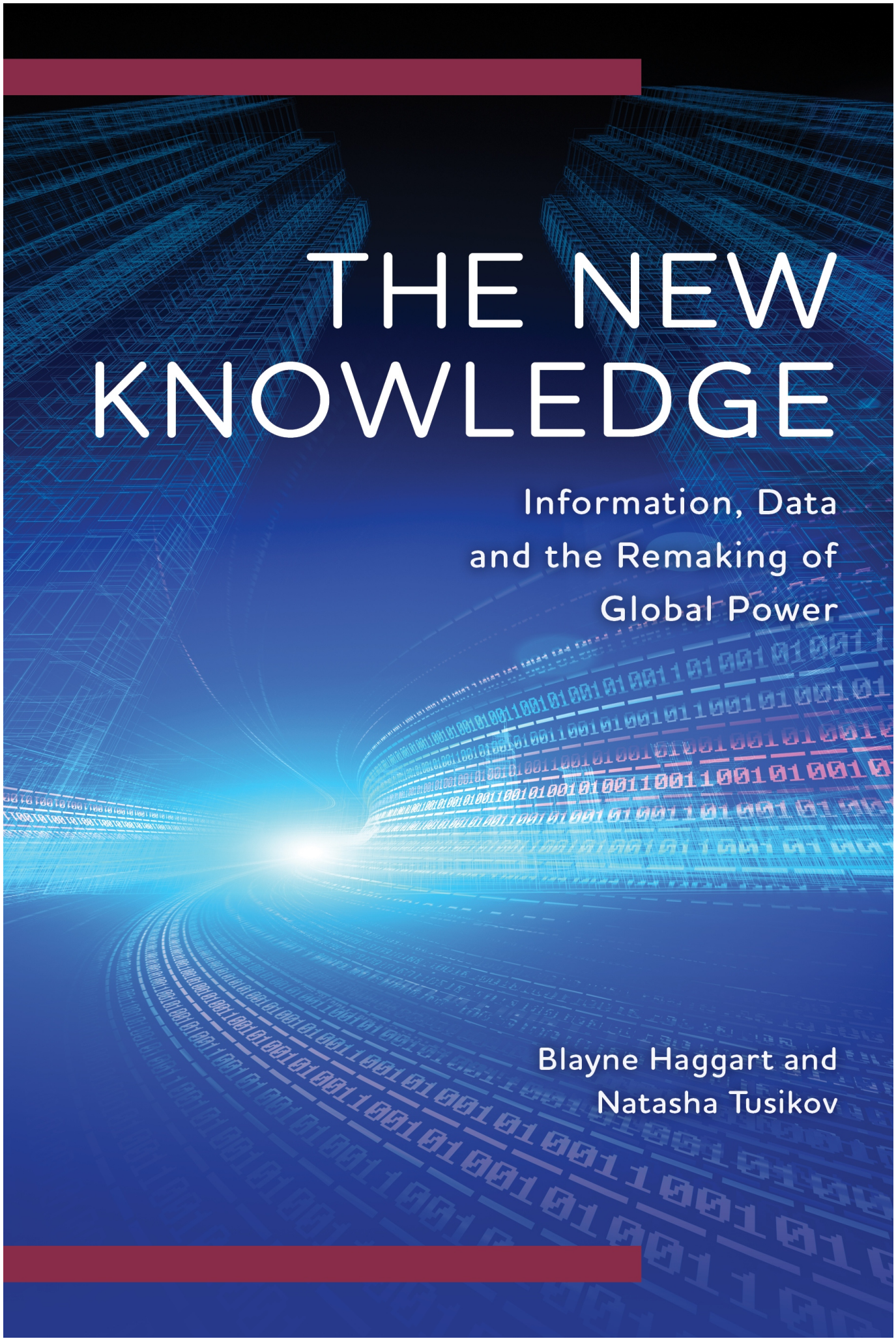
THE NEW KNOWLEDGE
Information, Data and the Remaking of Global Power
Blayne Haggart and Natasha Tusikov

The New Knowledge

Digital Technologies and Global Politics

Series Editors: Andrea Calderaro and Madeline Carr

While other disciplines like law, sociology and computer science have engaged closely with the Information Age, international relations scholars have yet to bring the full analytic power of their discipline to developing our understanding of what new digital technologies mean for concepts like war, peace, security, cooperation, human rights, equity and power. This series brings together the latest research from international relations scholars – particularly those working across disciplines – to challenge and extend our understanding of world politics in the Information Age.

Governing Cyberspace: Behaviour, Power and Diplomacy
Edited by Dennis Broeders and Bibi van den Berg
Internet Diplomacy: Shaping the Global Politics of Cyberspace
Edited by Meryem Marzouki and Andrea Calderaro
The New Knowledge: Information, Data and the Remaking of Global Power
Blayne Haggart and Natasha Tusikov

The New Knowledge

Information, Data and the Remaking of Global Power

Blayne Haggart and Natasha Tusikov

ROWMAN & LITTLEFIELD
Lanham • Boulder • New York • London

Published by Rowman & Littlefield
An imprint of The Rowman & Littlefield Publishing Group, Inc.
4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706
www.rowman.com

86-90 Paul Street, London EC2A 4NE

British Library Cataloguing in Publication Information Available

Library of Congress Cataloging-in-Publication Data

Names: Haggart, Blayne, author. | Tusikov, Natasha, author.
Title: The new knowledge : information, data and the remaking of global power / Blayne Haggart and Natasha Tusikov.
Description: Lanham, Maryland : Rowman & Littlefield, [2023] | Series: Digital technologies and global politics | Includes bibliographical references and index. | Summary: "Offers a unique and comprehensive overview of knowledge-governance issues in the 21st century through the novel, concrete and easily accessible lens of a single crucial smart-city project"— Provided by publisher.
Identifiers: LCCN 2023007635 (print) | LCCN 2023007636 (ebook) | ISBN 9781538160879 (cloth : acid-free paper) | ISBN 9781538160886 (epub)
Subjects: LCSH: Knowledge management. | Knowledge, Sociology of. | Internet governance. | Intellectual property—Management. | Power (Social sciences)
Classification: LCC HD30.2 .H338 2023 (print) | LCC HD30.2 (ebook) | DDC 658.4/038—dc23/eng/20230316
LC record available at https://lccn.loc.gov/2023007635
LC ebook record available at https://lccn.loc.gov/2023007636

♾™The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992.

Contents

Acknowledgements

This book brings together research interests and questions that we have been developing in various places for almost a decade. Like all such books, it is a culmination of a journey of many steps, and one that has been helped by so, so many others.

Our interest in and research on knowledge governance and the complex interplay of state and non-state actors dates back to our dissertations and first books: *Copyfight: The Global Politics of Digital Copyright Reform* (2014) for Blayne and *Chokepoints: Global Private Regulation on the Internet* (2016) for Natasha. We developed and refined the theoretical framework and many of the empirical case studies we draw on here in a series of journal articles, chapters in edited volumes and opinion pieces.

In the course of preparing this book, we conducted a number of interviews with academics, activists and policy experts in Canada, the United States and Brazil. Their contributions helped to shape our understanding of and sensitivity to questions of power asymmetries and of the consequential importance of the control over knowledge and intellectual property in contemporary society. We thank them profusely.

We owe a great debt to everyone who participated in the workshop that led to our first co-edited volume (with Kathryn Henne), *Information, Technology and Control in a Changing World* (2019), which served to test the utility of a Susan Strange–focused approach to knowledge governance.

We owe a similar debt to those who participated in our second co-edited volume (with Jan Aart Scholte), *Power and Authority in Internet Governance: Return of the State?* (2021). That volume was produced with the Käte Hamburger Kolleg/Centre for Global Cooperation Research (KHK/GCR) at the University of Duisburg-Essen in Germany, where we served as the

centre's inaugural fellows working on internet governance in 2018–2019. Thanks to Jan Aart Scholte for recruiting us, and to Jan, centre co-director Sigrid Quack and the centre for their support.

That second workshop and volume allowed us to further develop our thinking around the role of state and non-state actors in knowledge governance and data/internet governance specifically. Both workshops were an opportunity to learn from brilliant scholars from diverse disciplines; they represent high points in both our professional lives.

We also benefited from formal and informal feedback from talks we gave exploring various aspects of the arguments we develop in this book. We left all these talks richer in our understanding of our subject. In particular, we would like to thank the Weizenbaum Institute for the Networked Society in Berlin for their feedback in talks and for hosting Blayne as a senior fellow for an incredibly productive month just before the pandemic shut down the world. We can't wait to return to Berlin once we've seen the end of the pandemic. We would also like to thank the University College London's Department of Science, Technology, Engineering and Public Policy (STEaPP), Ingrid Schneider of the University of Hamburg, and the Centre for Advanced Internet Studies (CAIS) at the University of Bochum, for inviting us to speak.

Thanks to Dan Breznitz for confirming very early on our suspicion that a book on how the focus on the control over knowledge is affecting the exercise of power could be a useful endeavour and to Jim Balsillie for his support and insights into the importance of data and IP in the economy and society. Thanks also to Clara Iglesias Keller for the platform policy discussions and for her comments on several chapters.

Parts of this manuscript also benefited from the keen eyes of Randall Germain, Liam Midzain-Gobin, and Herman Mark Schwartz. All the usual disclaimers apply. We also want to acknowledge and thank the Social Sciences and Humanities Research Council of Canada (SSHRC), whose financial support made this project possible. Thanks also to the Käte Hamburger Kolleg/Centre for Global Cooperation Research and the Weizenbaum Institute for hosting us while we wrote and conducted research on the book, to Judy Dunlop for preparing the book's index, to Nancy Mackenzie for copyediting and to David Hodges for a last-minute proofread.

We'd also like to thank the following for discussions about data, knowledge governance and smart cities as a microcosm of the digital economy: Guy Baeten, Carina Listerborn and Maja de Neergaard in Sweden, and in Canada, Mariana Valverde, Alexandra Flynn, Neve Peric and Zachary Spicer.

Thanks to Susan Sell and Jan Aart Scholte for championing our work. Sara Bannerman is not only a friend stretching back to our days as public servants in Ottawa but the possessor of one of the keenest minds we know and someone who is always up to join us in a journey down yet another fascinating

theoretical rabbit hole. And a repeat shout-out to Kate Henne for joining us on the journey of our first edited volume. RegNorth is just around the corner.

We would like to end this litany of gratitude, first, by thanking Madeline Carr and Peter Drahos for their ongoing support and encouragement, two people whom we've adopted as mentors (whether they know it or not) and whom we feel fortunate to count as friends.

Second, we dedicate this book to the School of Regulation and Global Governance (RegNet) at the Australian National University. Major parts of our academic journeys started at RegNet – Natasha as a doctoral student and currently a fellow and Blayne as a researcher, fresh from completing his PhD. We continue to be inspired by RegNet's focus on regulation and governance in pursuit of a more just and equitable world.

Introduction

On the evening of 1 November 2017, we tuned into a live-streamed town hall meeting to see the future. Two weeks earlier, in the presence of Canada's prime minister, Ontario's premier and Toronto's mayor, Waterfront Toronto, a quasi-government agency responsible for developing Toronto's waterfront, announced the selection of a partner to help them design a smart neighbourhood, Quayside. The winning firm was Sidewalk Labs, a company created by Google in 2015 to get in on the bourgeoning smart-city market. This November town hall, hosted by the heads of Sidewalk Labs and Waterfront Toronto, was to be the Quayside project's coming-out party. In addition to the live stream, several hundred residents packed the hall to hear what these two organizations envisioned for the neighbourhood and for their city.

Sidewalk Labs had won the bid to propose a smart city in Quayside, a 12-acre piece of underdeveloped industrial land on Toronto's eastern waterfront. Welcomed enthusiastically by all levels of government, from Prime Minister Justin Trudeau on down (Bozikovic 2017), this was their chance to build a neighbourhood 'from the internet up', as they put it in their earliest promotional materials (e.g., Doctoroff 2016), a phrase that also featured multiple times in their submission to Waterfront Toronto (Sidewalk Labs 2017a, Appendix; Haggart 2019b).

As researchers interested in intellectual property (IP) rights, data governance and internet governance, we were curious to see what the two organizations had planned, and, more broadly, how they would deal with the data-intensive, always-connected, IP-underwritten issues that lie at the heart of any smart city. What we heard was heavy on dreams but light on details. We heard about how their plans would address climate change, housing affordability and transportation issues and improve community engagement through the deployment of new technologies. On offer was a utopian vision

of self-driving cars, heated sidewalks and even 'robotic vehicles that whisk away garbage in underground tunnels' (Gray 2018).

As exciting as these technologies sounded, the town hall was most interesting for what the organizations downplayed. The thing about projects like this – the thing about a knowledge-driven society – is that their most consequential aspects lie beneath the surface. The always-on connectivity on which smart cities depend to provide their services (Kitchin 2014b, 1–2) requires both constant surveillance and the collection of both personal and non-personal data. Computer systems are software-based and are protected by IP rights that restrict who can use these systems and how they can use them. Most, if not all, of the technologies they were proposing for this Toronto neighbourhood touched on all of these issues.

This focus on the physical infrastructure, such as heated sidewalks, pushed to the side the key policy questions in a knowledge-driven society, all of which are related to issues of control over the knowledge – the data and IP – embedded in these projects: Who should have it, how should it be used and in whose interests are they being used?

POWER IN A KNOWLEDGE-DRIVEN SOCIETY

Control over knowledge – particularly over data and IP – has become, to paraphrase International Development scholar Lynn Mytelka, a primary 'vector of structural power in the international political economy' (Mytelka 2000, 42).[1] What we saw, and what unfolded in Toronto, was bigger than the city itself.[2] Quayside, and smart cities generally, are a specific case of the more general phenomenon that we will be exploring in this book, namely, the increasing importance of control over the legitimation, creation, dissemination and use of knowledge as a vector of power. Quayside's challenges recur as a *leitmotif* throughout this book, a reminder of the grounded nature and concrete relevance of questions of knowledge regulation, of the extent to which this focus on the control of knowledge is transforming society at all levels.

We do not claim that knowledge didn't previously matter: 'knowledge is power' is a cliché for a reason. Humans have always produced and used data, just as we have always been creative. What's changed, however, is the *relative* importance we accord to the control of knowledge. We have moved from being a society that uses knowledge (as all societies do) as a means to accomplish various ends to a society in which the creation and control of knowledge have become economic and social ends in themselves. A participant at a May 2018 clean technology conference described it nicely to one of us (Haggart). Think about the sensors placed on tractors to measure, for example, soil compaction, moisture or other environmental conditions. Previously, the primary economic value for the sensor manufacturer would have

been in the production and sale of the sensors. Now, however, there is more money to be made by almost giving away the sensors and selling access to the data produced by the sensors, either to the farmer or to a company looking to aggregate data across many farms. Physical sensors had become merely the means to an end: data collection.

It's not only tech companies like Amazon or Google that are driven by data. The embrace of data-driven business models is an economy-wide phenomenon, with companies like Siemens and Rolls-Royce adopting a 'platform' model designed to capture as much data as possible from their production processes and from their products (Srnicek 2017).

We see a similar phenomenon at play with respect to IP. Intangible assets – not only IP but also 'brand names, research and development, patents and other forms of abstract capital such as digital platforms and data flows' – have moved from being 'a residual asset category known as "goodwill"' to overtake 'so-called fixed or tangible assets in the profitability and valuation of many leading corporations' (Bryan et al. 2017, 56). Intangible assets, which include IP, account for anywhere from 50 percent to 84 percent of the market value of the Standard and Poor's 500 index (Monga 2016; Ocean Tomo, LLC 2015).

This phenomenon has transformed manufacturing. Strong global legal protections for IP rights have given rise to 'so-called "manufacturers without factories" (like Nike and Apple), and global "retailers with (contract) factories" (Ikea and Walmart)' (Bryan et al. 2017, 57). In this business model, control over IP and data allows for control over companies that actually manufacture products. If you control the IP – the algorithms, designs, creative content or symbols – in something, you can control how that IP is used by others. Economically valuable IP is an essential component for a country or company wanting to position itself advantageously in a world of global value chains. Simply put, if the IP you control proves fundamental to a new technology, the pay-offs can be extraordinary.[3]

Apple, famously, is able to appropriate the lion's share of the profits from its iPhones through its control over the IP embedded in these physical products, that is, the knowledge used to build a smartphone (Dedrick et al. 2010). The production might happen in China (or elsewhere), but most of the money flows to Apple's headquarters in Cupertino, California. The global value chains that now structure a significant part of the global economy are made possible by IP, which creates and protects value in knowledge, and data, which allows home firms to exert control over far-flung operations. This change, as International Political Economy (IPE) scholar Herman Mark Schwartz has observed, has created a hierarchical economy in which a few IP-rich firms in a few Global North countries (primarily the United States) appropriate the lion's share of profits, worsening problems of income inequality and making it much more difficult for countries to climb the economic-development

ladder (Schwartz 2021; see discussion in chapter 3). Schwartz's work raises the uncomfortable possibility that the knowledge-driven society, far from delivering widely shared prosperity and economic development, is leaving most people and countries worse off.

Nor are global value chains the only part of the global political economy that runs on data and IP. Governments are increasingly turning to data- and surveillance-driven automated processes – colloquially known as artificial intelligence and regulation-by-algorithm – to provide services and security. A prime example of this tendency can be found in the smart city (see Edwards 2016; Kitchin 2014b; Shelton et al. 2015). The 'smart' infrastructure that comprises a smart city only works through constant data collection by ubiquitous networks of sensors. The data collected by governments, corporations or other organizations can be used not just to deliver the bells and whistles promised by innumerable tech start-ups but can also be deployed to pursue nefarious policies, such as denying certain classes of people access to services if they fit a certain data-constructed profile (Pasquale 2015; Eubanks 2018).[4] Data can also be repurposed for other reasons, including improving machine-learning processes (whose uses, similarly, may or may not be socially beneficial) or selling advertising.

While data and IP are usually treated as separate issues, they are part of a general phenomenon: the reorienting of the economy and society towards the capture and control of knowledge.

