, Airbnb, Uber, and Ola that see demographic data as good for the bottom line. UIDAI's massive trove of data and the linkage to other systems, databases, and transactions relies on public-private partnerships, industry and state collaboration, and melds the goals of the state with a broader vision of India's economic growth. Yet, as Henne points out, these hybrid systems and biogovernance agendas are not immune to privacy breaches or, at least until recently, to mining by third-party private actors, a particularly tricky situation when companies can access Aadhaar-linked data and when no meaningfully protections are in place to prevent security breaches. These observations prompt some questions about commonsense ideas:

- What kinds of commonsense ideas authorise the radical transferability between security and trade logics? (Fish)
- What kind of commonsense ideas make Aadhaar demographic data ripe for corporate use? (Henne)

These questions point to foundational issues of accountability—or a lack thereof. The language of voluntary participation is present in both chapters, but it is clear that the participation is in fact not voluntary. Instead, knowledge governance in both cases requires coercion. What happens, though, when there is no guarantee or provision for accountability when data are accessed or used for other purposes? Fish notes that the C-TPAT licence is "completely discretionary and not subject to appeal by applicants" should they be denied (this volume). The fact that voluntary participation can be coercive aligns with key insights that Tusikov's chapter separately describes: namely, that consumer "choice" is increasingly constrained. What Fish's chapter further illuminates is that the constrained choices individuals face are symptoms of broader structural trends where "opting out" isn't really an option where no meaningful venues for accountability exists.

In light of these concerns, we might reflect further on Henne's reference to the work of Virginia Eubanks, a political scientist whose work focuses on bringing some degree of justice and accountability for wrongs caused

by data-based and predictive technologies. We might ask what recourse is available for women, poor folkx, transgender people, Dalits, racially subjugated, and Indigenous peoples who become hypervisible to the state and its non-state partners without any form of recourse? How do C-TPAT applicants deal with—and perhaps resist—discretionary power when appeals are not possible? What happens when Aadhaar results in denying people access to social welfare and other desperately needed services? These questions are pressing in an era of data-driven governance. If knowledge serves the interests of those who are already in power and if the reproduction of power emboldens those with it to newly set the terms in which participation is defined, a granular exploration of the constrained choices that individuals face in navigating it offers a generative platform for greater exploration of the emergence of sociotechnical systems and structures of power, that are, by their very design, immune to accountability. In this vein, we see that feminism is critically important in understanding the scope and effects of structural power in everyday life and attending to inequalities and injustices that emerge within systems of knowledge governance.

References

Agnew, John. 2008. Borders on the Mind: Reframing Border Thinking. *Ethics & Global Politics* 1 (1): 53–80.

Beauchamp, Toby. 2014. Surveillance. *Transgender Studies Quarterly* 1 (1–2): 208–210.

Bedford, Kate, and Shirin M. Rai. 2010. Feminists Theorize International Political Economy. *Signs: Journal of Women in Culture and Society* 36 (1): 1–18.

Coleman, Mathew, and Angela Stuesse. 2014. Policing Borders, Policing Bodies: The Territorial and Biopolitical Roots of US Immigration Control. In *Placing the Border in Everyday Life*, ed. Reece Jones and Corey Johnson, 33–63. Farnham, UK: Ashgate.

Dill, Bonnie Thornton, and Ruth Enid Zambrana. 2009. Critical Thinking About Inequality: An Emerging Lens. In *Emerging Intersections: Race, Class, and Gender in Theory, Policy, and Practice*. New Brunswick, NJ: Rutgers University Press.

Dubrofsky, Rachel E., and Shoshana Amielle Magnet, eds. 2015. *Feminist Surveillance Studies*. Durham, NC: Duke University Press.

Express News Service. 2018, March 29. Supreme Court Steps in as Transgenders Face Trouble with Aadhaar-Pan Linking. *Express News Service*. http://www.newindianexpress.com/nation/2018/mar/29/supreme-court-steps-in-as-transgenders-face-trouble-with-aadhaar-pan-linking-1794028.html.

Jones, Reece, and Corey Johnson. 2014. *Placing the Border in Everyday Life*. London: Routledge.

Omi, Michael, and Howard Winant. 2014. *Racial Formation in the United States*. London: Routledge.

Platt, Brian. 2018. A War in the Desert. *Jacobin*. Accessed March 22, 2019. https://www.jacobinmag.com/2018/05/united-states-mexico-border-immigration-deportation-military.

Ratnam, Dhamini. 2018. In Aadhaar-PAN Linkage, a Gender Lost. *Hindustan Times*, March 1. Accessed December 13, 2018. https://www.hindustantimes.com/india-news/in-aadhaar-pan-linkage-a-gender-lost/story-q2wGlBpVU-bIR79oslhoM1I.html.

Runyan, Anne Sisson, and V. Spike Peterson. 2018. *Global Gender Issues in the New Millennium*. 4th ed. London: Routledge.

Spade, Dean. 2008. Compliance Is Gendered: Struggling for Gender Self-Determination in a Hostile Economy. In *Transgender Rights*. Minneapolis, MN: University of Minnesota Press.

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

United States Customs and Border Protection. 2018. *CTPAT: Customs Trade Partnership Against Terrorism*. Web page. Accessed December 29, 2018. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat.