A society and economy focused on the control of knowledge *in and of itself* functions differently from one in which the primary focus is, say, manufacturing or the maximization of financial wealth. It empowers different sets of actors with different sets of priorities and brings to the fore policy challenges that previously had lurked in the background. What's more, a knowledge-driven society follows its own particular logic, which manifests in challenges to previously deeply embedded norms. For example, as we see with the expanding universe of the Internet of Things (IoT) – physical goods whose functioning depends on the networked software embedded within them – control over the data produced by an internet-enabled device means that effective ownership often remains with the vendor, not the purchaser of that physical good. As chapter 7 discusses, this reorientation of effective ownership away from the purchaser is made possible through a combination of ubiquitous surveillance via digital, networked technologies. This is not just a technology story: this form of control is reinforced by contract and IP laws that privilege a property-rights regime that allows owners of IP to determine how knowledge is used (in this case, the software that enables the functioning of internet-connected goods) (Perzanowki and Schultz 2016). Because data (whether it's collected for commercial or security purposes) must be observed to be gathered, and IP must similarly be monitored to be enforced, the emerging knowledge-driven society necessarily privileges reduced privacy rights in both commercial and political interactions.

Given the centrality of property and privacy norms to liberal-democratic societies, these changes have the potential to enact far-reaching and fundamental shifts in the exercise of political and economic power.

UNDERSTANDING KNOWLEDGE-DRIVEN POWER

This book is a guide to and analysis of these changes and of the emerging phenomenon of the knowledge-driven society. It explores the emergence, nature and consequences of the knowledge-driven society, how the knowledge-driven society works, who controls it and to what end.

Much of what we cover in these pages will not be news to the many IP and critical data specialists and communications scholars whose work we draw upon to make our argument. After all, we were not the only ones with questions about Waterfront Toronto's smart-city plans. Over the two-plus years after that initial town hall meeting, before Sidewalk Labs abandoned the project in May 2020 in the early throes of the global Covid-19 pandemic, local activists and some local tech entrepreneurs raised just these questions in vociferous opposition to the Quayside proposal. Although Sidewalk Labs' abandonment of Quayside was due to a complex mix of changing internal-to-Google priorities and its inability to secure rights to land beyond Quayside's original 12 acres (O'Kane 2020), local activists helped to slow the approval process, and in doing so, drew attention to the project's myriad flaws. The immediate and negative reaction of the activists and businesspeople who questioned the project focused not on traditional NIMBY (not in my backyard) development issues but rather on the questions that lie at the heart of knowledge-driven society: who controls what knowledge and in whose interests.

While these activists understood the actual stakes of the Quayside project, the issues at play around data governance and IP rights remain shrouded in mystery for many people. Understanding the scope and implications of the transition to a knowledge-driven society can be a daunting task for policymakers and engaged citizens trying to figure out how to navigate this changing world. The key components of our knowledge-driven society – data, IP and knowledge itself – are largely intangible. A knowledge-driven society requires that we pay particular focus to questions of knowledge governance, but the idea of knowledge governance itself can be hard to grasp. The subject requires that we think about the nature of knowledge and reality, since it is the manipulation of knowledge, as data and IP, that forms the foundation of a knowledge-driven society. Most people – and even most academics – would be happy to leave such questions to impenetrable French philosophers.

If thinking about intangibles can seem daunting, IP law itself is even less welcoming, a maze of rules and exceptions that strikes fear into the heart of the uninitiated, or even those who are well versed in IP law. A senior IP scholar

of our acquaintance once confessed that current copyright law is so convoluted that they would teach basic concepts like the public domain (roughly speaking, the body of creative works that lie outside copyright protections) using historical examples like Shakespeare. Under today's copyright laws, attributing rights correctly is a complex process that's rarely clear-cut, which is great for lawyers paid to litigate these issues, but suboptimal for the rest of us.

Data, meanwhile, has taken on an almost mystical status, the fuel of algorithms and artificial intelligence (both equally talismanic terms). It also doesn't help that, as political scientist Dan Breznitz notes, even experts are not quite sure what we mean when we talk about data or about the best way to regulate it (Breznitz 2021).

For non-experts, these issues can be difficult to navigate, as we saw during the unfolding of the Toronto debate over Quayside. Through much of the two-year public consultation and planning phase, Waterfront Toronto and Sidewalk Labs faced questions from activists about the surveillance that would be needed to make the smart city technologies work, who would own and control the data and who would benefit from the IP relating to the technologies created. These critics understood that the world had changed, and that data collection and ownership, and knowledge commodification had become, in many ways, more important than the things – such as automated garbage disposal – that they enable. Sidewalk Labs was largely tight-lipped on how data would be collected, stored, used and governed. For its part Waterfront Toronto had been unprepared for the vociferous data- and IP-focused negative reaction, with protesters consolidating around the #BlockSidewalk hashtag. According to Kristina Verner, the organization's Vice President Strategic Policy & Innovation, 'I don't think Waterfront Toronto was ready for how fast the tsunami of everything hit us.'[5]

The Quayside project eventually collapsed. Following two years of constant, well-deserved criticisms and no shortage of bureaucratic intrigue,[6] in May 2020, Sidewalk Labs announced it was abandoning the project, citing the uncertainty brought on by the global Covid-19 pandemic. The project's unraveling, and its eventual demise, highlighted the problems that officials, individuals, governments and societies can run into when they fail to appreciate the central role of issues like who controls data, IP rights and surveillance – issues that we refer to in this book as knowledge-governance issues – when they don't understand what it means to live in a knowledge-driven society. Waterfront Toronto's lack of preparedness to deal with knowledge-governance issues was understandable. Waterfront Toronto officials were experts (and well-regarded ones) in land development, not esoteric issues like IP and data governance. Nor are they alone in failing to recognize how important these subjects have become or how their particular area of expertise was being transformed by the introduction of data and IP issues. As we

discuss in chapter 3, although IP rights have been an integral part of the international trade regime for three decades (joined recently by data and internet governance issues), they continue to be treated as secondary issues to more traditional trade issues by the people who negotiate these agreements.

This book is for those in the 'everyone else' camp, the non-experts for whom data and IP are subjects that can no longer be ignored. Living in a knowledge-driven society means that our lives, livelihoods and politics are increasingly affected by these previously esoteric issues. We need to understand the logic of the knowledge-driven society: how it works, what it requires to function and the policy challenges it presents. To that end, we have attempted to make these issues as approachable as possible in order to welcome more people into this crucial policy debate.

A KNOWLEDGE GOVERNANCE–FOCUSED THEORY OF INTERNATIONAL POLITICAL ECONOMY

Based within the field of IPE, this book proposes a framework for understanding the knowledge-driven society, as well as a guide to the resulting changes.

As the discipline focused most directly on questions of power as they relate to the global intersection of politics and economics, IPE has much to offer the study of the knowledge-driven society. To date, however, the most advanced research and theorizing about these changes have come from elsewhere. In communication studies, Manuel Castells's foundational trilogy on the information age (1996, 1997 and 2009) identifies several key aspects of the knowledge-driven society, arguing that its networked nature is its defining characteristic. Communication scholar Dan Schiller in 1999 presciently argued that digital technology was embedded within deeper structures of capitalism, creating what he termed 'digital capitalism' (Schiller 1999).[7] More recently, and also from communication studies, Shawn Powers and Michael Jablonski's masterful *The Real Cyber War* (2015) offers a convincing account of the politically contested relationships between the US state and US tech companies – what they refer to as the 'information-industrial complex'.

In the regulatory studies field, Peter Drahos coined the phrase 'information feudalism' to refer to the spread of strong IP rights – a phrase that holds particular resonance in our study, as will become clear (Drahos 1995; Drahos and Braithwaite 2002). More recently, scholars have argued that we are seeing the emergence of new forms of capitalism, such as 'data capitalism' (West 2019), 'platform capitalism' (Srnicek 2017; see also Jin 2015; and van Dijck et al. 2018) or 'surveillance capitalism' (Foster and McChesney 2014; popularized by Zuboff 2019). Along narrower, but no less important

lines, economist Joseph Stiglitz received the 2001 Nobel Prize in Economics for his work on information asymmetry, which provides us with a solid and critical foundation for understanding the economics of data and IP (e.g., Dosi and Stiglitz 2014; Baker et al. 2017).

Meanwhile, scholars in the field of critical data studies are engaged in invaluable research into understanding the conceptual shifts that underlie a data-driven economy, as well as their socioeconomic consequences (Gitelman 2013; Kitchin 2014a; boyd and Crawford 2012; Crawford et al. 2014; Hintz et al. 2018; Dencik et al. 2016; Taylor 2017b).[8] In the business studies field, Zuboff has emerged as a leading polemicist, arguing that the age of 'surveillance capitalism' is a 'terra incognita' for which we will need completely new maps and understandings of the world (Zuboff 2019, 17). This assertion is somewhat overstated, as many elements of our current terrain have been well mapped by contemporary communication scholars, critical data theorists, those working in the Science and Technology Studies field, among others, as discussed in Haggart (2019a).

An International Political Economy Framework

While IPE as a field is underrepresented in this discussion, it offers several tools to place such issues in their proper political-economic context. One of the marks of a good theory is its ability to account for events and outcomes that lie beyond its initial application. To this end, we adapt and combine the thinking of three IPE scholars – Susan Strange, Robert W. Cox and Karl Polanyi – whose work, while not developed either for or in the context of the rise of digital communications technologies or the knowledge-driven society, speaks directly to our current moment. Using their work as our foundation, we develop not a theory of the knowledge-driven society but rather a theory of the global political economy that includes, as a primary component, the control over knowledge.

This book examines the nature of the knowledge-driven society. We are interested in how the increasing emphasis on the control of knowledge as a key power vector is shaping society, economically, politically and creatively. Our interest is not, if you'll pardon the phrase, merely academic. We examine the ways in which these changes create winners and losers, and why some individuals, groups and policies thrive in this changing society, while others will not. To borrow Susan Strange's well-known research question, *Cui bono?*, we want to know who benefits and who doesn't from this move to a knowledge-driven society. Most importantly, we consider the fundamental issue of how best to respond to these changes so as to encourage widely shared prosperity and human development without compromising fundamental human and democratic rights.

Our argument is as follows. We are witnessing the emergence of a new type of society, the *knowledge-driven society*. In such a society, the control over knowledge represents a primary vector for the exercise of power, by both state and non-state actors. This shift to a knowledge-driven society brings new actors to the fore, with different conceptions of the public good and new ways of achieving political and economic prominence. Different types of societies give rise to different types of what we, following Cox (1987), call state-society complexes: the mix of state and non-state actors that is able to exert the structural power to set the rules and norms under which other actors operate. For example, all societies have security forces. However, a society in which security actors are dominant will function differently – will follow different logics, pursue different priorities – than one in which, say, financial, production or (in the current moment) knowledge are seen as more important (Strange 1994). The upshot of this insight is that understanding a knowledge-driven society requires understanding this type of society's internal logic and how this logic shapes society as a whole.

For reasons that we discuss in chapter 2, we refer to the state-society complex characteristic of a knowledge-driven society as an *information-imperium state*: the mix of dominant state and non-state actors capable of exerting structural power over the definition, creation, dissemination and use of knowledge in its myriad forms.

Crucially, the ideologies, values and preferences of these new, knowledge-based actors, while always subject to contestation, become dominant throughout society. As such organizations become more important, the gulf between knowledge (data-, IP- and internet-based) and 'traditional' companies disappears (think about the sensor-manufacturing company mentioned earlier). Knowledge-governance questions move to the centre of the agendas of businesses and governments alike, particularly the question of who should control knowledge and to what ends this control should be put.

This contest over the control of socially valuable knowledge defines the knowledge-driven society. It pits those who already possess socially valuable knowledge against those who desire access to or control over this knowledge. As the management of knowledge becomes increasingly central to social, political and economic organization, states and non-state actors will compete and cooperate to regulate, formally and informally, knowledge in its myriad forms. This type of economy and society will privilege knowledge-based economic models and public policies over others. In doing so, it will necessarily challenge conventional economic wisdom around liberalized cross-border economic exchanges and minimalist government intervention in the economy.

One of the characteristics of a knowledge-driven economy is greater state intervention in the economy than we witnessed under the market-friendly

neoliberalism that had been in vogue since the early 1980s. The two main economic strategies of the information-imperium state are *knowledge feudalism* and *digital economic nationalism*.[9] Knowledge feudalism supports strong global IP rights and free cross-border data flows. It is the preferred strategy of those who already possess economically valuable knowledge. In contrast, those countries that do not possess such knowledge (which is required to reap the economic advantages of the knowledge-driven economy) tend to practise digital economic nationalism, prioritizing domestic development and greater national (though not necessarily state) control over knowledge resources. While this division seems to mirror the long-standing free trade-protectionism debate, we argue in chapter 2 that knowledge feudalism and digital economic nationalism embody a different economic logic and that knowledge feudalism's effects are precisely the opposite of the win-win scenario on offer in traditional liberal trade theory.

Ideology, Not Technology

Equally important alongside the issue of control is that of belief. The primary characteristic of our knowledge-driven society is ideological, not technological. This society is driven not by new digital technologies but by a belief in data as a higher form of knowledge and in commodified knowledge as the foundation for economic success.

This ideology, which media studies scholar José van Dijck (2014) calls 'dataism', is pervasive. It is held not just by data companies like Google or governments that engage in the algorithmic provision of services. The ideology of dataism is suffused throughout society. For example, communication scholar Lina Dencik and colleagues highlight the degree to which social activist groups are implicated in the knowledge-driven society. Such groups not only organize using social media. They also have embraced the 'datafication'[10] of 'social relations in order to collect data and extend networks of connections, both for organization and mobilization of activities', for example, by quantifying supporters' approval for their campaigns (Dencik et al. 2019, 176).

Understanding Knowledge, and a Third Alternative

Understanding the internal logic of the knowledge-driven society requires understanding *what* knowledge is and how it 'works'. In particular, it requires understanding data (when seen through a dataist lens [van Dijck 2014]) and IP as what the mid-twentieth-century political economist Karl Polanyi called 'fictitious commodities'. Fictitious commodities are things (like human labour or nature) that, while not created as commodities, are treated as such in

the marketplace. Treating them as commodities effectively turns a bedrock of existence into a commercial asset to be bought, sold and hoarded in ways that harm the individual (or nature) that is treated as a commodity and the society that practices this commodification (Polanyi 2001).

Understanding knowledge as a fictitious commodity – that is, recognizing that knowledge is important in and of itself and cannot be reduced to something to be bought and sold – opens up a set of policy alternatives beyond knowledge feudalism and digital economic nationalism. Both of these strategies share an implicit commitment to the commodification of knowledge. As such, they both share complicity in the fact that many, if not most, of the harms from the knowledge-driven society that we identify in this book are a consequence of this reduction of knowledge to a commodity and the consequent forgetting that knowledge always serves some other purpose.[11] Just as limiting the extreme exploitation of human labour requires limits to how companies can treat people as mere economic inputs, such as minimum wages and maximum hours worked, addressing the particular policy challenges of the (commodified) knowledge-driven society requires *limiting* the commodification and instrumentalization of knowledge. We refer to this approach as *decommodification*. A decommodification approach to knowledge governance holds that knowledge should be regulated primarily to ensure that it is used in socially beneficial ways that reflect the human rights of the individuals and communities in which they are developed, not as economic commodities to be bought and sold, their uses divorced from the contexts within which they were obtained or created.[12]

On the 'Knowledge-Driven Society'

Before we continue, a word on our terminology. There exist many terms for the knowledge society phenomena we discuss in this book: *the information age*, *the information society*, *the innovation economy*, *the digital age*, *the knowledge economy* and the *datafied economy*. None of these terms, however, fully capture the extent of the 'what' that we identify here, which reaches beyond the economy into areas of national security and social control. Similarly, 'information' as a term has a relatively neutral connotation that, at least on the surface, tends to play down the extent to which the form of society that we identify is driven by the manipulation of information into knowledge. We elaborate on this point in chapter 1.

Nor does 'digital' exactly capture what we wish to talk about. Much of what we describe in this book is intimately tied to the diffusion of digital technologies. However, the rising dominance of knowledge as a vector of power was driven not by tech companies but by the US pharmaceutical and other IP companies in the 1980s, a point we will explore further in chapter

2. Focusing on the digital aspects of the knowledge-driven society, in fact, downplays the extent to which our current society is driven not by technological change but by a changed attitude towards the role of knowledge in society, which we discuss in chapter 5. It is an attitude that increasingly accepts knowledge, be it IP or data, as a commodity to be controlled and traded. This attitude emerges not from the spread of digital technologies but from the ever-expanding capitalist underpinnings of modern Western society, as we will discuss in the next chapter.

The concept of 'surveillance capitalism' as the preferred descriptor for our current political-economic moment has gained mainstream acceptance in the media, amongst policymakers and in some scholarly corners; however, this book does not employ the term. Originally coined by the Marxist scholars John Bellamy Foster and Robert W. McChesney (Foster and McChesney 2014; Morozov 2019), the term was popularized by business professor Shoshana Zuboff in her 2019 book *The Age of Surveillance Capitalism*. We reject Zuboff's underlying premise that 'surveillance capitalism' represents a fundamental break from capitalism that could lead us all to a 'seventh extinction' (Zuboff 2019, 516).

Far from being a corruption of capitalism, the commodification of intangible goods like digital data and the drive towards the proprietary control over the collection, use and assetization of data (Birch and Muniesa 2020) is pretty much business-as-usual for market-based societies (Jessop 2007; Morozov 2019; Polanyi 2001). Communication scholar Dal Yong Jin (2015), for example, situates data commodification within a wider system of economic and cultural imperialism he terms 'monopoly capitalism', in which, far from the current moment being characterized by the decline of the state, the state remains a central actor.

'Surveillance capitalism' as a concept obscures the fact that the defining characteristic of our moment is not surveillance but the commodification of knowledge as intangible goods or assets (West 2019). Surveillance is a means to this end. As we argue in chapters 1 and 4, this surveillance, far from being either an authoritarian corruption of liberal democracy or a perversion of capitalism (Zuboff 2019),[13] is inherent to a knowledge-driven society, particularly one built on the commodification of knowledge. It is the quest for commodified knowledge in the form of data that causes, say, a company like Google or a liberal-democratic government to embrace pervasive surveillance, with the objective of 'collecting it all'.

In contrast, a term like 'data capitalism' (West 2019) explicitly recognizes that it is not the fact of surveillance that matters but *what*, *how* and *why* specific data are collected. It recognizes that data is not neutral. It also recognizes that the quest for ever-more data touches on non-personal data as well as the personal data. The surveillance and capture of such data present their

own issues that need to be addressed. As we discuss in chapter 7, data-driven surveillance of agricultural production processes is reshaping the exercise of effective ownership rights, shifting the balance of power between farmers and farm equipment manufacturers.

'Data capitalism' as a concept allows us to investigate questions regarding whether specific practices and uses improve or exacerbate existing inequalities in terms of race, gender, class, nationality, sexuality and disability (Milner and Traub 2021; Alexander 2020; Benjamin 2019; Browne 2015). However, while we draw on the data capitalism literature, we go beyond it to focus on the control of knowledge in general, particularly via IP rights.

This book also sets aside some of the less-precise terminology that often gets deployed in discussions of the data- and knowledge-driven economy. The 'platform economy', or 'platform capitalism' (Srnicek 2017), has also emerged as a popular frame for discussing data governance. Definitions of platforms typically emphasize their facilitation or organization of interactions amongst producers, suppliers, advertisers and users (see, e.g., Srnicek 2017; van Dijck et al. 2018). In practice, however, its meaning is often in the eye of the beholder. As media scholar and principal researcher for Microsoft Tarleton Gillespie notes, 'platform' is an ambiguous term that is 'specific enough to mean something, and vague enough to work across multiple venues for multiple audiences' (Gillespie 2010, 349). Perhaps its most important function is to allow such companies to shape the regulatory environment in which the company operates to 'strike a regulatory sweet spot between legislative protections that benefit them and obligations that do not' (Gillespie 2010, 348). Data-driven companies have invested significant time and resources into creating a narrative around the term 'platform' that portrays their business models and practices as beneficial, commonly in terms of facilitating free speech and peerless innovation and offering an 'egalitarian and populist appeal to ordinary users and grassroots creativity' (Gillespie 2010, 358). In doing so, they downplay the inherent tensions between 'user-generated and commercially-produced content, between cultivating community and serving up advertising, between intervening in the delivery of content and remaining neutral' (Gillespie 2010, 348).

Efforts to position data-driven companies as intrinsically different from their analog antecedents because of their application of data-collecting technologies can be understood as appeals to technological exceptionalism, to a belief that technology-facilitated, data-driven companies should neither be legally defined as, or subject to, the same regulatory requirements as their analog competitors. Nor should they be legally considered as having employer responsibilities to their workers including minimum-wage protection, be they ride-hailing firms (the taxi industry) or commercial accommodation companies (the hotel industry).

In this book, we set aside such rhetorical positioning. Our focus is on data, IP and the broader move to capture and control knowledge, particularly intangible knowledge in the form of digital data and IP.[14]

The term 'knowledge-driven society' – which, given the dominance of economic imperatives in this area, we use somewhat interchangeably with 'knowledge-driven economy' – is intended to capture the wide-reaching effects of a society that has decided to concentrate on the control of knowledge as a primary vector for the expression of economic and political power. It describes a society with a particular approach to these abstract 'things': where once data and IP were inputs into production processes, now they are or are seen to be central to this power. This focus on both the political and economic aspects of knowledge control extends it beyond economist Ugo Pagano's concept of 'intellectual monopoly capitalism', for which we have a great deal of sympathy (Pagano 2014; see also Durand and Milberg 2020). Talking in terms of a 'knowledge-driven society' also allows us to discuss national security issues, most notably the desire of the state to give in to its already-existing impulse to measure everything (Scott 1998) by surveilling everyone, on a scale not previously undertaken by liberal democracies. Most importantly, it highlights the central importance, and political contestability, of the construction of the rules governing the legitimation, creation, dissemination and use of knowledge, by both state and non-state actors: rules that create winners and losers.

BIGGER THAN TECH

The knowledge-driven society, characterized by the embrace of dataism and commodified knowledge, is a pervasive phenomenon. What we describe in the following pages is a society that has embraced an ideal, one that is no longer confined to the tech sector, if it even makes sense to speak of a 'tech sector' in a world in which digital technology is ubiquitous.

After Sidewalk Labs left Toronto in May 2020, Waterfront Toronto shifted its plans for Quayside dramatically, unveiling plans for '800 affordable apartments, a two-acre forest, a rooftop farm, a new arts venue focused on indigenous culture, and a pledge to be zero-carbon' (Jacobs 2022). An article in the *MIT Technology Review* argued that this newly proposed development 'is a conspicuous disavowal not only of the 2017 proposal but of the smart city concept itself' (Jacobs 2022).

Despite this high-profile failure, celebrations of the death of the smart city – or at least, the ideologies and processes that undergird the smart city – are premature. On 8 July 2022, only nine days after that *MIT Technology Review* article was published, a coding error in a network upgrade by Canada's largest

telecommunications company, Rogers, effectively took large swaths of the entire country offline for an entire day (Posadzki 2022). This outage not only affected internet access for customers' home, mobile and smart devices but also crashed much of the country's online payment system, making it almost impossible for many people to use credit cards or ATMs. It kept many people from accessing emergency 911 services. Perhaps most absurdly, it also led to the cancellation of local Toronto hero The Weeknd's homecoming concert, in part because nobody could open the (networked) doors to the stadium – Rogers Centre – where he had been scheduled to perform (Wheeler 2022).

It's not hard to imagine a similar mistake shutting down all of Quayside had Waterfront Toronto and Sidewalk Labs realized their dreams. If nothing else, this outage, which affected a significant proportion of a highly industrialized country's economy and communications network, demonstrated the extent of our dependence on and faith in internet-connected digital technologies and the data they produce. The societal shift to a knowledge-driven economy, driven by always-on connectivity, the commodification of knowledge in the form of IP and the belief that the marshalling of ever-more digital data will usher in a better society, is bigger than the smart city. It is bigger than Google or the tech sector. Despite Sidewalk Labs' Toronto failure, and notwithstanding Waterfront Toronto's new direction, the rising importance of control over knowledge will continue to present significant and ongoing public-policy challenges affecting everything from agriculture and global manufacturing processes to democratic accountability itself. In the following pages, we attempt to unpack the nature and consequences of these challenges.

BOOK PLAN

This book is divided into three parts. Part I presents our theoretical framework. Our first step is to define the key term in our study, 'knowledge'. Discussions of what knowledge is tend to extend into metaphysical realms where non-philosophers fear to tread. However, since we've built a 'knowledge-based society' or an 'information economy', we should have some idea about what these terms actually mean. In chapter 1, we present our contribution to the discussion, in the form of eight principles for understanding what knowledge is and how it 'works' in a knowledge-driven society. We also introduce the first of our three key theorists, Karl Polanyi, and his concept of 'fictitious commodities' to describe the commodification of knowledge.

Chapter 2 presents the book's theoretical and analytical framework and introduces our two other main thinkers, Susan Strange and Robert W. Cox. Based on this framework, it identifies the three key events that have shaped

our currently existing knowledge-driven society. It also presents the two primary policy questions that shape a knowledge-driven society. Finally, this chapter introduces the two key policy paradigms – digital economic nationalism and knowledge feudalism – that largely define the parameters of policy debates in the knowledge-driven society, along with an alternative path, that of decommodification, a term we develop here.

In part II, we examine the knowledge-driven society through the lens of our framework. Each chapter focuses on a key aspect of global knowledge governance and how it is reshaping global society.

Chapter 3 addresses the role of IP rights in shaping the knowledge-driven society. As the primary legal way in which knowledge is commodified, IP rights are important both in and of themselves and as the policy area that served as a precursor to the emergence of dataism as a dominant ideology. As we argue, although IP rights provide the underpinning of the knowledge-driven society, and although their embrace is transforming the nature of economic development, they continue to be treated as a second-order policy area.

After chapter 3, the book's focus switches primarily to data. Chapter 4 sets the stage for this discussion by highlighting data's eight primary characteristics (and one inconvenient truth). These characteristics shape data's effects on the economy and society.

Chapter 5 tackles the ideological dimension of the move to a knowledge-driven society and the consequent emergence both of new forms of legitimate knowledge and a subtle but significant shift in the people and organizations that societies trust as legitimate experts. This chapter explores the strange phenomenon of the emergence of tech companies as 'experts' in everything from health to urban development to finance (fintech), even when they lack a substantive background in these areas. This redefinition of expertise and embrace of data and dataism (van Dijck 2014) as the pinnacle of human knowledge affects everything from who is able to exercise economic and political power to the distribution of economic rewards and what types of knowledge and cultural creation are privileged.

The next four chapters (6–9) explore the role of state and non-state (mainly industry) actors in regulating the knowledge-driven economy, while also highlighting several key governance issues.

Chapter 6 describes how the data economy functions through an exploration of the private, corporate side of the knowledge-driven society, specifically the emergence of private actors as consequential regulators through their control over data and data governance. It examines in particular two expressions of companies' structural power through data: by using automated data analytics to forecast future events and behaviour and, second, through data-driven standard setting with a focus on technology companies' expansion into the health sector.

Chapter 7 considers how the knowledge-driven society is affecting basic notions of property, ownership and control. It does so through an examination of the expanding IoT universe: networked devices for which ultimate control rests with the vendor, who can modify or even determine the product's lifespan at will.

Where chapter 6 explored the question of industry and knowledge governance, chapter 8 turns our attention to the state's interest in governing through data and algorithms in the quixotic pursuit of precisely quantified human behaviour and predictive regulation. It explores the development of the data-focused state, characterized by the 'information-industrial complex' (Powers and Jablonski 2015) that emphasizes the mutual dependence between surveillance-based companies and the state's interest in expanding its surveillance capabilities, particularly in relation to national security but also related to the provision and denial of public services through big-data-fuelled algorithms.

In chapter 9, we build on the preceding chapters to consider how data is and should be governed. We pay particular attention to modes of data governance that look beyond the individualistic approach to data rights. These include notions of group privacy, as well as the concept of data justice, that challenge the instrumental, economical treatment of data that an individual-rights approach to data governance tends to reinforce.

Finally, in the conclusion, we consider what our journey through the knowledge-driven society teaches us about how to respond to the challenges it presents and offer policy recommendations. Following Karl Polanyi's assessment of the harms that emerge when we treat fictitious commodities like knowledge and data as if they were actual commodities, we argue for the need to limit the commodification of knowledge if we want to harness data's potential and avoid locking up knowledge behind a wall of IP rights that benefit only its owners and not society as a whole. Just as the emergence of a knowledge-driven society was historically contingent and the result of human decisions, so, too, is its future path.

NOTES

1. While Mytelka uses this phrase in the context of intellectual property rights, the insight behind it applies to knowledge governance generally.
2. For an account of the Quayside project's tumultuous history, see O'Kane (2022).
3. We discuss IP and global value chains in chapter 3.
4. We discuss government use of algorithms in chapter 8.
5. Interview, Kristina Verner, 23 February 2022. Via Microsoft Teams.

6. Some of the project's problems were rooted in perennial questions about procurement processes and the appropriate relationship between state and non-state actors, including concerns that Waterfront Toronto had become engaged in a too-close relationship with Sidewalk Labs (Roth 2018). A year after the 2017 town hall, the auditor general of Ontario would allege that Sidewalk Labs had received preferential treatment during the bidding process, among other questionable practices (Auditor General of Ontario 2018).

7. We do not adopt 'digital capitalism' to describe what we are examining because, contra Schiller, we argue that the defining aspect of our current moment is the rising importance of the control of knowledge as a vector of power, not of digital technology per se. Digital technology has shaped, and been shaped by it, but as we argue in chapter 3, the main processes we identify predate the mainstreaming of the internet.

8. Other key sources addressing these issues include the following. On legal studies of intellectual property rights, see Perzanowski and Schultz (2016) and Horten (2016); on control of intellectual property, see Drahos and Braithwaite (2002). From Science and Technology Studies and internet governance, see DeNardis (2014). Within the field of International Relations (IR), Carr (2016; 2015) is one of the few texts on internet governance from an IR perspective. From Surveillance Studies, see Lyon (2015), Ball and Snider (2013) and the work published in the *Journal of Surveillance Studies* in general. This list is illustrative, rather than exhaustive. Breznitz (2021) stands out in its focus on both data and IP and their effect on economic innovation.

9. A note on terminology: To avoid confusion, when we refer to 'the state' on its own in this book, we are using it according to its traditional meaning. We use 'information-imperium state' exclusively to refer to the set of state and non-state actors capable of exercising consequential structural power through the knowledge structure, as defined explicitly in chapter 2.

10. That is, the reduction of social relations to a few measurable data points. For a fuller discussion, see chapters 4 and 5.

11. We elaborate on this point in chapter 2.

12. While governments, particularly the European Union, have sought to place limits on the collection and use of data on human rights grounds, as Daly (2021) argues, and as we discuss in chapter 9, these interventions are as much about constructing a market in data as protecting human rights.

13. For a critique of Zuboff's position that surveillance capitalism is a perversion of capitalism, see Morozov (2019).

14. This focus on data and the control of knowledge as the defining feature of these companies is in keeping with Srnicek (2017), who identifies data collection as the main objective of the platform business model. In chapter 6, which discusses the platform business model, we adopt Srnicek's data-focused approach to platforms.

Part I

UNDERSTANDING THE KNOWLEDGE-DRIVEN SOCIETY

Chapter 1

Defining Knowledge

The Eight Principles

The centrality of the control of knowledge – particularly commodified knowledge – to the exercise of economic, social and political power is the defining characteristic of the knowledge-driven society and the information-imperium state. Consider, as we did briefly in the introduction to the book, the case of data-collecting sensors on tractors, a topic we will revisit in chapter 7. In a world built around manufacturing, it is the sensor that has economic value: a company would be content to make their profits from the sale of the physical thing. Now, it almost goes without saying, companies are interested in the data – the knowledge – collected by the sensor as a commodity that can be bought and sold: the sensors are reduced to the thing needed to collect economically valuable data. The extent to which we take for granted the right of the sensor manufacturer to control and profit off the data produced by the sensor is the distance between then and now.

For a concept around which we have built an entire economy, what different authors mean by 'knowledge' (or 'data', for that matter) can sometimes be quite ambiguous. The situation isn't helped by the fact people often mean different things when they talk about 'knowledge' and 'information'. Colloquially, the terms are often used interchangeably. In the academic literature, scholars have their own precise, albeit contested, definitions. For someone looking for a foothold in this discussion, it doesn't help that the discussion about what constitutes knowledge is itself mixed up in foundational and insoluble questions about whether and how we can truly 'know' the world, conversations that tend to occur within esoteric and dense philosophy texts, and in graduate-level social sciences and humanities programmes.

In this book, we are concerned with understanding how the foregrounding of the control of knowledge has affected the global political economy. This is not a philosophical treatise on the nature of knowledge. Still, if we're

going to talk about knowledge and the knowledge-driven society, we need to identify the particular characteristics of what is being commodified and controlled. In other words, we need to get a bit metaphysical. Just as a monetary economist needs to understand how money functions in order to understand the dynamics of a monetized economy, those wishing to understand how a knowledge-driven society functions needs to understand how the element at its heart – knowledge – actually works.

In this chapter, we present a set of eight principles, a simplified engagement with the concept of knowledge. These stylized facts are designed to highlight, from a political economy perspective, the most important aspects of what knowledge is and how it functions. These principles highlight the extent to which the control and regulation of knowledge is a fundamentally political exercise that creates winners and losers. It is not a neutral process. What's more, the regulation of knowledge reflects the nature of the society in which the regulation takes place. Currently, the dominance of market forces is reflected in the marketization of knowledge or what Karl Polanyi calls the creation of 'fictitious commodities' (Polanyi 2001). This commodification of knowledge comes at the expense of its more important social roles, be they cultural, social or scientific. This tension between knowledge's economic and non-economic roles underlies most, if not all, of the policy challenges we discuss in this book.

Our starting point is our engagement with theories of social construction,[1] explained next and drawing in particular on sociologists Peter L. Berger and Thomas Luckmann's foundational 1966 work *The Social Construction of Reality* (Berger and Luckmann 1966).[2] We also introduce the first of our three main theorists, Karl Polanyi, and his concept of fictitious commodities, which we apply to knowledge.

Our purpose is to provide readers, analysts and policymakers with a useable starting point for thinking about knowledge governance, an introduction for non-experts that highlights the distinctive issues presented by a knowledge-driven society. We are very conscious that those in other disciplines, such as our philosophy-of-knowledge colleagues, have their own particular lexicon and sets of concerns and that they will almost certainly be driven to distraction by some of what we present here, such as our distinction, made in the next section, between 'knowledge' and 'information'.

Still, one has to start somewhere, and social constructivism starts from the premise that the world we experience is shaped by our shared assumptions about the world. Our main argument is that 'knowledge' is not a neutral category: the creation, dissemination and use of knowledge are all highly political acts that create winners and losers. This fact makes the control of knowledge itself political: it matters who regulates knowledge and to what ends.

THE EIGHT PRINCIPLES

Principle 1: 'Knowledge' and 'information' are two different things.

We start with what seems at first to be a paradox. By now, the phrase, 'Government policy should be data-driven' has become little more than a reflex, an empty set of words used by politicians and pundits to demonstrate their commitment to dispassionate, sound policymaking. The phrase itself implies that if policymakers could just set aside their human biases and focus on the real world, they would be able to identify the best possible policy in any situation and just get to it. This is the Silicon Valley view of the world: you can solve any problem if you can just collect enough data.[3]

And yet, as political scientist Virginia Eubanks thoroughly details in her book *Automating Inequality* (2018), and as we will discuss throughout the book, there exists example after example of governments and companies whose supposedly neutral datasets and algorithms repeatedly discriminate against particular groups, usually women and racialized people. For example, in 2015 Amazon – one of the world's leading data companies – found that its hiring algorithm downranked women's applications. The company realized that this was because the dataset it had used to train the algorithm had a disproportionate number of applications from men. Amazon eventually shut the programme down because even after correcting for this form of discrimination, there 'was no guarantee that the machines would not devise other ways of sorting candidates that could prove discriminatory' (Dastin 2018). Such stories are, unfortunately, commonplace.