Conclusion: Looking Back, Looking Forward

Natasha Tusikov, Blayne Haggart, and Kathryn Henne

Our goal in this book, and the workshop from which it emerged, was to spur an inter- and multi-disciplinary dialogue on the rising importance of knowledge to the global political economy and the role of knowledge in contemporary governance. We wanted to better understand what knowledge governance is, how it functions in today's world, and how we might productively work together to confront the challenges that arise from living in the "information age." We also wanted to see if we could engage a common vocabulary that would allow us to reach across disciplinary, substantive, and theoretical boundaries to understand what we all intuitively saw as parts of the larger puzzle. Consequently, we looked to Susan

N. Tusikov (✉)
York University, Toronto, ON, Canada
e-mail: ntusikov@yorku.ca

B. Haggart
Brock University, St. Catharines, ON, Canada
e-mail: bhaggart@brocku.ca

K. Henne
University of Waterloo and Balsillie School of International Affairs, Waterloo, ON, Canada

Australian National University, Canberra, ACT, Australia
e-mail: khenne@uwaterloo.ca

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8_14

Strange's understudied and, as Haggart, Bannerman and Orasch, and German point out, somewhat underdeveloped conception of the knowledge structure to provide this common ground, a shared vocabulary to kickstart discussions on the role of knowledge as an increasingly important area of governance. In particular, we saw its emphasis on the control over the creation, dissemination, use, and legitimisation of knowledge as a promising focal point for the workshop and for future research. As we hope the chapters of this book attest, it did this and more: allowing us to improve our understanding of how the control of knowledge affects the wider society.

In this concluding chapter, we review the preceding chapters to address our two final outstanding questions: To what extent can the work of Susan Strange provide a starting point for our conversations about knowledge governance in the twenty-first century, and what is the nature of the contemporary knowledge structure? We also consider how focusing on the constructing of the "rules of the game," by both state and non-state actors, can allow us to make sense of some of the most ideologically charged questions emerging from a knowledge-focused society, including the regulation of social media and fake news.

1 Common Ground: The Utility of Susan Strange

In terms of creating a multidisciplinary common ground, drawing on Strange is useful because it involves only a few fundamental propositions and concepts. First among them is that to understand the social world one should focus on structural power—the ability to set and influence rules and norms. Second, state and non-state actors can exercise structural power. Third, the fundamental forms of structural power involve production, security, finance, and knowledge, all of which are interconnected.[1] Fourth, the regulation of the creation, dissemination, and use of knowledge, as well as its legitimation, are crucial areas for study. More colloquially, in setting up the workshop that led to this volume, we argued that even for those participants who were less familiar with Strange's work, if you think that state and non-state actors are important, and that knowledge-regulation is important, then you are ready for the workshop.

[1] Strange likely would have gone further and say that none are a priori more important than the others. Haggart in this volume argues that that is not quite correct, although it does not prove a fatal flaw to Strange's approach.

Consider the results. Each of the chapters in this volume shares a preoccupation with the control over knowledge as an important form of power, interactions between state and non-state actors, and knowledge-regulation in its many forms. They also emphasise the role of agency and actors, both state and non-state in structural power, and consider the resulting winners and losers of any power arrangement. Further, they are concerned with uncovering and assessing the role of authority: which actors and institutions have the capacity and legitimacy to wield power, and with what results.

That said, as the astute reader will note, not all of them engage to the same degree with Strange the theorist. Nonetheless, they all fit within a Strangean approach. This fit reflects the fact that the commitments that you need to engage with Susan Strange—a focus on regulation (broadly defined) and both state and non-state actors—are relatively minimal and more ontological (what is in the world) than epistemological (how do we know the world). They identify a core upon which scholars from different disciplines can focus to facilitate dialogue. The process did not, we think, convert to the Church of Strange those who were not already using her framework, but that was never the point of the workshop. Instead, this multidisciplinary endeavour illustrated how theoretical diversity can be an asset. Our interest in the concept of knowledge governance, in all its diversity, meant that we could not fall back on the study of a particular thing, such as surveillance or intellectual property, to provide this volume's coherence. Strange provided us with a valuable tool: a common language and framework to engage with colleagues in other disciplines who are engaged in many distinct (yet related) issue areas.

Reflecting upon each of the chapters and our workshop discussions, Strange usefully provided a common ground that stimulated fruitful theoretical and methodological debates despite our disciplinary differences. Most importantly, the degree to which we were all able to engage with Strange in our diverse case studies validated our original assumption that these issues—surveillance, intellectual property, data governance, biogovernance—can be analysed as facets of the same structure, functioning according to similar logics, and should be studied together.

This is not to say that it led to consensus understandings. We highlight two issues in particular, the first of which is related to inequality and identity, and the second to the difference between knowledge and data. While this volume is intended to be more a study of knowledge governance than

a work of Strangean theory, the involvement of Strangean neophytes served to spur a discussion over some conceptual problems in Strange's approach. Reflections by Randall Germain and Jennifer Musto capture in particular the question of the location of individuals in our analyses, as well as Strange's treatment of gender, race, and questions of inequality, which are arguably reducible to crude materialist conceptions. For Strange, her research focus on finance and issues in the global economy, and, in particular, her contention that governments were destabilising the financial system, a problem she documents in her final book, *Mad Money* (1998a), was a problem that outweighed gender inequality. Simply put, Strange was primarily concerned with analyses of structural power involving the dynamics of states and multinational corporations.

The absence of gender within Strangean theory prompted us to interrogate her ideas in this area. For example, as Musto asked during one of our sessions, can one *gender* Strange? Along the same lines, can one apply an intersectional analysis to Strange? What would a Strangean intersectional analysis actually look like? Given the other significant challenges with Strange's knowledge structure discussed throughout the book, would an intersectional Strangean approach even be possible? The closest we get to answering those questions are the chapters by Harb and Henne, Fish, and Henne, each of which considers the relationships between power over and through the control of knowledge and its differential effect on Indigenous peoples, Mexicans at the U.S.-Mexico border and economically and socially marginalised Indians, respectively. These analyses, combined with the fact that Strange's framework encourages thinking in terms of the differential effects of the exercise of structural power suggest that we can at least forge a middle ground between intersectional analysis and Strange's conceptions regarding structural power. These chapters further suggest the utility of attempting to do so.