If the bias and discrimination problems identified by Eubanks were the result of poorly programmed algorithms or flawed datasets, they could be corrected relatively easily without thinking through more existential, foundational problems. Would that it were so simple. This isn't a problem that can be solved with more or better data: it's inherent in the nature of knowledge itself and (here's where things get metaphysical) its connection with reality.

The question of how we know what is in the world has bedevilled philosophers for centuries (Jackson 2016). It involves questions about the 'hook-up', as IR scholar Patrick Thaddeus Jackson (2016) calls it between our minds and the external world. We need not concern ourselves with these issues here, not least because they are likely insoluble (Jackson 2016; Strange 1994, 136). Although here we adopt one particular approach to thinking about these issues, the fact that this uncertainty about something as basic as how we know the world is pervasive should give pause to those who would accept data as an unproblematic representation of the world.

Social constructivism holds that what we experience as reality is always mediated or interpreted (Berger and Luckmann 1966). What's more, we are

only ever able to partially interpret this reality. The most obvious way we interpret reality is through our five senses, but as quantum physicists constantly remind us, our senses (and our measurement apparatuses) are only capable of apprehending a slice of this underlying reality. When physicists talk about there being more than four dimensions, this is part of what they're trying to get across: the reality separate from our senses is vaster and weirder than we can possibly imagine or fully measure.

Not only do we exist in a complex reality that we are incapable of fully interpreting due to our limited senses, but we also have to decide which parts of the reality that we can apprehend are the most important and relevant for us to focus upon. Deciding what's most important requires assigning objects and actions particular meanings so that we can distinguish between what is important/relevant and unimportant/irrelevant and focus the majority of our attention on the most important parts of reality.

Importantly, these interpretations can never capture fully the entirety of the thing under consideration. Think about yourself and the different ways that others can identify you: gender, age, height, education, skin colour, hair colour. The list of identifiable characteristics that can be used to describe you is almost endless. And while any particular descriptor may accurately capture a dimension of who you are, it would be impossible to sum up the entirety of who you are in these descriptors. Instead, we use a selection of these elements as shorthand to describe a person, chosen depending on the perceived needs of the circumstances in which we find ourselves.

Or consider the case of a song, itself a form of knowledge. There are many elements that go into a song: the beat, the melody, even something ineffable as the feel, to say nothing of the personal touch the individual performers can give a song. However, we've decided that some parts of a song are more important than others. Historically, only the melody, not the beat, has been protected by copyright law, a partial consequence of the fact that at the time that copyright developed in Europe, the melody was seen as the most important part of a song (Byrne 2012). While copyright regulates music, it doesn't fully capture every aspect of what constitutes a song.

This chain of reasoning – we can never fully describe reality, and we also have to interpret (i.e., make choices about how to understand and represent) this reality – gets us to our understanding of knowledge and the distinction we draw between knowledge and what we refer to in this book as information. In this book we use *information* to refer to the phenomena – to the reality – that exist whether or not someone observes it, independent of our understanding of it. Following this definition, *knowledge* refers to the interpretation of this reality. The act of deciding to observe something, and then observing it, transforms information into knowledge. Put another way, knowledge involves giving social meaning to phenomena. And because we can never fully know

this underlying reality, our knowledge of the world is always and necessarily partial. What's more, our interpretation of our partial understanding of the world is itself filtered through our existing understandings of the world.

Focusing on the role of interpretation in constructing our understanding of the world is particularly useful to help clarify the nature of data. For example, International Political Economy (IPE) scholar Christopher May sees information as equivalent to data: information is 'data, characterized as a passive resource which can be packaged and transferred in discrete units'. Knowledge, meanwhile, is 'the theoretical or intellectual tools that are needed to produce further (knowledge-related) resources from this raw information' (May 2010, 6). Information in May's account is synonymous with data and is treated as a neutral building block to create knowledge.

In contrast, we see data as a form of knowledge rather than the building blocks of knowledge because defining what matters as data is itself an interpretive act. Our information-knowledge distinction draws not only on Berger and Luckmann's point about the social construction of reality but more directly from critical data scholars' fundamental insight that data is never neutral. Data 'does not just exist – it has to be generated' (Manovich 2001, 224). Equating information with data fundamentally overlooks this central point.

Creating data involves a decision to measure a part of reality and to interpret it in a particular, and necessarily incomplete, manner. There cannot be raw data 'because what is "given" must first be configured for "capture"' (Couldry and Mejias 2018, 8). To collect data, one must first decide what phenomena should 'count' as data. In other words, data 'do not exist independently of the ideas, instruments, practices, contexts, and knowledges used to generate, process and analyse them' (Kitchin 2014a, 3). 'Data inherently reflect choices – choices about which data to collect (or to exclude) and what tools or parameters will be used in their collection. . . . These choices reflect the human agency present in the creation of data' (Scassa 2018a, 3; Kitchin 2014a). We discuss the nature of data as a social construct further in chapter 4.

Our use of the term 'knowledge' as meaning the interpretation of an underlying reality and 'information' as synonymous with an underlying reality that cannot be fully captured by human observation or interpretation is designed to highlight how, when it comes to interpretations of the world, it really is (partial) knowledge, all the way down. Knowledge, as we use the term here, isn't just the complex assembly of information or collated data that provides us with a higher-level understanding of something. The knowledge-information distinction we are drawing here highlights the role of human decisions at every step in the knowledge-production process. From this perspective, technology is a form of knowledge since it is the embodiment of ideas of

how to manipulate our physical and social realities, as is intellectual property (IP), which structures things like sounds and the collection of symbols into discrete, identifiable (intangible) entities. As forms of knowledge, moreover, they are necessarily only ever partial, only one possible way of apprehending reality rather than being a neutral representation of this underlying reality.

Another example to illustrate even more concretely the difference between information and knowledge: consider your heartbeat. The human heart beats whether or not we are paying attention to it. That is information, the underlying reality. Now, we can also decide to measure the rate at which it pumps blood, which we define as a heartbeat. The measurement of the heartbeat gives us a piece of data, a partial representation of an underlying phenomenon, the functioning of a human heart. In other words, knowledge.

Principle 2: There are always rules and norms governing knowledge.

This tendency to think of data as a neutral representation of reality is partly the consequence of a lack of analytical clarity about the relationship between information-as-phenomena and knowledge as the human act of interpreting phenomena. This proclivity, moreover, is often mirrored in our approach to IP rights.[4]

Understanding this point requires thinking about the role that rules play in creating knowledge. Legal and economic accounts of IP rights tend to start from the assumption that knowledge (in the colloquial sense) is what economists call non-rivalrous and non-excludable. What that means is that knowledge, in its natural state, cannot be kept from being shared (non-excludable) and can be enjoyed or used by others without exhausting the original supply. For example, if I sing a song (a form of knowledge in that it is a collection of sounds arranged in a particular way and recognized as a tune), this doesn't affect others' ability to sing the song (non-rivalrous). Nor does someone else singing it reduce or consume that song so that it is unavailable to others (non-excludable).

IP laws, from this perspective, set unnatural restrictions on who is allowed to sing and share this song. These restrictions transform the song into something both rivalrous and excludable.

We will discuss these issues with respect to IP in greater detail in chapter 3, but the immediate relevant point is that line of thought – captured by the polemical slogan 'Information wants to be free' – treats the regulation of knowledge (such as through IP rights) as a trade-off between freedom and control. If we could just get rid of these rules, then people would more easily be able to share knowledge, and culture and humanity would flourish.

This approach, however, misunderstands the nature of the knowledge-governance trade-off. When we say that knowledge is socially constructed, we

are saying that knowledge itself is constituted by rules. Knowledge is always governed by formal and informal rules and norms that people and societies come up with in order to decide what counts as useful or valuable knowledge and how this knowledge is to be used and by whom. Knowledge does not exist separate from the formal and informal rules and norms that determine what counts as knowledge, including rules governing who can create knowledge and who can distribute and use it. Knowledge in its natural state is not unrestricted by rules; it is defined by them. The creation and use of knowledge are always and everywhere subject to rules, both formal and informal.

The actual trade-off is not between a world in which information (knowledge) is free and one in which it is in chains, or between control and freedom. Rather, it is between different sets of rules and different forms of control. Put most bluntly, there is no such thing as free speech, in the sense of 'speech unconstrained by rules'. Freedom of expression may be more or less widely practised, but even in the absence of formal rules there are unwritten rules and norms that regulate who is effectively allowed to speak, and what they are allowed to say.

At the most trivial level, these rules (such as grammar) render coherent the communication of knowledge. Beyond these, we have informal rules, such as social taboos against the use of profanity or the discussion of politics at family dinners or a stand-up comedian mimicking the feel of another's act.

The most formal rules are those covered by formal laws, such as IP or hate-speech laws, or governmental freedom of information acts. Rules can also be specific to a culture or community, such as those pertaining to traditional Indigenous knowledge that determines who are the custodians of specific cultural knowledge (see Pool 2016). Speech and data use can also be governed by companies' terms of service – for example, Twitter's (unevenly applied) rules against hate speech. Rules and norms may be more or less permissive, as in the case of the US First Amendment (an exceptionally permissive outlier among democratic states [Franks 2019]), but they are always there.

There are always rules governing knowledge, including speech. This insight can help to clarify some of the more contentious debates regarding, for example, the role of governments in regulating social media websites. A free speech–focused site may impose few rules on content and conduct, but the harassment that is effectively permitted by such a set-up also effectively regulates the ability of marginalized individuals and groups to enjoy their formal free-expression rights. Our understanding of knowledge, which starts from the point that there are always rules governing speech, transforms the policy debate over speech regulation. Instead of a false choice between rules and no rules, or (state) regulation or no regulation, we are forced to consider *which rules* we should adopt in order to improve social well-being, with the

debate now focused on the question of how to define 'well-being' (Haggart 2020a; Haggart and Keller 2021).

Humanity has always constructed rules regulating knowledge (and speech); it is through rules that knowledge itself is constituted and created. Now, however, we are at a moment in which we are thinking through what these rules should be, perhaps more consciously and involving more perspectives than had previously been the case. As we discuss in chapter 2, the primary issue in a knowledge-driven society involves deciding how to regulate knowledge. It is crucial that we address these issues with an understanding of what rules govern knowledge and not with the impossible assumption that the goal should be to avoid regulating knowledge altogether.

Principle 3: Knowledge rules will always favour some groups and outcomes over others. Those who control the definition, creation and use of knowledge also control the future direction and development of knowledge.

Knowledge is defined by the rules that constitute it. Because knowledge itself is always and necessarily only a partial apprehension and interpretation of an underlying reality (of information, in other words), these rules are necessarily partial. These rules emerge as a consequence of human action and reflect individual and societal biases. More to the point, rules governing the identification, creation, dissemination and use of knowledge are made by people, who themselves have their own biases, prejudices and partial understandings of knowledge.

In other words, knowledge, and knowledge regulation, is political. Knowledge is always partial, and the rules and norms governing knowledge are socially constructed – that is, they are the product of human actions. As a result, these rules and norms will always create winners and losers, both in terms of groups and in the types of knowledge that are created. All sets of rules, even the most permissive, will favour certain forms of control and thus will favour the creation of certain forms of knowledge, activities and actions over others, and certain groups over others. Knowledge rules, like data itself, are never neutral.

The processes through which these rules (which we define permissively to include formal and informal rules and norms that structure human activity) are determined, what they allow and who they benefit, play a significant role in determining the dominant players – be they state or non-state actors – and the extent to which we end up with a winner-take-all economy. The control of knowledge shapes not only the economic development of society (e.g., by determining what new technologies get produced) but also its

social, cultural and ideological development (e.g., by shaping who gets to tell what stories).

Consider the evolution of hip-hop. Before copyright law caught up to this new art form in the early 1990s, several sample-heavy (i.e., tunes made up of snippets of other songs) classics emerged, including Public Enemy's *It Takes a Nation of Millions to Hold Us Back* (1988), De La Soul's *Three Feet High and Rising* (1989) and the Beastie Boys's *Paul's Boutique* (1989). Subsequent changes in copyright law rendered the use of even very short samples in music prohibitively expensive to say nothing of the complexity of clearing songs that are often controlled by more than one owner. Communication studies scholar Kembrew McLeod and legal scholar Peter DiCola estimate that under these new rules the Beastie Boys would have lost US$4.47 per album sold, or US$19.8 million overall (McLeod and DiCola 2011, 210). MacLeod and others correctly take this as an example of how changes in copyright effectively 'pushes the most complex and musically interesting sample-based works into either the non-commercial sector, the underground economy, or nonexistence' (2011, 188). However, as they also note, these changes did not destroy creativity; rather, they led musicians and artists to change the types of music they created, away from direct sampling to, for example, more live music or samples that are so heavily altered their original source cannot be identified (McLeod and DiCola 2011, 190).

What this means is that while it may now be financially prohibitive to create another *It Takes a Nation of Millions* . . . , the flipside is that the creation of some of the types of music post-copyright changes (say, those based around only one sample, or hip-hop that incorporates more live music) would become relatively more likely. All knowledge rules encourage certain types of knowledge and creative expression and discourage others.

The question we need to ask in this case, then, is not, will these changes reduce creative output? Changes to copyright laws alter the type of knowledge that is created, but they do not eliminate knowledge creation itself. The more appropriate question is, what type of creativity/knowledge creation will these rule changes encourage and discourage, and who will be affected by these changes? This question forces us to make value judgements about what knowledge should be created and in whose interests. In the case of sample-heavy music, the losers are clearly the artists for whom this was their means of expression, as well as those of us who loved this type of music. Furthermore, there is a racial component to these rules: given that the 'practice of appropriation [which includes sampling] is an important aspect of African American music', commodifying and making sampling prohibitively expensive will have a disproportionate effect on African American musicians (McLeod and DiCola 2011, 48, 97, 108). These particular losses may amount to only a small change in the big picture, but in a knowledge-driven economy, the question of what type of

knowledge is created, in whose interests, who is making these decisions and with what effects is not a marginal one of interest only to music fans: it touches on the power dynamics at the very heart of the global political economy.

Principle 4: New knowledge builds on existing knowledge. Control over knowledge is thus a consequential political issue.

The creation of new knowledge invariably builds on existing knowledge, be it a well-footnoted textbook or a patented drug. Knowledge is both its own input and its own output. This reality is built into IP laws. Patents and copyrights are always limited in time and scope because failure to include such safety valves in IP laws would provide those who currently control knowledge with an ever-greater hold over the creation of new knowledge. This reality is both why IP owners are always pushing to restrict or eliminate these limits and why policies such copyright term extensions are so problematic from a public-policy perspective. It's also why data collection is so important to companies: Data produced and captured in a production process can be used to improve these processes (Srnicek 2017). Stronger IP protections and proprietary data are ways in which those who control economically valuable knowledge can further strengthen control over the future creation of knowledge, which is itself, as we've noted, a source of power.

That knowledge is both its own input and output suggests how central issues of control over the creation and use of knowledge are to a knowledge-driven society. While most discussions around IP and data see such control in terms of individual ownership, this proprietary view of knowledge is neither the only nor necessarily the best way for a society to control knowledge. Types of knowledge can be treated as a communal resource subject to no formal controls, as is the case of books that are out of copyright and thus (largely) formally removed from IP law's purview. But it can also be subject to community control, as with some forms of Indigenous, or traditional, knowledge. Moreover, concepts like public data trusts, in which data collected from a citizenry is treated as a communal resource, are garnering increasing interest (Srnicek 2018), as we will explore in chapter 9.

That the current dominant form of control over knowledge is proprietary has given rise to one of the main challenges of the information age: the winner-take-most economy. In such an economy, the actor that controls foundational knowledge can force everyone else to pay up if they want to use that knowledge, or they can exclude others entirely from using it. As we will discuss in chapter 3 with respect to IP, the monopoly rents afforded by strong IP protection have helped to create a hierarchical global economy in which the lion's share of economic benefits flow to a small number of IP-rich

companies and workers, primarily located in the Global North, particularly in the United States (Schwartz 2021).

Proprietary control over data can also allow for the creation of new forms of power. For example, the pharmaceutical/agricultural giant Monsanto/Bayer has an agricultural app for farmers, Climate FieldView, that aggregates data from public sources (like government satellites) together with real-time tractor-gathered data on temperature and soil moisture. The company combines this data to make a proprietary source of knowledge that it then sells to farmers (Carbonell 2016, 5). What was previously considered farmers' traditional knowledge – detailed experiential knowledge of soil fertility, crop yields, and planting timelines – has become proprietary data controlled by commercial interests, while farmers have become, in a sense, 'glorified sharecroppers' on their own farms (Carbonell 2016, 5) or 'bioserfs' (Shand 2002, cited in Carbonell 2016, 5). We will explore these issues in detail in chapters 4 and 7.

The current stock of knowledge is not just used to create more economic knowledge. It can affect the capacity of governments to make policies in the public interest. Legal scholar Teresa Scassa (2017) has studied how Airbnb's claims over the data produced by its users as its own property impair cities' ability to fulfill their traditional zoning and taxation functions to ensure that neighbourhoods have a socially acceptable mix of businesses and/or residences and that everyone pays their legal share. The data on who was running hotels and rooming houses used to be collected by the city. Now, as Airbnb enters a market and this service goes digitally underground (from the city's perspective), more and more of that data is held close by the company, inaccessible to city officials, thereby creating 'data deficits' that harm public planning and regulatory functions (Scassa 2017). Officials are left with the options of losing control over their zoning role and tax base, negotiating with Airbnb for the data or forcing the company to give the data to the city. Control over this (proprietary) data places Airbnb, a company, in a position of authority, allowing it to serve as a de facto regulator over commercial accommodation. We will return to these issues in chapter 8.

Principle 5: Processes of knowledge production are shaped by the society in which they occur.

Knowledge creation results from human action. We must decide what information counts as knowledge and what form that knowledge will take. To use our previous example, we can decide to measure our heartbeat and in doing so produce (partial) knowledge of the human heart. This data doesn't tell us *everything* about the nature of the heart, but it tells us something that we've decided is important to know.

Decisions about what knowledge to create, and what to do with it, are themselves informed by the society within which we live. These decisions are shaped by individual and societal politics, economics, culture, ethics and morality. Knowledge, in the form of data and IP, for example, is created within the context of historically contingent social relations (Couldry and Mejias 2018, 8). As we will cover in chapter 3's discussion of IP rights, processes of capitalism – particularly its inherent tendency towards commodification – have shaped our conceptions of what knowledge is and in whose interests it should function (Couldry and Mejias 2018; Thatcher et al. 2016). That a trade agreement – the 1995 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) – has emerged as the world's most consequential IP treaty cements the treatment of knowledge as an economic, tradable resource. Nor is it mere happenstance that universities around the world are being directed to commodify the knowledge that they produce rather than share it openly, as has been the custom in academia for centuries (Drahos 2021, 59). IP rights are primarily commercial rights, the commodification of knowledge, be it of industrial processes or the collection of tones assembled into a song.

The interpretation of information, the creation of knowledge, is shaped by a society's, and our own individual, values. The same heartbeat that we used to illustrate the difference between knowledge and information can also help us understand how historically contingent social beliefs and processes can influence how knowledge is created and the uses to which it is put. Think of the uses to which the measurement of your heartbeat – a form of knowledge – might be put. A doctor might measure your heartbeat to determine, and improve, your overall health. Or a digital-fitness company might measure your heartbeat, and commodify it, to be sold to an insurance company looking to deny coverage to individuals it deems unhealthy. The commodification of heartbeats is not a dystopian possible future: it's happening right now. Mirroring what companies in South Africa and the United Kingdom are doing, the American insurance company John Hancock announced in September 2018 that it would only sell life insurance to people who agree to have their vital signs tracked by an app (Barlyn 2018).

Principle 6: In a market society, knowledge is a 'fictitious commodity'.

If you want to understand the knowledge-driven society, there are few better starting points than the work of the great mid-twentieth-century political economy scholar Karl Polanyi. In his landmark 1944 book, *The Great Transformation*, he argued that enormous pressures exist in market-based societies, such as the ones that currently dominate the globe, to turn everything into a commodity that can be bought and sold (Polanyi 2001). He argued that if one

allowed the market to expand unchecked throughout society, it would end up destroying that society. In a market economy, commodities are created, bought and sold. However, noted Polanyi, some of the foundational commodities in a market society – land, labour and money – are not actually created or produced. Instead, they are what he called 'fictitious commodities'. As the IPE scholar Bob Jessop remarks, 'what we call labour is simply human activity, whereas land is the natural environment of human beings, and money is just an account of value' (2007, 116).

This creation of fictitious commodities, Polanyi warns us, comes with a cost. If we forget that labour, or human resources, are human beings, we end up valuing people based only on what they can deliver in the marketplace. If we forget that land is the environment that we need to support all life and not just a set of resources to extract, we will end up rendering the planet unliveable. If we forget that money is just a unit of account to keep track of credits and debits across a society, we put ourselves in the position of ruining the lives of people, families and societies who are unable to balance their books. This is the reason we have labour laws mandating eight-hour workdays, anti-pollution laws and bankruptcy courts: to keep the market in its proper place so that it can benefit society, not destroy it.

As Jessop (2007) argues, IP is also a fictitious commodity. Like land/real estate, labour/humans and money/account of value, it is a way to turn thoughts, concepts and cultural products into discrete units for exchange and manipulation. While Jessop's analysis was limited to the forms of knowledge commodified as IP, there is no limit to the types of knowledge that can be turned into commodities. Data is simply the measure of human activity or the natural world that has been captured because of its perceived value (Haggart 2018b). And yet we 'produce' and 'sell' data as if it were an actual commodity. As we write this particular paragraph, in early 2022, the mania for non-fungible tokens (NFTs) is in full swing. NFTs, as communication professor Ian Bogost explains, are best thought of as 'the first step in the securitization of digital assets. They turn data into speculative financial instruments' (Bogost 2022). However, as new and intimidating and confounding as NFTs may appear, they represent the same tendency towards commodification identified by Polanyi almost eighty years ago and that is embedded in our ideas about IP rights. The only difference between IP as a commodity and NFTs as a commodity, or asset, is that knowledge protected by IP is backed by the authority of the state, while NFTs are not.

Whether data, IP or NFTs, these knowledge-regulation processes share similar challenges. Commodifying knowledge, detaching it from the individuals and social contexts that produced it, gives knowledge an instrumental (often for-profit) characteristic, often placing it in a closed economic system and under the control of specific groups or individuals (Jessop 2007), for the

benefits of those who control the knowledge-as-property. In the case of data, commodification and 'knowledge-ification' reconfigures 'the flow of everyday life . . . in a form that enables its capture *as* data' (Couldry and Mejias 2018, 4, emphasis in original) so as to benefit those who extract the data produced by individuals not the ones whose actions produced the data in the first place. Sociologist Nick Couldry and communication studies professor Ulises Mejias refer to this process as 'data colonialism', which entails the transformation of '*human life* into a new abstracted social form that is also ripe for commodification: data' (2018, 4, emphasis in original). And it does so in a way that presents itself as both natural and inevitable, even as it is the product of unequal social relations that benefit some groups over others (Thatcher et al. 2016).

A society that fails to place limits on this commodification of knowledge (as IP or as commodified data) will, Polanyi warns us, incur significant costs. Much of the rest of this book can be read as a warning about the implications of treating knowledge – data produced by observing individuals, social interactions and natural processes, the intellectual activity covered by IP – as commodities rather than as the natural by-products of human activity.

Principle 7: Knowledge is intangible.

One of the challenges of understanding the knowledge-driven society is coming to terms with what makes (commodified) knowledge different from tangible goods. Because IP, for example, creates a form of commodified knowledge that can be bought and sold on the market, IP is often treated as equivalent to physical goods. Chapter 3, for example, details how IP rights have been included in international trade agreements for several decades, with data and internet governance policies more recent additions to the international trade agenda.

While knowledge can be commodified, its lack of materiality means that it functions according to its own particular logic. For example, it is easy, under current laws, for transnational corporations to engage in tax arbitrage by moving the 'value' attributed to knowledge across borders because there is nothing physical to transport. Similarly, the nature of knowledge production means that knowledge-intensive companies involve different types and levels of employment than traditional manufacturing companies and have different spillover effects into the local economy. The foreign branch plants that largely were responsible for creating the modern Canadian economy, for example, generated enormous economic benefits in terms of numerous well-paying manufacturing jobs and the construction of spin-off companies, such as a vibrant auto-parts sector. However, a strategy of attracting knowledge-based branch plants does not bring with it the same economic effects as a traditional manufacturing plant

(Carmichael 2018; McIntyre 2018). Companies like Google employ a fraction of the employees that a firm like General Motors (GM) did at its height, limiting the labour-spillover effects from their economic activity. What's more, what such companies produce – IP and data – is easily transferred out of the country, with relatively little value-added left behind.

Principle 8: A society based on the exploitation of knowledge requires constant surveillance to function properly and efficiently.

For Karl Polanyi, fictitious commodities present a challenge to the survival of society when we forget that these fictitious commodities are actually something else. At the extreme, if you forget that natural resources are the environment that sustains our very existence, you will destroy the biosphere upon which our physical existence depends. Regulations are required to keep these tendencies in check.

The need for surveillance is one of the primary things that makes a market society structured around the control of knowledge such a threat. Traditionally, surveillance meant 'the focused, systematic, and routine attention to personal details for purposes of influence, management, protection or direction', whether undertaken by public actors, private actors or some hybrid arrangement thereof (Lyon 2007, 14). In a knowledge-driven society, however, surveillance has broadened from focused attention on specific individuals and instances to 'always-on, ubiquitous, opportunistic, ever-expanding forms of data capture' – that is, constant, ubiquitous surveillance of all people and objects, by state and non-state actors alike (Andrejevic and Burdon 2015, 19). Data can only be collected via observation, which is to say surveillance, while surveillance is also needed to enforce IP rights (i.e., to see if someone is violating your IP rights).

In a knowledge-driven society, there exist strong and intertwined commercial and security incentives to collect as much data – that is, to engage in as much surveillance – as one possibly can. With respect to business, companies providing traditional services like transportation and lodging have adopted intensive data collection practices in order to deliver those services, such as Uber's real-time monitoring of its drivers' locations and dynamic pricing based on available vehicles and customer demand (see Rosenblat 2018). Surveillance is also integral to the advertising-based business models of Google and Meta, where increasingly the value is in predictive behaviour analysis of its customers' future desires, actions and purchases. Beyond these usual surveillance suspects, IPE scholar Nick Srnicek (2017) points out that 'industrial platforms', such as Rolls-Royce, have retooled their production lines to maximize the data they can extract from them, in order to improve their production efficiency and product quality.

For companies with data-intensive business models reliant upon IP, surveillance is not only a business model (Schneier 2015) but a regulatory mechanism. Not only must data be collected from the environment or user, but the company must also monitor the customer to ensure the protection of the IP. With respect to IP, any unauthorized use of a company's IP implies a potential loss for the IP owner, which explains the enduring interest by copyright and trademark owners in coercing internet intermediaries such as Google to surveil their users for IP infringement (see Tusikov 2016).

We can witness a similar dynamic when it comes to national security. Total societal surveillance used to be associated with the worst totalitarian states. But particularly since the 11 September 2001 terrorist attacks on the United States, we've witnessed a convergence between liberal-democratic states and authoritarian states in terms of the surveillance practices employed to monitor their citizens (see, e.g., Hintz et al. 2018; Lyon 2015; Glasius and Michaelsen 2018). Part of the dynamic driving this push for increased surveillance is political. Democratically elected politicians fear that they would be held responsible for another similar attack, despite little evidence of such programmes' effectiveness in intercepting terrorists (in the US context, see Granick 2017).

In a society that focuses on the control of knowledge (as opposed to manufacturing, for example) for its economic and physical security, anything less than total surveillance will be seen as an economic loss or a potential threat, and not just by a power-hungry state or rapacious corporations, but by citizens themselves. This simple formulation also suggests why it will be very difficult to rein in the excesses of the surveillance economy and the surveillance state: for those who have adopted the mindset of a knowledge-driven society, to do so would be to invite ruin.

It is in this context that the notion of privacy has emerged as a mainstream issue in discussions around the data-driven economy. The evocation of privacy rights – however defined – represents an attempt to place a limit on the surveillance imperative lest it overwhelm the rest of society. It is an attempt to begin a discussion about how to restrict the reach of the knowledge-driven society, recognizing that there are some situations in which surveillance is not appropriate or data collection should not occur. Such a discussion, however, involves pushing back against the powerful economic and security logics of the knowledge-driven society. It requires asserting an alternate societal logic based on human rights and human dignity.

CONCLUSION

In this chapter, we have highlighted how everything to do with knowledge is deeply political, down to the designation of certain data points as

representative of the world in which we live. All forms of knowledge, and all forms of knowledge regulation, are political. Neither data nor IP – indeed, no type of knowledge – is neutral. Decisions about which data to collect to train an algorithm designed to approve or deny refugee claims, about what parts of a song merit protection and which ones don't: these and all decisions related to the creation, dissemination and use of knowledge benefit some individuals, groups and interests over others. Understanding the dynamics of knowledge that we've covered in this chapter is the necessary first step towards being able to assess and address the promises and perils of a knowledge-driven society.

As we will demonstrate in the coming chapters, placing the control of knowledge – in this case, commodified knowledge – at the heart of the economy and society creates particular systemic challenges. These challenges in turn are centred around a specific set of policy questions related to the power to define, create, disseminate and use knowledge, and the contest between state and non-state actors to exert this power.

NOTES

1. In terms of our particular fields, social constructivism has been in the mainstream of International Relations for several decades, Wendt (1999) being a classic departure point. We also draw on the ideational aspects of historical institutionalism (e.g., Thelen [1999] and Campbell [1998]). Within IPE, Innis (1950) is a classic text; see also Jackson (2016). As noted in the introduction to this book, Jessop's concept of 'cultural political economy' has also explored this terrain (see, e.g., Jessop 2007, 2010; Jessop et al. 2012). From a socio-cultural perspective, see Burke (2000). From a sociological perspective, see Giddens (1990), Bourdieu (2013) and Foucault (1980); from the perspective of Science and Technology Studies, see Latour (1988) and Jasanoff (2004). Within the copyright literature, the relationship between regulation and ideas is well covered by Rose (1993), May (2010), Drahos and Braithwaite (2002), among others.

2. In citing Berger and Luckmann, our ambitions are much less grand than those of Nick Couldry and Andreas Hepp, whose excellent book has the goal of 'reoccupying the space associated' with Berger and Luckmann's book in the context of the digital age (Couldry and Hepp 2017). Rather, our goal is to highlight some basic points about the nature of knowledge and socially constructed reality that are necessary to understand how a knowledge-driven society functions.

3. This ideology is known as dataism (van Dijck 2014). We discuss dataism in chapters 4 and 5.

4. On IP rights as a 'reified' construction of reality, see May (2006).

Chapter 2

New Policy Challenges, New Strategies

In this chapter, we set out our concepts and road map for understanding how the knowledge-driven society emerged and the nature and dynamics of our current moment. It is a moment in which the power to control how knowledge is legitimated, created, disseminated and used is becoming a primary 'vector of structural power', in the evocative words of the late International Development scholar Lynn Mytelka (2000, 42). These changes have had the effect of rewiring society and reworking how power is exercised, by whom, and for what purposes. In particular, we introduce three main concepts – structural power, the knowledge structure and the information-imperium state – that we believe are crucial to understanding how power is exerted in a knowledge-driven society.

We situate our work within the field of International Political Economy (IPE). IPE's remit – understanding macro-level changes in global politics and economics – makes it ideally suited to consider issues related to global transformations, including whose interests are served by these transformations. Chapter 1 highlighted Karl Polanyi's concept of fictitious commodities and applied it to knowledge. Here we draw on the work of our two other main theorists. We use Susan Strange's theory of structural power – the ability to set the conditions under which others operate – as it plays out in four key sectors – security, production, finance and knowledge – to explain how our knowledge-driven society came into being and its implications. Other scholars, such as sociologist Michael Mann (Mann 1984, 1986), have put forward similar typologies.[1] We chose to use a modified version of Strange's structural power because its key categories, particularly her division of economic power into finance and production, are better suited than Mann's to understanding changes in the political economy, for reasons that should become obvious shortly.[2]

We also draw on the work of the late Canadian IPE scholar Robert W. Cox, particularly his work on the close relationships between state and non-state (read: business) actors, which he calls *forms of state*, or state-society complexes, and how dominant economic and political actors can shape the overall political climate and transform the policy agenda to suit their interests and needs. In the knowledge-driven society, we call the dominant form of state the *information-imperium* state. It is characterized by a focus on the control over knowledge as a primary economic and social policy objective. Taken together, these two theorists help us understand how the control of knowledge moved to the top of the policy agenda and what this means for policymakers and publics going forward.

THE CHAPTER IN BRIEF

As academics, we believe it's important to explain the theories behind our work: that is the purpose of this chapter. For those readers more interested in the data and intellectual property (IP)-governance issues that we explore in subsequent chapters, our argument in this chapter is as follows.

Understanding politics and power in the global political economy requires focusing on structural power, that is, the ability to set the conditions under which others operate. The exercise of structural power, in turn, is necessary to determine an authoritative set of values for a society, that is, to shape the nature of the society. In this contest to shape societies, four key sources of structural power stand out in terms of their importance: security, production, finance and knowledge. No one of the four is *a priori* more important than the others, but when one form of power dominates, actors based in that structure are able to set overall social, political and economic priorities in their own image and to influence others' beliefs about how society should be organized.

Our current moment is characterized by the rising importance of the knowledge structure. Power in the knowledge structure involves power over the legitimation, creation, dissemination and use of knowledge, including IP and data. With the increased importance accorded to the control of knowledge has come a new state-society complex, which we will define more completely later in the chapter. This state-society complex brings together state and non-state actors with common interests in regulating knowledge, particularly as it relates to data and IP, and the extent of state (security) and non-state (commercial) surveillance. We call this state-society set-up an information-imperium state because of the priority it accords to knowledge-control and surveillance issues.

In such a state, actors become increasingly reliant on the control of data and surveillance for the provision of security and (alongside IP rights) for their commercial activities. These changes have significant implications for

how we define both security and economic prosperity, issues that we will unpack throughout the rest of this book.

Finally, the emergence of the information-imperium state signals a refocusing of our primary economic policy questions and ideological fault lines, from a focus on free trade versus protectionism to digital economic nationalism versus knowledge feudalism. While these two approaches represent different and conflicting economic strategies, they also share an understanding of knowledge primarily as a fictitious commodity. In contrast, a third approach, knowledge decommodification, rejects the intertwined economic logic of the first two approaches in favour of placing limits on knowledge commodification so as to tame the harms that arise from the unfettered knowledge-driven society.

The remainder of the chapter is structured as follows. The first section explains what we mean by structural power. The second section outlines the four structures, paying particular attention to the knowledge structure, which is the book's main focus. The third section uses Cox's forms-of-state framework to trace the emergence of our current information-imperium form of state from its roots in the 1970s US embrace of strong IP rights in its trade agenda. The fourth section describes the politics of the information-imperium state and the key questions it must address. We end the chapter by setting the stage for the rest of the book.