One of the persistent challenges with Strange's knowledge structure is her conflation of knowledge and information, as Haggart discusses in his chapter. Given the interdisciplinary diversity of our contributors, we did not seek or even desire common definitions of knowledge, information, or data. In fact, we contend that the different understanding of these concepts in this volume is a strength that demonstrates the utility of thinking about knowledge governance from different disciplinary perspectives. Bannerman and Orasch, and Haggart articulate distinctions between knowledge and information in their chapters, and this is a subject worthy of further discussion.

The distinction between knowledge and information is particularly important when it comes to discussing data. The control and manipulation of data has emerged as much more central to daily life than it was at the time of Strange's death in 1998. This volume, particularly the chapters by Haggart, Tusikov, and Fish, lends support for the contention that data is socially constructed, that it is—in the terminology of this volume—a form of knowledge. Drawing from critical data studies (e.g., Gitelman 2013), Haggart's and Tusikov's chapters in particular suggest that changing information (independently existing) into data is a deliberate act that entails making decisions about data collection, categorisation, and storage. Fish, taking a slightly different, albeit complementary, approach, highlights the way surveillance and the resultant collection of data constructs fundamental and emotive notions, such as "trust."

One final issue of note: Strange is often criticised as not offering a "real" theory—a position with which she disagreed (Strange 1998b)—because hers lacks the elegance of other theorists, such as Mann (1986, 1993), who take a similar approach to *States and Markets.* A committed materialist, as discussed in the introduction of this book, she is criticised by poststructuralists for not taking ideas seriously enough (Langley 2009), while others note her bias toward the power of states. As we have already noted, actual persons do not tend to show up directly in Strangean accounts. Moreover, her theory, like all theories, is necessarily incomplete, which in any case would not have bothered her since she eschewed grand theorising. For our purposes, though, her purported weaknesses provided a foundation upon which we could build.

Strange is undoubtedly an unusual theorist, but it is this oddness that makes her particularly suited to cross-discipline dialogue and to generating useful research questions. She was a materialist who nonetheless included at the very heart of her theory the idea that the legitimation of knowledge was a key source of structural power: it is impossible to get any more immaterial than that. A focus on legitimation also opens up a possible focus on the role of identity construction and the exercise of power, both material and immaterial. She might have been state focused, but she explicitly emphasises the role of non-state actors. People, or bodies, may not be directly referenced in her approach, but her emphasis on winners and losers invites their inclusion in our analyses. In short, her approach is messy, but so is life. The key point is, it focuses us on some key relationships and allows for productive interrogations of the world around us.

2 Describing the Current Knowledge Structure

As the chapters in this book explore, knowledge-regulation entails considering how and why knowledge is legitimised and by whom, the interests served, and the specific power structures underlying these arrangements. Each chapter analyses a specific form or case of knowledge-regulation. Bannerman and Orasch reflect upon the reflexive interactions between the knowledge structure and Strange's other identified primary sources of structural power, while highlighting the importance of considering these interactions when analysing the emergence of, for example, digital communication technologies. Haggart, meanwhile, examines the insertion of intellectual property provisions within international trade agreements, which set rules about who gets to own and control knowledge in the form of copyrights and patents, as well as governing the use and ownership of global flows of data.

Winseck's and Tusikov's chapters shift the book to an assessment of knowledge governance in the interplay between the physical and digital realms in the form of internet infrastructure and the Internet of Things (IoT). Winseck explores the regulation of knowledge through physical and digital internet infrastructure projects being built in the Asia-Pacific and African regions by a complex array of state and private actors. Those who build, own, or operate this infrastructure may embed their preferred rules relating to, for example, the ownership of data or monitoring internet traffic. Tusikov, meanwhile, explores knowledge-regulation within the intellectual property rules, largely copyright, and corporate terms-of-service agreements that govern how consumers may use their IoT objects. Knowledge here is in the form of the IoT products' software, over which IoT manufacturers retain control and ownership, thereby significantly curtailing consumers' capacity to use and "own" the objects they have purchased.

In the next set of chapters, Halbert examines copyright law as a form of cultural and speech governance, while Harb and Henne's contribution considers how the governments use their power to create strategic mis- and disinformation about Indigenous peoples, while de-legitimising Indigenous speech and protest. Halbert demonstrates that copyright law enables copyright owners, especially large players in the music or software industries, determine who can be creative and the use and appropriation of creative works. While proponents of weak copyright laws have tended to argue against restrictive copyright laws for these reasons, its weaponisation

to target socially harmful speech raises uncomfortable questions not only about cultural regulation, but about the possible limits to free-speech advocacy.

Henne's and Fish's chapters move the book into an exploration of state surveillance practices as a form of knowledge governance over its subjects. Henne considers the state's tracking and authentication of social assistance recipients through data-intensive surveillance programmes as a mode through which to use knowledge about its subjects to govern—and arguably control—populations. Through a case study of India's Aadhaar programme, a biometric management system and the largest such project globally, Henne reflects upon the hybridity of this form of knowledge governance that brings together state and non-state actors, the latter principally technology providers. She argues that Aadhaar represents a new phase in the state's commitments to delivering services and to marking and delineating its subjects. Complementing Henne's analysis, Fish's chapter examines the emergence of a unique intersection of law and technology that facilitates the state's governance of the passage of commercial goods at land border ports-of-entry between the United States and Mexico. Fish contends that the state's determination of trustworthiness of commercial shipping actors operates as a form of knowledge governance that works to control the flow of people and goods involved in commercial trade across the border. Knowledge, in this case, is in the form of information ideologies and logics that are in the service of commerce, namely the movement of commercial traffic, which also draw upon securitised and militarised logics that underpin border areas.