THINKING CLEARLY ABOUT POWER

'Power', like 'knowledge', is one of those words that everyone uses but that is surprisingly difficult to define precisely. The common-sense understanding of power involves the ability to compel someone to do something they wouldn't otherwise do. This type of power, which Susan Strange referred to as 'relational power', is often apprehended by looking at an actor's material capacities, such as the size of a country's economy or military. It is on display most clearly in violent situations, such as when one country conquers another or someone robs a bank at gunpoint.

In this book, we are interested less in expressions of relational power, such as Google's market capitalization or the annual number of patents China produces. Instead, we focus on structural power, the power to set the conditions – the rules and norms – in which others operate. As Strange puts it:

> 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)

The ability to influence rules and norms confers an enormous advantage on the rule-setter. If an actor is able to set the rules and norms in ways that favour their strengths, minimize their weaknesses and reflect their values, they're already half-way to securing their preferred outcomes.

Who Can Exert Structural Power?

While we tend to think of states as the ultimate rule-setters, Strange noted that non-state actors are also capable of being consequential regulators. Ongoing critiques of Facebook/Meta and other tech companies with a global reach, for instance, of being the 'sovereigns of cyberspace' (MacKinnon 2013, xxvi), reflect this insight. On the opposite side of the ledger, digital rights groups like the American, libertarian-leaning Electronic Frontier Foundation tended historically to focus their fire on states rather than companies in large part because they did not appreciate that companies could be consequential regulators (Glaser 2018).

The emergence of corporations as rule-setting actors is not a new development. Nor is it a consequence of a global internet. Companies have been key international players and rule-setters for decades. The internationalization and globalization of the economy itself were shaped by US multinational corporations, dating to the 1950s. The modern field of IPE was founded in the early 1970s partly in response to the observation that corporations have become increasingly consequential rule-setters throughout the global economy (Cooper 1980; Strange 1970).

Both state and non-state actors are capable of exerting structural power. Companies are important but states – particularly large states – continue to matter. The exercise of structural power involves a contest between and among states and non-state actors. It involves conflict and cooperation, as different actors work alternately together and against each other to promote their particular interests.

LOCATING STRUCTURAL POWER: THE FOUR STRUCTURES

Every generation of scholars faces the temptation to believe that their moment is unique. The technological changes that we've witnessed since the 1980s have made us particularly susceptible to this urge. For example, Shoshana Zuboff in her *The Age of Surveillance Capitalism*, which has become the bible of our current moment, claims that she is mapping a 'terra incognita' (Zuboff 2019, 17). In describing what she calls the coming 'seventh extinction' (2019, 518), the word 'unprecedented' appears 114 times, or once every 4.6 pages of text. In such an unprecedented context, it makes sense that she concludes the book with a nebulous call for new social movements rather than with specific policy reforms.

This emphasis on novelty, however, ignores important and decisive continuities with previous eras. Such continuities are important because they suggest that we already have the tools to understand and address our current moment.

Take the 'datafication' of the economy. Businesses throughout the economy are retooling themselves to maximize data commodification and capture (Srnicek 2017; van Dijck 2014). We will discuss datafication further in chapters 4 and 5. As political scientist Dan Breznitz notes, there is little consensus on how data should be regulated (Breznitz 2021). However, that is not to say that we do not understand anything about the phenomenon of datafication.

We can start with the fact that this is far from the first time that one sector has reshaped how the entire economy and society functions. The 1980s witnessed the emergence of the 'financialization' of the economy. In a financialized economy, 'all elements of the economy, companies and workers included, should be viewed, managed and valued as financial assets' (Breznitz 2021, 163). This approach reprioritizes a firm's economic goals from maximizing profits to maximizing shareholder value (Breznitz 2021, 163). Financial actors such as bankers, financiers, investors, rating agencies, securities commissions and finance ministers are the primary economic and policy players, and economic and policy decisions are seen primarily through the lens of financial markets.

The case of General Motors (GM) exemplifies how financialization works. Throughout the beginning of the twenty-first century, GM – the very symbol of a manufacturing powerhouse – derived a substantial proportion of its profits from its financing arms, which cover not only car financing but also mortgage lending, insurance, banking and commercial finance. According to sociologist Donald Tomaskovic-Devey (2011), 66 percent of its profits came from its financing wing in 2004. Although ostensibly a vehicle company that provides some financing, GM had become, in a sense, a finance company that also makes cars.

Or think about how, during the Second World War, private-sector production was driven almost exclusively by the imperative to prosecute a war. Or how, following the Second World War, countries worked to promote manufacturing, as captured by the slogan, 'What's good for General Motors is good for America'. In each period, a particular segment of society emerged as a primary force shaping the overall society. In a knowledge-driven society, firms are evaluated by their ability to produce and control data, IP and knowledge generally.

All societies, Strange noted, must fulfil four basic needs. They must provide members with wealth – the ability to satisfy material wants and needs. They must provide security for the person and the group. They must also

provide a degree of individual freedom to pursue individual desires. Finally, they must also provide justice or equity – that is, the sense that group members are treated fairly. Societies and actors differ in how they rank these values and in the degree of emphasis they give to each (Strange 1994, 17–18). Unsurprisingly, how to rank and implement these values is the primary source of political conflict.

The exercise of structural power is the means by which actors seek to implement their preferred value rankings. Structural power exists throughout society but some forms are more consequential than others: the International Olympic Committee (a non-state organization), for example, exerts enormous structural power over international sport, but unless you're an athlete or run a city bidding on the Olympic Games, they can be ignored most of the time. Strange identified four primary sources of structural power in society. Production power involves the power to create and allocate material goods. Financial power is the power to supply or deny credit and to structure monetary relations. Security power involves the power to create or deny physical security, against human and natural threats. Finally, knowledge power involves the power to control the legitimation, creation and dissemination of knowledge deemed to be socially important (Strange 1994, 26–30).

Different theoretical approaches rank the importance of each of these structures differently. Marxists, for example, argue that it is the production and class relations that matter most, production being the motor that drives history. Within the field of International Relations, realists would counter that the power to create or deny security is paramount: without security, one cannot even have a society.

In contrast, Strange argues that these four sources of power are all interdependent: national security, for example, requires access to intelligence sources (knowledge). It depends on a strong manufacturing base, which must be paid for somehow. We can run the same argument in any direction among the structures. And while she grants that in the ultimate instance a bullet will put an end to any conversation, in practice most human interactions don't descend to this primal level. Consequently, the relative importance of these four structures – that is, which structure's logic will become most important – is not predetermined. It is historically contingent, the result of political contestation, among other things. This contingency means that the key structure in a society – the main players and prevailing ideologies – can and will change over time (see May 1996, 178; see also Cox 1996a). Today, financial industries may be the most significant players; tomorrow, it could be the military or the tech sector.

Rise of the Knowledge Structure

The financialization of an economy or society is characterized by the relative importance placed on financial actors and objectives. Similarly, the 'knowledge-ification' of society, the emergence of a knowledge-driven society is distinguished not by the presence of digital technologies and IP rights but by the *relative* importance accorded to the control of knowledge as an economic commodity and as a form of social control.

Let's return to GM. Patents and research and development have always played a role in its business activities. Now, however, the control of knowledge in the form of data is becoming an end in itself, rather than a means to the end of producing more vehicles. This move is part of a larger trend identified by IPE scholar Nick Srnicek (2017) of companies retooling their business models to maximize the capture of data, now prized not only as a means to improve the production process but also as a commodity itself.

For example, in 2016, GM partnered with the ride-hailing company Lyft as part of a move to help develop self-driving vehicles, a technology where the revenues would come as much (if not more) from the sale of data- and algorithm-based 'self-driving' services to consumers as of vehicles themselves (O'Brien 2018). Although the two companies are no longer as tightly related as they were initially (Wayland 2017), GM continues to harbour ambitions in this area, competing against Google subsidiary Waymo 'to be first to bring fully autonomous cars to market' (LaReau 2018). Elsewhere, GM and other manufacturing companies are realizing that the data produced by their products can itself be a valuable resource (Srnicek 2017). For three months in 2017, GM monitored the radio-listening habits (including where and when people listen to the radio) of about 90,000 drivers in Los Angeles and Chicago (customers give GM the right to monitor them when they accept the terms of service and privacy statement associated with GM's connected services, a practice we will discuss in much greater depth in chapter 7). Talking with the *Detroit Free Press*, Saejin Park, GM's director of global digital transformation said, 'We sampled (the behaviour) every minute just because we could' (LaReau 2018). Such data represents a potentially new revenue stream for GM, as the data could be sold to advertisers, or to turn GM cars into a platform with captive drivers and passengers that GM could deliver to anyone wishing to pay to reach them: Facebook on wheels.

Unpacking the Knowledge Structure

The knowledge structure comprises the rules and norms governing 'what knowledge is discovered, how it is stored, and who communicates it by what means to

whom and on what terms' (Strange 1994, 121). These rules and norms regulate knowledge and involve both formal and informal rules governing the creation, dissemination and use of knowledge. Examples of this form of structural power include censorship and IP laws, telecommunications regulations, data governance rules, the structure of networks like the internet and the norms governing epistemic communities. Many other examples could be added to this list.

Just as a financial company like Goldman Sachs can be said to be based on the financial structure, certain actors can be said to be based on the knowledge structure. These are individuals and organizations

> 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. (Strange 1994, 121)

In our contemporary society, these actors include data-collection and data-processing companies, telecommunications companies, content creators, universities, epistemic communities, governmental statistical agencies and state intelligence agencies, among others. For example, although their influence and interests pervade the economy, companies like Google and Amazon are situated primarily within the knowledge structure.

As Strange's definition suggests, power in the knowledge structure is qualitatively different from power derived from the other structures. In one sense, power in the knowledge structure can resemble power in the other three structures: the power to set rules controlling access to a necessary societal resource – security, material goods, finance and knowledge (e.g., culture or education). This is the 'knowledge-regulation' part of the knowledge structure.

However, what differentiates power in the knowledge structure from other forms of structural power is that it also includes the power to decide what is deemed to be what Strange called the '"right", desirable knowledge' – that is, the power to determine what counts as legitimate knowledge and what doesn't, which experts are worth listening to and which can be safely ignored and even what is considered to be truth itself (May 1996, 185).[3] We refer to this as knowledge-legitimation power. In chapter 5, for example, we argue that the most significant effects of the digital age have been the emergence of commodified knowledge in the form of IP and data as the most important form of legitimate knowledge and the redefinition of expertise to favour those who control such knowledge.

Rising Importance of the Knowledge Structure

Evidence that the power exerted through the knowledge structure is reshaping society is plentiful. We have already offered the example of GM. We can

also point to the explosion in the quantity of cross-border data flows, which according to the consulting firm McKinsey & Company grew 45 times larger between 2005 and 2016 (McKinsey Global Institute 2016, vi). According to a 2019 Organization for Economic Cooperation and Development report, the explosion in data transfers 'translates into an estimated contribution of US$2.8 trillion to global economic activity, or 3.5 percent of global GDP' (Casalini and López González 2019, 9).

Nick Srnicek's succinct but invaluable book *Platform Capitalism* offers a clear and concise account of how 'digital technology is becoming systematically important, much in the same way as finance', and how it is becoming 'an increasingly pervasive infrastructure for the contemporary economy' whose collapse would be economically devastating (2017, 5). Digital economic development is quickly becoming synonymous with economic development, as economies rework themselves on the high-tech model:

> The digital economy is becoming a hegemonic model: cities are to become smart, businesses must be disruptive, workers are to become flexible, and governments must be lean and intelligent. In this environment those who work hard can take advantage of the changes and win out. Or so we are told. (Srnicek 2017, 5)

In the new, knowledge-driven economy, 'data have become increasingly central to firms and their relations with workers, customers, and other capitalists' (Srnicek 2017, 6). Capturing data and exploiting IP becomes the path to success, not just for companies like Google, but old-economy companies like GM and Siemens. These companies not only are figuring out ways to extract data from their customers, they are also being forced to capture all relevant production data in order to improve efficiency in a marketplace where their competitors are doing the same thing (Srnicek 2017). These findings are what one would expect in a political economy in which the knowledge structure had become ascendant.

While the current knowledge structure is characterized by a strong emphasis on the capitalist commodification of knowledge, it is not reducible merely to an economic logic, nor does it only have economic effects. As we detail in chapter 8, the drive to quantify and surveil that is characteristic of the current manifestation of the knowledge structure is also present in a state logic that has driven even liberal-democratic states to embrace total surveillance of their citizenries in the name of security. This surveillance, while it uses the same technologies as commercial surveillance, is driven by a separate imperative, namely the physical security of the citizenry and protection of the state against perceived threats. In terms of non-economic effects, the drive towards total surveillance is also reflected in the embrace of devices for the voluntary quantification of the body in the belief that measuring the number of steps

one takes, or one's breathing during sleep, or the number of people who read a tweet is providing them with a new and valuable (meaningful, legitimate) form of knowledge about their bodies, health and social interactions (e.g., Lupton 2018; van Dijck and Poell 2016). The key point here is that the knowledge structure should be analysed on its own terms, and when it is a dominant structure, we need to pay special attention to its particular logic.

EMERGENCE OF THE INFORMATION-IMPERIUM STATE

Susan Strange's language of structural power allows us to understand what has been commonly observed – the rise to global prominence of technology-and-IP-based companies – as the rise of the knowledge structure. More importantly, she allows us to understand the significance of this change: a change in the relative importance of a structure implies not only a new set of actors at the top of the political and economic hill but also a change in political and economic priorities to reflect the ideologies and interests of these newly powerful actors. A world in which Google is the paradigmatic company and everyone looks to data scientists for insights functions differently from one in which GM is the top dog.

However, while Strange can tell us that the primacy of the military, or manufacturing, or finance, or tech companies is historically contingent, we have to look elsewhere to understand *how* this switch between structures happens. For these insights, we turn to Canadian IPE scholar Robert W. Cox for inspiration.[4] One of Cox's key insights is that these large changes in the relative importance of these structures – from, say, security, to production, to finance, to knowledge – affects and is affected by states as much as non-state actors. The relative rise and fall of structures changes both the goals pursued by states and how they pursue them (Cox 1987, 1996a).

It's not just the economy that changes if tech or financial companies increase in relative importance; it's the state itself and the goals it pursues. The state, far from being a monolith, is actually composed of different parts that are not always pushing in the same direction. A government's environmental ministry, for example, may pursue different policies than its natural resources ministry. Along the same lines, a government whose environmental ministry commands significant influence will act quite differently from one that tends to listen mainly to the economists in its natural resources ministry.

Just as the state isn't a monolith, neither is a country's business sector. Every business may be out to make money, but *how* it creates those profits will depend on the nature of its industry and its choice of business model. These choices and twists of fate, in turn, will shape the type of policies for

which different companies and industries will advocate. And in pursuing their preferred policies, they will tend to gravitate towards those parts of the state that share their interests and engage in a degree of cooperation to realize their objectives.

State-Society Complexes and Forms of State

The political picture this account paints is much more complicated than a simple business-versus-the-state contest for structural power. States (as a whole and its various parts) both compete and cooperate for influence with non-state actors. However, when it comes to the overall orientation of the state – in this case embracing protectionism or trade liberalization – some non-state and state actors are more powerful than others. Even in the United States, usually seen as the most free-market-oriented of the major economies, Powers and Jablonski (2015) identify what they call the 'information-industrial complex', a mutually reinforcing network of connections between industry and government, forged by government investments in tech companies and billion-dollar contracts and reinforced by state dependence on private-sector technology. This phrase, itself a play on the famous 'military-industrial complex' term, is what Cox would call a 'state-society complex', a particular self-reinforcing set of state and non-state actors that work together (not in all things, but overall) towards a shared set of objectives.

Cox calls this overall orientation of a particular state-society complex a *form of state*. These forms of state, or state-society complexes, include both state and non-state actors because, as Cox and Strange recognized, structural power does not just rest with the state. A company can also set rules and norms under which we live.

A form of state in a society in which the financial structure has pre-eminence (a financialized state) implies a different set of primary actors and priorities than a situation in which the production structure is relatively more important. This form of state will give pride of place to this form of structural power, drawing 'resources from the society and us[ing] these resources to maintain and reproduce the society' (Cox 1987, 106), for example, by pursuing policies and institutions that maintain the advantages of this part of society. These can include reinforcing the economic advantage of specific forms of production or privileging security forces over other actors, as might happen to maintain a police state. If successful, the state-society complex can become hegemonic, naturalizing its position and making it harder for subordinate parts of state and society to assert their interests.

Even when a form of state is hegemonic, political contestation is always possible. Subordinate actors or groups in the state and society have an interest

in challenging the status quo and will do so using those material resources, ideological arguments and institutional frameworks (which themselves can also be changed) at their disposal. Most basically, Cox notes that societal change can be driven by shifts in material capabilities, ideas about how society should be organized and the institutions undergirding society (Cox 1987).

Changes in forms of states imply changes in a society's objectives and preferred policies. A financialized state-society complex, for example, privileges financial actors and well-being over manufacturing interests and cross-border capital and investment flows over domestic capital controls. Following the same logic, a state-society complex that emphasizes the control of knowledge as a primary objective privileges state and non-state actors that control the creation, distribution and use of socially valuable knowledge. Reflecting the importance of knowledge control to the exercise of power, we refer to this state-society complex (i.e., the combination of actors capable of exercising structural power in the knowledge structure) as the *information-imperium state*: information for the role that such actors play in translating raw information into knowledge and imperium to capture the extent to which control over knowledge is itself a form of dominance.[5]

Origins of the Information-Imperium State

New forms of state do not emerge from nowhere. Nor are they an inevitable outcome of capitalism or great-power politics. Instead, they emerge from political contestation, political battles amongst competing interests. The emergence of a form of state is a historical process. A world in which control over IP and data and the attendant ubiquitous surveillance are seen as vectors of power does not just happen according to the laws of history or capitalism. Rather, it was the result of a chain of events and ongoing political contest for economic and political dominance in domestic and global society.

With respect to the emergence of the information-imperium state, which reflects a society characterized by its emphasis on commodified knowledge and surveillance, three events, in particular, stand out:

- the US embrace in the 1970s and 1980s of strong IP rights as central to its economic development (see Sell 2003) and, eventually, its national security (Halbert 2016);
- the commercialization of the internet in the 1990s; and
- the US government's national-security-driven embrace of total surveillance in response to the terrorist attacks of 11 September 2001.

These three events give the information-imperium state its defining characteristics. At the same time, as we will see, its form was also shaped by its

interactions with the other structures, particularly the finance structure, which has assumed a new prominence in global politics since the 1980s, when financial interests and constraints, and financial actors and institutions became much more influential in shaping outcomes in the global political economy.

That all three events directly involve the United States is not an accident. As the dominant Western, and then global, state of the second half of the twentieth century, the United States has used its hegemonic position to exert an outsized influence on world affairs, shaping both the material and ideological development of the knowledge-driven society. For the same reasons, it is the leading information-imperium state, and while not all countries can emulate it, all are forced to react to it.

Commodification of Knowledge: Strong Intellectual Property Rights Go Mainstream

Many, if not most, accounts of the Information Age see the creation of the internet (with some focusing on its popularization and commercialization in the 1990s) as the catalytic moment. While undoubtedly an important contributor to our story, our current moment is not just about how a certain technology changed the world. More recent accounts focus on the emergence of 'big data' as ushering in a new moment in capitalism or civilization (Srnicek 2017; West 2019; Jin 2015; see also Mayer-Schönenberger and Cukier 2013; Crawford et al. 2014; Lyon 2015). While the changes discussed by scholars of big data are certainly relevant to the creation of our current moment, in a sense it simply represents the culmination of changing dominant attitudes towards knowledge itself.[6] This attitude emphasizes the importance of *control over* and *commodification* of knowledge, most obviously in the forms of IP rights and data (be it proprietary or open source). This corporate view of knowledge stands in contrast to the principles of access and sharing of knowledge championed, for example, by universities and centuries of scholars.

The United States' decision to place IP rights at the heart of its international trade agenda is ground zero for the information-imperium state. As regulatory scholars Peter Drahos and John Braithwaite (2002) and IPE scholar Susan K. Sell (2003), among others, document comprehensively, this decision, beginning in the 1970s and gaining unstoppable momentum in the 1980s, was based largely on lobbying by industries like the pharmaceutical industry, whose business model was based on the strong protection of IP rights. US policymakers, concerned about the prospect of losing international economic hegemony to the so-called 'Asian Tigers' (such as Japan, South Korea and Taiwan), agreed and used the carrot of access to the US market (and the stick of limiting said access) to convince other countries to change their IP laws. Their strategy reached its peak in 1995 with the Agreement on Trade-Related

Aspects of Intellectual Property Rights (TRIPS). The signing of TRIPS and its strong global IP protections was one of the United States' main conditions for agreeing to the creation of the World Trade Organization (WTO) (Sell 2003, 37; Drahos and Braithwaite 2002, 11; Thumm 2000, 63–64).

TRIPS's significance comes from the fact that it instituted a global floor on IP rights that, unlike other IP treaties, was enforceable (through the WTO's dispute settlement mechanism) and that commits all countries to following the same IP rules (with some limited exceptions). Although it contains exceptions for health and developing economies, for example, TRIPS solidified the idea that knowledge should be seen primarily as a commodity.

Commercialization: The Internet Goes Corporate

The history and significance of the internet to the creation of a global knowledge society have been so widely covered[7] that we need not devote much space to describe how this decentralized network, originating as a US military project to create a communication system that could survive a nuclear war, has become a global, ubiquitous, essential decentralized communication network. The politically, economically and socially disruptive nature of this new technology is similarly well-examined (see, e.g., Castells 2009, 2015; Fuchs 2008, 20, 2016). While its decentralized networked nature is undoubtedly important, the decision in the 1990s by the United States to develop the internet on a commercial model, moving it away from what had previously been largely an academic non-profit network looms particularly large in shaping the internet as we know it today (Schiller 1999). While many thinkers predicted (or hoped) that the internet would create a 'New Economy', information and communication historian Dan Schiller argued (correctly) in his 1999 book *Digital Capitalism* that the internet would instead be shaped by these commercial forces (Schiller 2015, 1999). The decision to commercialize the internet provided the preconditions for business to assume an outsized influence as participants in the information-imperium state-society complex.

Taken together with the increasing commodification of abstract works through IP rights, the commercialization of the internet provided the conditions for a globally dominant form of market-based dissemination of knowledge, which would become hegemonic (see particularly Horten 2016). It also led to the eventual ascendance of companies like Google and Facebook, which have assumed responsibility for knowledge-structure activities that previously had been associated with the public sector and the domain of private life: the organization of information (previously the primary domain of libraries) in Google's case and individuals' conversations in the case of Facebook. As a consequence of the migration online of a significant amount of our social lives and of the dominance of for-profit

platforms of these online spaces, these companies have been granted enormous power to police dialogue, legitimizing certain ideas and censoring others (Gillespie 2018; Noble 2018; Vaidhyanathan 2018). This power is reflected in the ongoing debates over what rules platforms like Facebook and TikTok should adopt to police users' activities.

Pervasive Surveillance: 9/11 and the Rise of the Ubiquitous Commercial Surveillance

Pervasive surveillance of online activity by commercial and state authorities is fast becoming an unavoidable fact of life, even in liberal democracies that historically have regarded such surveillance with suspicion. Urban centres, for example, are increasingly places where people's activities and movements are monitored and commodified. With the rise of smart farming, the 'surveillant farm' (Klauser 2018, 370) is similarly a site reliant upon the mass accumulation and transfer of data, typically to large agricultural interests like John Deere and Monsanto/Bayer (see Carbonell 2016). As well, while people have tracked their bodily details for centuries through scales and diaries (see Crawford et al. 2015), the contemporary age is marked by ordinary people tracking and quantifying their bodies and social interactions through social media platforms, wearables and a wide range of health/fitness apps (see, e.g., Lupton 2016; van Dijck et al. 2018).

Surveillance is a necessary, inescapable part of a knowledge-driven society. It is necessary in order to enforce the integrity of the knowledge in question, whether it involves IP rights, the proper use of Indigenous traditional knowledge, or (in a previous knowledge-driven age) the enforcement of rules against blasphemy. More fundamentally, data and observation are inseparable: you cannot collect data without surveilling your world.

Surveillance by US intelligence agencies has a long history, stretching back to the Black Chamber programme in the 1920s that was the precursor to the US National Intelligence Agency (see McCoy 2009) and the mass wartime collection of telegraphic data in and out of the United States in the 1940s (see, e.g., Bamford 1982; Harris 2015). An intensification and dramatic expansion of the US national security apparatus that solidified the persistent state and commercial surveillance way of life emerged in the American reaction to the 11 September 2001 terrorist attacks. Without the embrace of persistent surveillance as the US government's primary response to the 9/11 attacks, we would likely not have seen the emergence of this particular mutant strain of information capitalism, as it violated previously strongly held norms against such surveillance in liberal democracies (Zuboff 2019). In the panicked atmosphere of a hastily declared Global War on Terror, however, such norms were significantly diluted, although staunch criticism of US surveillance programmes

continues to this day. The norm weakened, ubiquitous surveillance was soon adopted commercially, first by Google, and eventually became the internet's dominant business model (Zuboff 2019).

However, just because some surveillance is necessary in a knowledge-driven society does not mean that pervasive, ubiquitous commercial and state surveillance is the only option available to governments wishing to deal with social problems. Limits, both formal and informal, can be placed on the amount and scope of surveillance that we are willing to accept as part of our social bargain. After all, just because we live in a market society based on wage labour doesn't prevent us from limiting the extent to which labour can be commodified. Time off from work is mandatory; minimum wages exist. When data is commodified, it, like labour, becomes a fictitious commodity to use Karl Polanyi's term. The limits we place on labour, or the limits placed on surveillance – themselves de facto limits on the commodification of knowledge – are a recognition of the need to protect the fundamental integrity of the thing in question from the dangers of excessive commodification. They recognize that some human rights, such as the right to privacy or to culture, should trump commercial rights and that surveillance – specifically, the over-commodification of knowledge – can damage the individuals and society being surveilled. Surveillance can be constrained. The state, for example, could break up monopolistic platforms, institute new laws to thwart advertising-based business models or, more boldly, designate certain critical platforms as publicly owned utilities, thus reducing their incentive to surveil (see, e.g., Rahman 2018; Srnicek 2017).

Other events also played important roles in shaping the information-imperium state. For example, the 2008 Global Financial Crisis and the resultant search for high returns to capital helped push the knowledge-driven economy into overdrive. Enormous amounts of money sloshing around the globe seeking decent returns have flowed into tech companies in search of monopoly returns (Srnicek 2017). Tech companies have also taken full advantage of lax global tax regimes and the intangibility of IP to shift intangible knowledge assets to low-tax jurisdictions, a clear example of how history – in this case, the history of the financialized economy – has influenced the knowledge-driven society (Bryan et al. 2017).

In all cases, it was people, in response to events and in pursuit of their own interests, who drove forward events, not the impersonal hand of history or economics. Many of the resulting actions responded to market and capitalist imperatives: US fears of economic decline, pharmaceutical companies' desire to strengthen their patents, the tech sector's desire to profit from the construction and use of the emerging 'Information Superhighway', as well as Google's 'googlization of everything' (Vaidhyanathan 2012). The internet's emergence, however, was not just an economic phenomenon: security

imperatives drove its construction and proved an essential backstop after the dot-com bubble burst in 2000 (Powers and Jablonski 2015), while fears of terrorism created the opening for ubiquitous state and commercial surveillance. The links between military and commercial interests run both ways (Harris 2015; Powers and Jablonski 2015). A full accounting of the functioning of the knowledge structure and the information-imperium state must address both its economic and non-economic aspects.

UNDERSTANDING THE INFORMATION-IMPERIUM STATE

When the knowledge structure rises in importance, questions surrounding the regulation of knowledge, by definition, become much more important than they were previously. Companies that were previously blissfully ignorant of IP and data find that they not only have to learn about them but that they also must change how they operate to incorporate their particular logics.

New powerful players who can harness the power of knowledge emerge with a transformative influence that extends over the economy and society. For example, a new player in the data economy is the so-called 'voice intelligence industry', composed of smart-speaker makers like Amazon (Alexa) and Apple (Siri), marketers and call centre companies. As communication scholar Joseph Turow (2021) notes, the voice intelligence industry was built to collect data on people's speech patterns and vocal sounds with the aim of trying to discern people's emotions, sentiments and personalities to influence consumer behaviour. Not content with trying to predict people's purchase habits, researchers are engaging in what's known as voice profiling: using automated data tools analysing people's voice characteristics to draw inferences about people's ethnicity, age or health conditions (Turow 2021, 265). Voice profiling, Turow remarks, could result in people being denied jobs, loans or services 'on the basis of physiological characteristics and linguistic patterns that we typically don't change and whose existence is certified by a science that may not actually be good at predicting behavior' (Turow 2021, 228).

Within the state, meanwhile, issues related to the collection and control of data have become relatively more important. One effect of this change is that traditional policy debates are reframed around the issue of who controls knowledge. For example, as we discuss in chapter 3, the move to an economy based on intangibles like data and IP wealth makes the debate over protectionism and free trade – a debate that unfolded in a world based on manufacturing production – a poor guide to understanding the economic stakes faced by a knowledge-based economy.

The emergence of a newly dominant knowledge structure does not imply a monolithic, specific set of policies or outcomes. It does not eliminate politics. Rather, it focuses political debate on a specific set of (knowledge-related) issues and gives pride of place to those actors deemed to have expertise in the knowledge-governance issues under discussion.

Policy Issue 1: Who should have control?

An information-imperium state must address two key policy issues. First, it must decide which actors should be allowed to control economically and socially valuable knowledge, the primary types at the moment being data and IP. This policy issue touches on questions of state-industry relations of the type involved in deciding, for example, whether data collected within a smart city should be controlled by the company that is collecting it, the city in which the data collection occurs or the individuals who serve as a source of the data. Should data, or IP, be shared amongst actors, as with a sovereign patent fund? Should data and IP produced within a country stay in that country? Beyond the state-market angle, Indigenous critiques of data and IP policy raise similar questions, whether control over knowledge produced within a group's traditional lands or that exploits Indigenous knowledge should stay with the group (see, e.g., Desai 2007; Sherwood and Anthony 2020).

Policy Issue 2: What should be the limits on this control?

The most important knowledge-governance policy in a knowledge-driven society involves deciding where to set the lines that restrict the use of knowledge. In an economy based on the control of proprietary knowledge, unlike one based on the trade in goods, it is very hard to avoid finding oneself in a zero-sum game. Because it takes knowledge to make knowledge, controlling economically valuable IP and data can allow a dominant firm to set the terms of entry into the market. The more proprietary the knowledge, the more 'winner-take-most' the game becomes, as the winner can effectively control the rate of innovation of its competitors, as the rents accrue to it and its home state. The role of knowledge in spurring innovation in production thus gives the control of knowledge a (state-based) national-security dimension, as countries seek to keep economically and militarily valuable knowledge out of competitors' hands (Vanderklippe 2018; Department of Finance Canada 2022b).

As we discussed in the previous chapter, commodified knowledge, such as with commodified data and IP, is a fictitious commodity. In other words,

the knowledge that is 'enclosed' by IP laws (May 2010) has uses beyond those of a mere economic commodity. Patents can (and do) restrict access to life-saving drugs. Copyright rules can kill off musical subgenres, such as sample-dense hip-hop (McLeod and DiCola 2011). Most importantly, because it takes knowledge to make knowledge, too-strict controls over knowledge can allow those who control current knowledge to stymie the creation of future knowledge that they believe may threaten their economic or social position.

Mainstream debates over how to regulate knowledge, be it data or IP, tend to assume that knowledge in general should be more freely available and that more access to knowledge is always better. This is not always the case. Sometimes, as with sacred Indigenous knowledge, or nuclear secrets, we may not want to have knowledge flow *too* freely. In any case, deciding where to draw the line between access and restriction will always involve assessments of competing interests. And no matter where you set the line, there will always be winners and losers.

A Note on Surveillance

Related to the question of limits on knowledge commodification is the question of surveillance. As with the limits on data or IP as a commodity, the question of when surveillance should or shouldn't be allowed is a central one, affecting as it does the ability to exercise basic rights such as freedom of expression and assembly. Surveillance itself is not the issue. Rather, it's the extent and purposes of surveillance that should raise concerns. Questions about surveillance necessarily entail discussions about privacy rights: not just their scope, but whether we should think about privacy as a right accruing to individuals or to groups (Taylor et al. 2017a). We discuss this issue in greater detail in chapter 9.

The New Dichotomy (Plus One): Knowledge Feudalism Versus Digital Economic Nationalism

The economic debates of the twentieth century were largely centred around support for protectionism or liberalized trade. In other words, whether governments would directly try to support their own industries by, among other things, raising barriers to trade in goods or whether they would lower these barriers to make their industries more efficient via free markets and international competition. The poles are always openness and liberalization versus protectionism and cross-border restrictions. By the 1990s, the forces of free trade had pretty convincingly defeated the latter.

The economics of knowledge governance, however, do not map easily onto the liberalization-protectionist topology. One approach to this debate is framed in terms of techno-nationalism (akin to protectionism) and techno-globalism (akin to trade liberalization) (Ostry and Nelson 1995). Techno-nationalism tends to be state-driven and 'seeks to justify limits on international trade and economic cooperation' (Banet 2018, 78), while techno-globalism 'supports global trade and sharing the benefits of technology innovation' across international borders (Banet 2018, 78; Ostry and Nelson 1995, 79).

The techno-nationalist/techno-globalist dichotomy is defined by the treatment of cross-border knowledge flows: open or restricted. This division, however, is not the most important aspect of this debate. Focusing on the control over the knowledge that is flowing (or not) across these borders is much more consequential because control over knowledge can persist even in the presence of open borders. Control over knowledge lies at the heart of power in the global political economy. What matters is not whether the knowledge is flowing but *who controls the knowledge even as it flows across borders*.

As illustrated in table 2.1, while techno-globalism imagines a world of international technological spillovers, international agreements such as TRIPS and the global footprint of large technology companies have created a world in which the economic benefits accrue back to the home office and the home country, with relatively few spillovers into the local economy (Drahos and Braithwaite 2002; Schwartz 2021).

Although the free-trade debates of the previous century trained us to focus on borders, the main economic contest in the twenty-first century is not between welfare-impairing protectionism and free knowledge flows. Rather, it is centred on the question of who controls knowledge and who benefits from this control. Instead of something being exchanged, the fact that knowledge remains controlled by the actor that initially possesses it leads to relationships of domination, in which whoever controls knowledge sets the terms upon which new knowledge/technology – and thus prosperity – can be created. Table 2.1 sums up the differences between the two frames. In the framework that we adopt, the two positions along the continuum are

Table 2.1: Summarizing the Contending Frameworks

Framework	*Key Policy Debate*
Protectionism v. Trade liberalization	Open versus closed borders for economic exchange
Techno-nationalism v. Techno-globalism	Open versus closed borders for knowledge/technology transfer
Digital economic nationalism v. Knowledge feudalism	Who will control economically and socially valuable knowledge?

knowledge feudalism and digital economic nationalism.[8] We now turn to a discussion of these concepts.

Knowledge Feudalism

Control over the creation, dissemination and use of knowledge is a fundamental lever of power in the knowledge-driven society. As we noted in chapter 1, one of the defining characteristics of knowledge is that it takes knowledge to make knowledge. Countries and companies that already possess stores of economically and socially valuable knowledge will tend to seek to preserve this advantage, by making it more difficult and expensive for others to access this knowledge. We call this strategy *knowledge feudalism*. We derive the term from Drahos and Braithwaite's concept of information feudalism, a metaphor which they used to describe economic relations, structured by IP rights, that involve 'a transfer of knowledge assets from the intellectual commons into private hands' (Drahos and Braithwaite 2002, 3).[9] We extend this idea to include all forms of knowledge, including data and other intangible assets, such as standards. Like information feudalism, knowledge feudalism describes an economic relationship of domination: it takes knowledge to create knowledge, so you need to pay to play in the knowledge-driven economy.