3 Bringing It All Together

Strange's framework provides us with a way to think about the myriad changes affecting society, from the embrace of constant surveillance by liberal-democratic states and the emergence of intellectual property as a key driver of value in global production, to fears about social media's effect on democracy and the datafication of everyday life. They are all linked because they involve the construction of knowledge—that is, our mediated interpretation of reality. This does not just involve knowledge in the form of, say, books or cultural works, but knowledge of our own identities and others: who constitutes a threat, who is an ally? To understand the dynamics of a world dominated by the knowledge structure—as is early twenty-first-century society—we need to focus on the rules and norms that shape the legitimation, creation, use, and dissemination of

knowledge. Moreover, we must examine who is shaping these rules, which includes the state and non-state actors, and in whose interests. As Strange would ask, *Cui bono*—who benefits?

The contributions to this volume, supplemented by their related reflections, confirm the importance of several key areas and issues related to the construction of knowledge. In particular, they focus on:

- the increasingly ubiquitous surveillance that makes a knowledge-dominated society possible (Tusikov, Harb and Henne, Henne, Fish);
- the information technology, such as the internet, that undergirds our knowledge-based society (Winseck)
- the role of data (Tusikov, Henne, Fish) and intellectual property (Halbert, Tusikov) in constituting and regulating it; and
- our changing conceptions of how regulation should be deployed—at the border (Fish) or in the form of copyright (Halbert)—as forms of control.

In each case, moreover, state and non-state actors cooperate and compete to exercise structural power.

While the volume's authors broadly reflect upon the control of knowledge as a mode of governance, each chapter studies distinct expressions of knowledge governance in the current era. Bannerman and Orasch, as discussed earlier, consider how the knowledge structure can help explain the rise of and consequences from the knowledge- and data-intensive information society typified by the rise of sharing economy industries and data-driven platforms like Google and Amazon. Haggart, meanwhile, focuses on intellectual property and data-governance rules as a form of knowledge governance in international trade agreements. Halbert examines the use of copyright as a form of cultural governance exerted by institutional copyright owners to censor unwanted, but not always copyright-infringing forms of creative expression. Fish, Henne, and Harb and Henne, in contrast, examine various ways that governments control knowledge by leveraging information technologies to surveil, sort, and control different populations that their governments consider somehow risky. Winseck and Tusikov explore how technology companies exert control over knowledge through their provision of vital hardware and software infrastructure that comprises the internet, and their control over software that enables the functionality of Internet-of-Things objects.

3.1 Technology

Technology is an important element of the knowledge structure. Broadly conceived, technology involves systematised processes, machinery and devices, encompassing both new and old technology. Bannerman and Orasch, in their contribution, identify technology as a distinct part of the knowledge structure. Studying the relation of technology to practices of knowledge generation and regulation may involve examining how multiple systems of knowledge governance come to co-exist and inhabit the same space. Despite the differences in their empirical work, the chapters consider the role of technology, both as an object of regulation and as a regulatory instrument.

As many of the chapters argue, the emergence of techno-legal systems needs to be examined holistically and placed in historical context. Fish, for example, traces the historical emergence of state-deployed technologies to monitor and control movement across the United States-Mexico border. Halbert's "weaponisation" of copyright occurs online. Winseck, meanwhile, examines the growth of internet infrastructure in the Asia-Pacific and African regions in the context of previous communications technologies to reflect upon the future of internet governance in a world in which non-American actors increasingly control this infrastructure. By examining the interaction of law, regulation, and technology in facilitating knowledge governance, scholars can begin to diagnose the ways in which structural power is functioning and, equally importantly, identify and assess remedies to address the consequences of those power arrangements. The intersection of technology with human rights, especially in relation to state/corporate censorship of information and the contemporary problem with mis/disinformation is an important topic that demands additional scholarship.

The analysis of context enhances the study and scrutiny of how knowledge governance draws upon and can reinforce inequalities and social categories of difference. Henne and Fish explore how governments use various information communications and surveillance technologies to regulate targeted populations through knowledge. Importantly, these authors also focus on the populations under surveillance—Indian residents subject to Aadhaar, and Mexican truck drivers surveilled at land ports of entry—and the consequences of this surveillance. Harb and Henne accomplish something similar with their study of information strategically used to manipulate and control Indigenous peoples. The authors'

analytical focus is both on the systems of knowledge governance that facilitate government control over risky populations and on the often-detrimental effects they face.

Winseck and Tusikov, meanwhile, investigate the ways in which corporate actors can set or shape rules broadly relating to the creation or dissemination of knowledge by controlling access to systems of technical infrastructure. These rules can affect how people may use or even own internet-connected products and they shape the provision of internet infrastructure. Similarly, Haggart considers how the regulation of data is becoming a key element of international trade agreements, with the underlying idea that the free flow of data across borders being seen as an essential element of the global political economy.

3.2 Surveillance (State and Non-State)

Surveillance is another key element of the current knowledge structure. This volume considers the nature and ramifications of surveillance efforts by state and corporate actors, as well as the increasingly common hybridised public-private programs reliant upon the private sector for technology provision and data analytics. While their goals may differ, state and corporate actors have shared interests in the mass accumulation, mining, storage, and interpretation of personal data through the use of various monitoring technologies to predict or affect human behaviour. In particular, the growing role of private actors in technology provision and data analytics raises serious questions about the ethics and legitimacy of such hybridised surveillance projects. Fish and Henne, as well as Harb and Henne to a lesser extent, each reflect upon the role of corporate actors enabling state surveillance practices and pay particular attention to the ways that these practices entrench inequalities relating to class, race, gender, Indigeneity, and nationality. Winseck similarly explores the possible configurations of the surveillance programmes that will emerge from the complex consortia of public-private actors building and operating internet infrastructure in Asia and Africa. The chapters by Halbert and Tusikov, meanwhile, concentrate upon private actors monitoring the public for suspicion of copyright infringement.

Assessing the dynamics between state and non-state actors in regards to the creation and regulation of knowledge, whatever its particular form, is another key theme throughout the volume and one that echoes Strange's analysis. Throughout her work Strange argued for the importance of the

state in the global political economy (Strange 1994). The contributors reflect upon the role of the state in directing, facilitating or deriving benefit from governing knowledge and the relationship of the state with private actors in creating and regulating knowledge. In particular, Harb and Henne, Henne, and Fish draw attention to the rise of public-private partnerships in the provision of security knowledge in which private firms supply surveillance technologies that governments employ to monitor and manage certain populations. Winseck's exploration of public-private partnerships is in the context of the diverse consortia of government and corporate actors involved in building internet infrastructure in the Asia-Pacific and African regions. These public-private partnerships may bring together the local and global as national governments procure technology services from globally operating multinational technology companies. The long-term implications of these partnerships and, more broadly, the effects of private technology companies' accumulation of power through the provision of knowledge in the forms of data and technology are critical areas for future research.

Other private actors may rely upon the rules or structures established by the state in order to regulate knowledge or establish their own knowledge governance regimes. This is particularly apparent in the outsized roles that corporate actors have assumed in exploiting or shaping the direction of intellectual property regimes, as Halbert and Haggart each explore. Copyright owners, as Halbert explains, establish private enforcement regimes to protect their copyrights and accord themselves considerable latitude to remove content that they contend constitute an infringement of their creative works. These systems of private censorship rely upon copyright law for their authority and legitimacy. Similarly, the manufacturers of internet-connected goods in Tusikov's chapter use intellectual property law, bolstered by complex terms-of-service contracts, to extend their control over physical goods by laying claim over the products' software systems.

3.3 Knowledge, Information, and Data

One of the key points that emerges from an analysis of knowledge governance as a form of structural power is that the ability to legitimise what constitutes important knowledge, and to shape its creation, use and dissemination, is a form of power. Power and knowledge are inextricably linked. The regulation of knowledge in all of its forms is not a neutral

exercise, and the particular forms it takes has consequences. For example, decisions about what kind of data is important or useful to collect are indicative of underlying arrangements of power, and involve biases about what information is determined to be valuable. They influence what data is excluded or overlooked, what might be stored and how, and how the data is governed. This dynamic is described in Henne's study of Aadhaar and Fish's exploration of the Ambos Nogales border crossing. Knowledge is always partial, reflecting the fact that some data is always deliberately or inadvertently omitted from collection or analysis, and that our observation of some information reflects biases of gender, class, race, sexuality, or other social traits (see Crawford et al. 2014; for a perspective on colonialism, data, and Indigenous peoples, see Pool 2016). Scholars must therefore be attentive to identifying and assessing the underlying power dynamics and inherent biases in the creation and use of knowledge.

Control over data will increasingly be fundamental to the acquisition and expression of power, economically, politically, and socially, as the chapters in this volume attest. States and companies are recognising that they can set rules through the control over data—its collection, use, ownership, and, increasingly, its interpretation. Actors that have the ability and, equally importantly, the authority to interpret data can command a considerable capacity to regulate populations through knowledge governance. By amassing and mining data relating to health care or the criminal justice system, for example, data analytics companies are determining through proprietary algorithms what constitutes a healthy individual or risk for recidivism. Private actors' involvement as standard-setters in regard to what constitutes legitimate knowledge raises serious questions about their legitimacy, their accuracy and reliability of their algorithms, as well as user consent and privacy, particularly when they rely upon practices that amass and data-mine customers' personal data. Such standards are typically developed using proprietary software, which means that the underlying criteria and processes for determining what constitutes "normal" or "healthy" are not available for public scrutiny (see e.g., Pasquale 2015).

Companies operating data-intensive business models like Google, Amazon, and Samsung realise that the control over data is central to economic power. As the chapters by Tusikov and Winseck show, companies making internet-connected goods and building and operating internet infrastructure achieve economic dominance by controlling data. The free flow of data across borders, a now common feature of international trade agreements, as Haggart points out, generally privileges countries with data-intensive companies already dominant in data accumulation and

analytics. Data flows "freely" from users less data-intensive countries like Canada to large companies typically headquartered in the United States or the European Union, thereby entrenching those companies' economic advantage.

Strange's conception of the knowledge structure is particularly valuable for its early recognition that the creation of wealth in the global political economy is changing from the production of tangible objects to the production of intangible objects. This explains the value accorded to the software systems embedded within Internet-of-Things products. As Tusikov shows, manufacturers lay claim to the product's software and, in doing so, have the capacity to set rules governing the use of the product itself, as well as the data generated by the device. Those who control knowledge, in other words, can appropriate a disproportionate share of revenue from the value chain, as Haggart details in regards to intellectual property rules and international trade agreements. Controlling the means of knowledge creation and production also enables actors to shut others out of creative expression. Copyright owners, Halbert argues, have considerable power to determine who can share, stream, or use their creative works by wielding copyright as a system of private cultural governance, even of political speech.

3.4 Policy of "Truth"

Individual agency plays a central role in all of the case studies in this volume. The chapters in this volume are describing momentous, potentially epochal changes related the rising dominance of the knowledge structure. Despite this enormous context, these changes are the results of human decision and action. They are institutionalised in the form of rules and norms via structurally expressed power. By focusing on the making and shaping of these rules as they relate to knowledge, we can understand how power works, and can offer ways to think about the consequences of the expression of these powers.

The importance of structural power in terms of norms and rules is generally relevant, but focusing on it is particularly important in the knowledge structure. One of the principal insights from this project, and a cornerstone of Susan Strange's knowledge structure, is that knowledge is always regulated. There are always rules that regulate knowledge, whether formal or informal, whether implemented by state or non-state actors, and whether instituted by people directly or through technology. Knowledge is constituted by rules, and rules are set by people. Knowledge ungoverned

by rules is an impossibility. This point may flow logically from everything discussed in this book, but it is not easily grasped in a world influenced so deeply by the American concept of "free speech," in which speech in its natural state is supposedly unregulated, and in which any regulatory interventions is seen as inherently problematic.

That speech/knowledge always involves regulation and requires decisions about what these regulations should accomplish was a key point of Halbert's chapter. The reasons for regulating knowledge can change over time, from a church's prohibition of certain books as "sacrilegious" to governments' censoring of media articles as detrimental to the "national interest." Similarly, the mode of knowledge-regulation can change, as can the actors who are involved as regulators. Starting from the false premise that speech is free in its natural habitat has complicated reactions to some very important current challenges, particularly related to "fake news," disinformation (as Harb and Henne remark), and the dissemination of society-destabilising violent, racist, and misogynistic content on social media. While we were writing this book, the question of who can—or, more importantly, should—control knowledge in these areas was a very contentious topic.

Between 2017 and 2018, much of this debate focused on whether such destabilising speech should be regulated, and if so, whether it was the responsibility of non-state actors—that is, internet intermediaries, particularly the large, U.S.-based social media platforms YouTube, Facebook, and Twitter, or the state. For example, in July 2018, Facebook, Apple, YouTube, and a host of smaller platforms including Spotify and Pinterest removed videos, podcasts and other content from the U.S. right-wing conspiracy website Infowars for spreading hate speech. In their statements regarding the removal of the website's content, which is run by the far-right commentator Alex Jones, these technology companies cited content that was Islamophobic and transphobic, and that encouraged physical harm based on religious affiliation or gender identity (Wells 2018). Given Infowars' popularity among right-wing conservatives in the United States with an appetite for conspiracy theories, the removal of content elicited protests across the conservative media and charges of censorship (see e.g., Baker 2018).

Intermediaries' stance against Infowars, along with their similar efforts against a neo-Nazi website in August 2017 following the violent march by white supremacists in Charlottesville, Virginia (see Tusikov 2017), sparked a larger discussion about the nature of free speech and censorship, especially in the online environment. Articles in prominent media outlets such as *The New Yorker*, *The Guardian*, and *The Washington Post* debated the

role of private companies in determining hate speech and limitations on speech, and raised concerns of corporate over-reach and arbitrary censorship by powerful private actors, as well as worries of government censorship (e.g., Coll 2018; Greene 2018; Wong and Solon 2018). However, discussions about regulating speech can become unhelpfully polarised between extremes of censorship and absolute free speech, the latter typically referencing the U.S. First Amendment.

Touching, as it did, on fundamental questions related to "free speech" and the government's role in the economy, this debate hit several raw nerves, with calls for some form of regulation being challenged by worries about "censorship" of free speech. Similarly, many commentators were worried about the state assuming an undesirable role in regulating what people could say, leading democracies down an authoritarian, unfree path.

Both of these dichotomies are, however, based on a false assumption. Thinking about knowledge in the context of Strange's knowledge structure offers a way to move us beyond the rigid binaries of free speech versus censorship, or arguments that neither private companies nor governments should police speech. If, as Strange reminds us, all knowledge is regulated, then the choice is not between free speech and regulated speech, it is between different forms of regulation. A fundamental purpose of scholarship is therefore to determine how that regulation occurs, who benefits, and who bears the consequences.

Similarly, the fear of state regulation of social media is at least partly based on the assumption that non-state actors do not act in a regulatory manner, as if the rules that they enforce, say, through their terms of service, do not affect speech as directly as a government regulation. Web hosts, search engines, social media platforms, and other internet intermediaries have faced varying kinds of responsibility for third-party content on their platforms since the late 1990s (see e.g., Zittrain 2006). As well, scholars studying online content moderation from disciplines including law, communications, and criminology have explored intermediaries' policing of their platforms, through both their internal terms-of-service policies and legislation (e.g., Tusikov 2016; Noble 2018; Gillespie 2018). Facebook and Twitter have frequently courted controversy and attracted media attention with their complex and seemingly arbitrary rules regarding what they consider hate speech that should be removed from their platforms (see Roberts 2016). Twitter, for example, even controversially awarded "verified status badges" to the Twitter accounts of self-proclaimed

white supremacists before reversing that decision after protests against the company (Wong 2017).

An approach that focuses on the exercise of structural power, by state and non-state actors allows us to move the discussion beyond reasons why private companies and governments shouldn't remove certain information. Instead, we need to fully acknowledge that governments and, increasingly, private companies already regulate (censor) information, and focus our attention on how this regulation is occurring, its consequences, and the interests being served.

We also need to consider the social, political, economic, legal, and technological perspectives underlying the type of regulation (or regulatory actors) we may consider legitimate or illegitimate, and who it benefits/represents. Underlying much of the analysis of online content regulation in the United States, for example, is a strong ideological commitment to the First Amendment to protect free speech (see e.g., Gillespie 2018; Vaidhyanathan 2018). In contrast, in the European Union there is stronger support for the protection of individual privacy, indicating a different balance between free speech and privacy, as is evident in the EU's General Data Protection Regulation that came into force in May 2018 (see e.g., Butterworth 2018). The United States-European Union tension in the balance between freedom of expression and privacy usefully highlights the importance of values in framing how regulation operates in different spaces.

Different societies will strike different (and, for them, legitimate) balances regarding the regulation of speech, depending on their perceptions of the relative importance of particular values and issues. Similarly, both state and non-state actors can act as consequential regulators, although their ultimate goals and means by which they can be held accountable will differ. Focusing on the effects of specific regulations, including their effects on actual people, groups and societies, can be more useful than arguing abstract constitutional principles (Glaser 2018). Emphasising concrete harms and benefits can ground our discussions of these sensitive issues, a point made clear by Halbert's discussion of the intersection between commercial copyright regulation and hate speech. Similarly, Henne and Fish's chapters both address how surveillance is intimately bound up with concerns about state security and justice (e.g., in preventing fraud, in the case of Aadhaar), and individuals' and communities' civil and human rights.

Equally importantly, Strange reminds us that there is no generally accepted form of knowledge-regulation, of (to get metaphysical) truth. This is one of the key points emerging from Halbert's chapter. If knowledge

is always regulated, it will necessarily favour some forms of expression over others. This may seem like a self-evident assertion, but it deserves additional consideration when reflecting upon the nature of regulating knowledge. A lack of consensus on the nature of truth, for example, clearly poses a challenge for those who want intermediaries to remove fake news quickly and effectively, as well as for those companies like Facebook planning to rely heavily on algorithms to target problematic content (see e.g., Bickert 2018). Rather than a consensus on truth, there are different power structures that legitimise certain forms of knowledge and exclude others. The result is polarised views of what counts as truth, which can be problematically amplified by social media platforms that tend to reward controversial, conspiratorial, or inflammatory content (see Gillespie 2018).

At its base, a regulatory, Strangean perspective highlights that the main issue that those concerned about social media need to focus on is not whether they should be regulated, but by whom, and to what ends. It also highlights that, regardless of whether regulation is carried out by state or non-state actors, it will necessarily affect what knowledge is created and how that knowledge is used, and by whom. Whatever regulations are chosen, they will create winners or losers. Granted, a Strangean analysis does not necessarily lead to any easy solutions, but it does help clarify the nature of the debate, and allow for us to chart a path forward, fully understanding the nature of the game.

4 Conclusion: Continuing the Conversation

This volume is not intended as a definitive statement on knowledge governance, either in terms of how it should be studied, or its dynamics and effects. Rather than a capstone, we hope that it will serve as an argument that knowledge-governance issues should be considered within their wider contexts. Specifically, issues such as intellectual property rights, internet governance and surveillance cannot be considered in isolation; they are part of a larger knowledge structure and need to be considered as such, as Haggart, Tusikov, Winseck, and Halbert contend. So too must analysis investigate state-corporate dynamics, specifically how state or private actors may exert structural power and the particular expression and consequences of that power. Furthermore, as Bannerman and Orasch argue convincingly, and as Halbert, Harb and Henne, Fish, and Henne illustrate in their respective chapters, developments in the knowledge structure (including technological developments) can only be understood

fully by considering their situation within their historically specific social, legal, political, and economic context.

The chapters in this volume are wide-ranging in scope, yet they are all unified by a focus on knowledge governance and the knowledge structure. This eclecticism is a reminder that when defining knowledge and knowledge governance, and analysing its effects, we should cast a wide net. This volume, for example, has been relatively silent on issues of traditional, or Indigenous, knowledge. If studying power in the knowledge structure is about identifying who is and isn't setting the underlying rules, it is incumbent upon researchers to identify and research alternative existing and possible knowledge-governance regimes. And, we acknowledge the need to recognise and support the Indigenous scholars doing important work in these spaces (see, e.g., Kukutai and Taylor 2016; Tuhiwai Smith 2008).

Our discussants' reflections on the chapters they critiqued were intended to act as a reminder that this book is part of an ongoing conversation that we hope will be picked up by future students and researchers. We thus turn to them for some guidance on where and how we might continue this conversation.

Carr's discussion of the materiality of the Internet of Things and the internet itself suggests the importance of considering the intersections and interactions between the materiality of the physical and the immateriality of knowledge. On one level, it could involve focusing on how knowledge governance influences the material world, and vice versa, such as in the case of sensor-laden smart cities. Haggart's intervention, written in dialogue with Sherman, meanwhile, focuses on the relationship between the rules and authorities governing knowledge and the construction of legitimacy. This intervention is a reminder that the effects of knowledge governance stretch far beyond the marketplace and state-security-focused cyberwar issues. Power and rules in the knowledge structure legitimate truths and construct identities.

Germain, in his reflection, invites researchers to follow Strange's example and to get into the weeds of empirical research. We need to focus not just on the plumbing of power, or what's behind the walls—"who has power"—but also on how they exert structural power: "[W]hat resources do they have at their disposal, and how are these used to pursue policies that benefit them" (Germain, this volume). Strange, he reminds us, provides us with a framework, not "a grand theory designed to answer questions about how the world works." This framework has its share of contradictions, such as its unresolved (by her) tension between materialist

and non-materialist conceptions of knowledge. Nonetheless, her framework overall is conducive to generating questions. The knowledge structure is the physical networks in the sense of cables, logistics, and information systems that identify people and link them, and the information systems that identify things and link them together, and the rules and norms that govern their behaviour. Issues regarding control over the physical infrastructure and over the rules governing the legitimacy, creation, dissemination, and use of knowledge are very complex. Understanding these issues requires reaching across disciplinary barriers, including from International Political Economy. As this volume shows, this multi-disciplinary approach is both possible and highly productive. Our research agendas should embrace this complexity rather than shy away from it.

Strange, as Germain notes, was a big-picture thinker. While a bird's-eye view has its appeal and advantages, Musto's reflection reminds us that our research should never forget that actual people are implicated in these power relations. Again, the knowledge structure does not exist in a vacuum, but within a specific lived context of physical environment, race, gender, class, and ideologies. Analyses that ignore this context are missing the bigger picture.

Often, the most vulnerable persons are overlooked even though they are almost invariably the first ones subject to new coercive technologies of knowledge governance. Understanding the structural power at play in the knowledge structure is not just about identifying who has power, but who doesn't; not just who benefits (*cui bono?*) but also who suffers. Whether one's goal is to stabilise the world, as Strange wanted, or to change it, the first step requires understanding structural power, who has it, and who it affects, so as to make the invisible visible.

References

Baker, Brian. 2018. Horray for Censorship: Liberals Wetting Themselves with Delight After Twitter Permanently Bans Alex Jones and Infowars Accounts. *Clicks on the Right* (blog), September 7, 2018. Accessed November 8, 2018. https://www.wibc.com/blogs/chicks-right/hooray-censorship-liberals-wetting-themselves-delight-after-twitter-permanently.

Bickert, Monika. 2018. *Testimony Before the United States House of Representatives Committee on the Judiciary*. July 17, 2018. Accessed November 9, 2018. https://judiciary.house.gov/wp-content/uploads/2018/07/Bickert-Testimony.pdf.

Butterworth, Trevor. 2018. Europe's Tough New Digital Privacy Law Should Be a Model for US Policymakers. *Vox*, May 23. Accessed November 10, 2018. https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge.

Coll, Steve. 2018. Alex Jones, the First Amendment, and the Digital Public Square. *The New Yorker*, August 20. https://www.theguardian.com/technology/2018/aug/10/alex-jones-banning-apple-facebook-youtube-twitter-free-speech.

Crawford, Kate, Kate Miltner, and Mary L. Gray. 2014. Critiquing Big Data: Politics, Ethics, Epistemology. *International Journal of Communications* 8: 1663–1672.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press.

Gitelman, Lisa, ed. 2013. *Raw Data Is an Oxymoron*. Cambridge, MA: MIT Press.

Glaser, April. 2018. The Watchdogs that Didn't Bark. Slate.com. Accessed March 23, 2019. https://slate.com/technology/2018/04/why-arent-privacy-groups-fighting-to-regulate-facebook.html.

Greene, David. 2018. Alex Jones Is Far from the Only Person Tech Companies Are Silencing. *The Guardian*, August 12. https://www.theguardian.com/technology/2018/aug/10/alex-jones-banning-apple-facebook-youtube-twitter-free-speech.

Kukutai, Tahu, and John Taylor, eds. 2016. *Indigenous Data Sovereignty*. Canberra: Australian National University Press. https://doi.org/10.22459/CAEPR38.11.2016.

Langley, Paul. 2009. Power-Knowledge Estranged: From Susan Strange to Poststructuralism in British IPE. In *Routledge Handbook of International Political Economy (IPE): IPE as a Global Conversation*, ed. Mark Blyth, 126–139. New York: Routledge.

Mann, Michael. 1986. *The Sources of Social Power, Volume 1: A History of Power from the Beginning to AD 1760*. Cambridge: Cambridge University Press.

———. 1993. *The Sources of Social Power, Volume 2: The Rise of Classes and Nation States, 1750–1914*. Cambridge: Cambridge University Press.

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

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Pool, Ian. 2016. Colonialism's and Postcolonialism's Fellow Traveller: The Collection, Use and Misuse of Data on Indigenous People. In *Indigenous Data Sovereignty: Toward an Agenda*, ed. Tahu Kuktai and John Tailor, 57–76. Canberra: ANU Press.

Roberts, Sarah T. 2016. Commercial Content Moderation: Digital Labourers' Dirty Work. In *The Intersectional Internet: Race, Sex, Class and Culture Online*, ed. Safiya Umoja Noble and Brendesha M. Tynes. New York: Peter Lang. Accessed November 9, 2018. https://ir.lib.uwo.ca/commpub/12/.

Strange, Susan. 1994. *States and Markets*. 2nd ed. New York: Continuum.

———. 1998a. *Mad Money*. Manchester: Manchester University Press.

———. 1998b. *What Theory? The Theory in Mad Money*. CSGR Working Paper No. 18/998. Accessed November 8, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=146958.

Tuhiwai Smith, Linda. 2008. *Decolonising Methodologies: Research and Indigenous Peoples*. New York: Zed Books.

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

———. 2017. Why We Shouldn't Cheer for White Supremacist Website Deletions. *The Conversation*, August 21. https://theconversation.com/whywe-shouldnt-cheer-for-white-supremacist-website-deletions-82810.

Vaidhyanathan, Siva. 2018. *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford: Oxford University Press.

Wells, Sarah. 2018. *Here Are the Platforms That Have Banned Infowars So Far*. Updated August 13, 2018. TechCrunch. Accessed November 8, 2018. https://techcrunch.com/2018/08/08/all-the-platforms-that-have-banned-infowars/.

Wong, Julia Carrie. 2017. Richard Spencer and Others Lose Twitter Verified Status Under New Guidelines. *The Guardian*, November 15. https://www.theguardian.com/technology/2017/nov/15/twitter-verified-blue-check-marks-richard-spencer.

Wong, Julia Carrie, and Olivia Solon. 2018. Does the Banning of Alex Jones Signal a New Area of Big Tech Responsibility. *The Guardian*, August 10. https://www.theguardian.com/technology/2018/aug/10/alex-jones-banning-apple-facebook-youtube-twitter-free-speech.

Zittrain, Jonathan. 2006. A History of Online Gatekeeping. *Harvard Journal of Law & Technology* 19 (2): 253–298.

Index[1]

[1] Note: Page numbers followed by 'n' refer to notes.

B. Haggart et al. (eds.), *Information, Technology and Control in a Changing World*, International Political Economy Series,
https://doi.org/10.1007/978-3-030-14540-8