Because it seeks to extend control over knowledge, knowledge feudalism is a 'leader' strategy based on maximizing control over economically and socially valuable knowledge, which, in our society, is primarily data and IP. Much as free trade is the preferred economic strategy of dominant-producing countries (Chang 2002), knowledge feudalism is the economic strategy of a dominant information-imperium state. The United States is the world's premier example of a knowledge-feudalist state.

A knowledge-feudalist approach to economic policy comprises two key parts:

- strong protection of IP rights and control over data; and
- free cross-border knowledge flows.

At first glance, this combination of strong controls over knowledge and free cross-border flows may seem contradictory (Haggart and Jablonski 2017). Generally speaking, this is not the case. Rather, the guarantee of free cross-border knowledge flows is essential to create the conditions that allow a knowledge-feudalist state and its companies to dominate other markets internationally. Open borders are the necessary condition to pursue global monopolies. Strong IP rights ensure that rights holders, a substantial portion of them American (most others being from the European Union or Japan), get paid, while cross-border data flows create the precondition for data-based companies

like Google to exist at a global scale. While this open-borders approach superficially resembles the conditions necessary for countries to benefit economically from liberalized trade, cross-border knowledge flows operate according to a different logic than the international trade in goods. As we will discuss in chapter 3, while open borders combined with strong IP and data protections benefit the home country, their effects are much less beneficial for others.

While free cross-border flows are generally in the interest of the knowledge feudalist, its position as the holder of key economically valuable knowledge, such as patents, places it in a position to exert (somewhat hypocritically) structural power through its ability to deny access to its knowledge to actors it perceives as a threat. The United States' move in October 2022 to restrict significantly Chinese access to advanced semiconductors can be seen as an attempt to exert its structural power over knowledge to thwart the rise of an economic and military rival (Sheehan 2022). Similarly, parallel US restrictions on the importation of communication technologies made by Chinese national champions Huawei and ZTE can be seen as a knowledge-feudalist attempt to stymie the rise of a rival in a key part of the knowledge structure, for security and economic reasons (Demarais 2022).

Knowledge feudalism, in its current iteration, is underwritten most directly by international trade agreements. Highly commodified knowledge rules, imposed via treaties such as the TRIPS Agreement, create monopolistic conditions, in which new entrants to a market, lacking the needed IP, must effectively pay to play. These rules, therefore, provide rule-makers with the ability to set the direction of economic and social development, dividing society in two: those who control knowledge and those who wish/need to use this knowledge. Similarly, as economist Dan Ciuriak (2018b, 6) notes, there seems to be a 'tendency in the data-driven economy towards concentration at a global level' that raises competition concerns. Elsewhere, he hypothesizes:

> While firms can work their way around patents, there is no way to work around lack of access to data. This points to extreme network externalities in the data-driven economy, where firms that secure access to data will gain powerful competitive advantages in terms of having smarter AI (in other words, the superstar firm advantage). (Ciuriak 2018a, 7)

In terms of the balance between state and non-state power, one can expect a knowledge-feudalist approach to have a general distaste for *direct* industrial policy once the conditions for strong knowledge protection and free and open borders have been secured for their industries. That said, such states will tend to find a way to provide de facto support for their preferred industries, the US military's support for Silicon Valley and high technology manufacturing in general being just the most obvious case (Powers and Jablonski 2015).

Knowledge feudalism, then, is a nationalist strategy of open borders and strong IP and data protection (for owners) practised and promoted by states whose companies are dominant owners of knowledge and that control basic internet infrastructures/platforms. It tends to be pitched in a universalist manner even though it places those who control knowledge in a dominant hierarchical relationship with others. Its objective is domination akin to what Couldry and Mejias (2018, 2019) call 'data colonialism' with respect to data and what Drahos and Braithwate (2002) call information feudalism with respect to IP. In contrast, digital economic nationalism is the information-imperium state policy practised by challengers to the dominant state player(s).

Digital Economic Nationalism

We live in a knowledge-feudalist world. As Breznitz details in his essential 2021 book *Innovation in Real Places* and as we explore in the following pages, the current global IP regime is designed to stifle, not encourage, innovation, channeling control and profits to those – primarily American – companies that already control economically valuable IP (Breznitz 2021). Similarly, Breznitz argues that policymakers have been slow to understand how important data creation and control is for economic success and that merely having, for example, a US-based multinational as the anchor in your smart city does not guarantee sustained economic development if the multinational retains control over the data produced in the smart city (Breznitz 2021).

Knowledge feudalism is a leader's strategy that is not available to other actors. It does, however, invite responses that address situations in which control over valuable knowledge resources rests with others. Such responses are not new to the information age. The current situation has echoes in the literature related to the New World Information and Communication Order (Rogerson 2003, 145–47) and concerns about communications sovereignty dating to the 1970s (Schiller 1975). In both situations, control over the knowledge that societies needed to develop politically, culturally and economically lays with dominant powers, particularly the United States.

We call this response digital economic nationalism. If knowledge feudalism is a strategy based on maximizing control over existing knowledge and IP, focused primarily on maintaining global dominance of a single country and its companies, then digital economic nationalism can be thought of as nationally coordinated attempts to generate and control economically valuable IP and data. Examples of such policies include Canada's 'superclusters' policy (Knubley 2021), in which the federal government has targeted funding at six priority industries for development.[10] It also covers such initiatives as national AI strategies in the European Union (European Commission 2018), sovereign patent funds (Clarke 2017; Lee-Makiyama and Messerlin 2014)

and the use of government procurement to promote domestic IT industries (Belsher 2016).

Unlike knowledge feudalism, digital economic nationalism encourages a degree of (often state-led) knowledge sharing among a state's companies. This sharing is designed to counter the economies of scale and scope of the dominant knowledge-feudalist companies. As the 'nationalism' term implies, however, this cooperation is limited by borders. Digital economic nationalism reframes cross-border IP flows as potential threats to national security, such as concerns about Chinese access to IP developed in Canada but paid for by Chinese funding (Fife and Chase 2021).

Again, this focus on borders bears a superficial resemblance to protectionist policies in traditional trade policy. However, while open borders in a free-trade world are supposed to lead to more efficient production, open borders in a knowledge-driven world create the condition for global monopolies, traditionally the bane of economists for their tendency towards inefficiency. Here, an emphasis on cross-border restrictions, at least in principle, can serve as a means to stave off global monopolies and induce greater competition.

Far from being an illegitimate 'authoritarian' imposition on a free market or (at the extreme) on free speech, digital economic nationalism is a logical response to the underlying economic logic of a knowledge-driven economy, that is to say of an information-imperium state. Both knowledge feudalism and digital economic nationalism are designed to maximize the benefits to the home country's state and businesses (technically, to the dominant state-society complex) in a global economy. While a knowledge-feudalist approach presents itself as a universalist ideology that ignores the hierarchical relations of dominance it creates, its explicit reference point is the national community, with companies defining themselves by their nationality.

That the state plays an explicit role in digital economic development does not make it an authoritarian strategy. The pursuit of economic advantage via government policy is something all states do. The pursuit of national advantage in data-intensive industries and technologies like machine learning/artificial intelligence is being pursued widely across countries and continents. This is not creeping authoritarianism; it's a response to a knowledge-based economy in which the winner takes all.

Both knowledge feudalism and digital economic nationalism are nationalist strategies that seek to maximize their economic position in the global economy. In terms of the role of the state, the key differences between the two are an explicit embrace of state industrial policy by digital economic nationalist states to promote the interests of specific economic sectors, as well as 'picking winners' – favouring certain companies in ways that go beyond helping the very smallest companies get off the ground. It is an approach that directly embraces the idea of national champions and state support since

the state is usually the only entity with the capacity to confront larger global players.

Given the strong connotations around the word 'nationalism', we should note that we are not referring here to ideologies of ethnic or racial supremacism. As the term suggests, digital economic nationalism is driven by an economic logic, not a racist one. On the IP side, it takes knowledge to create more knowledge. In a knowledge-feudalist regime, characterized by the rampant commodification of knowledge, this reality means the control of knowledge can be (and is) used to shut competitors out of markets and shape the direction of innovation in a direction that suits the incumbents' interests. This is the 'patent thicket' problem, in which patents are used not to promote the dissemination of knowledge but as a protectionist barrier against market entry (Drahos and Braithwaite 2002, 49). Small companies and small countries wanting to move up in the knowledge game must figure out a way to balance against the knowledge-controlling foreign giants and how to keep knowledge – redefined as a key asset underwriting a company's value – out of competitors' hands.

Similarly, control over data has been identified as a key economic issue (beyond social concerns regarding privacy) as data is the primary input into machine-learning processes that stand to revolutionize the economy through a vast new wave of automation. In keeping with the nationalist theme, data is identified in the digital economic nationalist perspective as a resource that is extracted by foreign companies with little benefit to the home economy. From this perspective, ensuring that local communities benefit from the data extracted from them is a perfectly reasonable demand.

On and Outside the Continuum: Control and Decommodification

In between digital economic nationalism and knowledge feudalism lie many strategies that take the current knowledge-feudalist system (as well as a highly dysfunctional financial regime, a topic that lies outside the scope of this book) as a given. What these strategies all have in common is an emphasis on the need to control knowledge in some way, usually related to economic and security issues, while also being prepared to defend one's community against dominant actors' attempts to use their proprietary knowledge to stifle this new innovation or reduce a country's security (Breznitz 2021).

While digital economic nationalism and knowledge feudalism are somewhat in tension with each other – the leader is trying to maintain its dominance against those who would challenge it – they also share some important commonalities. Most significantly, they both place the control of knowledge at the core of the state (and the state-society complex's) purpose. As a result,

they both embrace the same economic and security imperatives to collect as much data as possible while also pursuing strong IP rights (albeit a bit looser for in-groups under a digital economic nationalist approach). These imperatives by definition imply the need for extensive surveillance to collect data and to enforce IP rights.

This point highlights the limits of digital economic nationalism as a challenger to knowledge feudalism. Digital economic nationalism embraces the basic tenets of a knowledge-driven society: that the key to prosperity and security is the capture and control of information. The goal of the digital economic nationalist isn't to overturn the system but to overthrow and replace the dominant knowledge-feudalist actor. As such, while digital economic nationalism is a logical response to living in a knowledge-feudalist world, it leaves mostly untouched the problems that arise from treating knowledge as a Polanyian fictitious commodity. These issues can only be addressed by placing limits on our treatment of knowledge as a commodity and by, in turn, focusing on who *should* control knowledge and for what purposes. These questions can lead us to consider interventions from scholars and others interested in issues of data justice and Indigenous data and knowledge sovereignty that often go unexamined in more economic- and security-focused policy debates.

Thinking about the role of surveillance, meanwhile, points us towards the overarching regulatory duty of the information-imperium state to address the tensions inherent in the creation of any fictitious commodity. The logic of the information-imperium state and its two main strategies (digital economic nationalism and knowledge feudalism) is to maximize control and thus surveillance, in the name of economic prosperity and national security. However, as with all fictitious commodities, embracing these maximalist tendencies will lead the knowledge-driven society to erode the foundations of society – such as the need for a degree of individual privacy or for access to life-saving drugs – that make a society humane. In other words, governments and non-state actors with an interest in the long-term stability of society must also develop regulations that restrict this unfettered commodification and surveillance. This need for a limiting rule suggests that in addition to digital economic nationalism and knowledge feudalism, we need also to consider a third strategy, one that transcends the limits of a knowledge-driven society, namely knowledge decommodification.

A decommodification strategy still requires considering issues regarding the control and transmission of knowledge, because as we've noted, knowledge is constituted by such questions. However, pursuing a policy of knowledge decommodification raises the possibility that we might consider alternative forms of creating, controlling and using knowledge for humane purposes that do not treat knowledge as either a commodity or simply as a national-security input. For example, facial-recognition technology may make a great deal of sense from both economic and national-security perspectives, but it has come

under intense and thoughtful criticism for its potential to violate civil rights, turning a community into an Orwellian surveillance state, where somebody is always watching you (Deibert 2020; see also Lyon 2015). Restricting some forms of data collection and use is not just about protecting individual privacy. It also pushes back against the growing belief in dataism, which is the belief that data and data-driven automated decision-making systems provide a more objective means of regulating society.[11]

To figure out how to navigate a knowledge-driven society, we should not let its internal logic define our ultimate objectives. The goal, as we will discuss throughout the following pages, should not be to make the knowledge-driven society work as efficiently as possible but to limit the commodification and control of knowledge sufficiently to ensure that we can capture its benefits in service of our overarching goals of improving individual and social well-being.

CONCLUSION

Using Susan Strange's concept of structural power, we have argued that we are witnessing the rising importance of the knowledge structure over other structures. This 'knowledg-ification' of society involves the reinterpretation of economic and social activities in terms of the data and knowledge that they produce. It emphasizes control over knowledge, particularly in the form of IP rights and data, as a means for exerting economic and social power. Economically, this involves the commodification of knowledge in the form of data and IP in pursuit of profit. From a security perspective, it involves equating security to the state's ability to collect data on its citizens and their environment to prevent threats. In both cases, ubiquitous surveillance plays an essential role: reduced surveillance is equated with reduced security and lost economic opportunities.

In a knowledge-driven society, who controls knowledge and the rules governing its uses (as well as who determines those rules) become primary political battlegrounds. Importantly, as Strange notes, both state and non-state actors can exert structural power in this area. The issue of who controls knowledge and for what purposes is a first-order concern in a knowledge-driven society. Many of the issues we examine in the coming pages turn on this question.

These issues cannot be separated from their global context, if only because the dominant actors, such as Google and Amazon, have a global reach, underpinned by the long-term nurturing of a knowledge-feudalist regime by the United States. It forces a reconsideration of what counts as sound economic and social policy, as well as a re-examination of the role of the state in promoting a strong economy and healthy society. The following chapters are designed to walk readers through what it means that data and IP, and a small number of tech companies like Google, have become so central to our lives.

NOTES

1. Palan (1999) explicitly remarks on the similarities between the two, who were colleagues at the London School of Economics, though he is careful to remark, 'The extent to which Mann influenced Susan's ideas is unclear to me'. The two, he notes, employ somewhat different terminology: Mann equates military power with Strange's security structure; unlike Strange, Mann does not divide economic power into its finance and production components; and Mann decomposes what Strange sees as a single knowledge structure into two components – ideological and religious. On the knowledge structure, Palan further notes that hers was probably less influenced by 'a sociological conception of knowledge' than by 'the work of the New Trade theorists' (Palan 1999, 127).

2. These modifications to Strange's theory of the knowledge structure were first discussed in Haggart (2017) and Haggart (2019c).

3. The emphasis of, for example, Foucault (1980) on the role of power in constructing knowledge can be seen as a similar approach. We discuss the role of knowledge legitimation in the following pages.

4. We are not the first to see the potential benefits in pairing Robert Cox's work with that of Susan Strange. Christopher May suggested it over two decades ago, although we do not believe many, if any, have developed it significantly (May 1996). Cox himself noted the complementary nature of their approaches (Cox 1996b).

5. The concept of the information-imperium state was first outlined in Haggart (2018a). Thanks to Peter Drahos for suggesting the term. We had also considered knowledge-driven state. However, we believe that information-imperium state better captures the nature of power as it relates to the control of and over knowledge.

6. Though see our discussion in chapter 4 regarding issues with the term 'big data'.

7. While this is very much a non-exhaustive list, see Castells (2009), Comor (1996), Benkler (2007), Bell (1976), Jin (2015), McChesney (2007) and Mosco (2009).

8. The idea that trade liberalization can create win-win situations is not without its critics, who highlight how such policies can serve as a means to cement the dominant position of industrialized states (see especially Chang 2002; for a discussion of the limitations of free trade as an economic policy see Rodrik 2011). While trade liberalization is not exactly equivalent to policies encouraging cross-border knowledge flows, the free-trade critique highlights how even perceived situations of openness can create asymmetrical power relationships. Nonetheless, in this chapter we present the liberal argument for free trade as our starting point because free trade-versus-protectionism remains the dominant trade-policy frame.

9. Following Drahos and Braithwaite, we do not claim that we are witnessing a return to medieval times. Rather, we use feudalism as a metaphor designed to highlight an economic model based on raising 'levels of private monopolistic power to dangerous global heights' (Drahos and Braithwaite 2002, 3). For a critique of the concept of 'techno-feudalism', see Morozov (2022).

10. These industries are: digital technologies, plant proteins, advanced manufacturing, AI in supply chains and 'oceans', each based in a region of the country (Innovation, Science and Economic Development Canada 2021). Launched in 2018, the federal government's April 2022 budget renewed its mandate while rebranding them as Global Innovation Clusters (Department of Finance Canada 2022a). Not all of these clusters involve digital tech; however, they all reflect a more nationalist, government-led approach to economic development than had been seen in Canada since the early 1980s.

11. We discuss dataism further in chapters 4 and 5.

Part II

EXPLORING THE KNOWLEDGE-DRIVEN SOCIETY

Chapter 3

Intellectual Property and the Economics of Control

To understand how the knowledge-driven society functions, at a macro level or at the level of the smart city, we have to pay attention to intellectual property (IP).

A knowledge-driven society – that is, a society in which the knowledge structure is dominant – is defined by the extent to which control over knowledge shapes outcomes in other sectors of society. In our market-based society, IP is a primary instrument used for exerting this control, particularly over production processes. Control over key IP rights can set up companies to receive licensing fees from those who want to use their protected ideas.[1] Knowledge builds upon knowledge, meaning that control via IP can provide IP owners a significant say in the future direction of cultural, economic and social innovation, promoting some paths and actors, while inhibiting others.

Such control places enormous power in the hands of those actors – typically companies – that control socially and economically valuable knowledge. To take one example, seed patents are based on the idea that control over life – in this case plants – can be granted to an actor, thereby allowing corporations to sue farmers for the unauthorized planting of proprietary seeds (Schauenberg 2019). When people and governments are not able to afford or access patented life-saving drugs and vaccines, this type of control can be literally a matter of life or death.

The control over proprietary technology allowed by IP rights can also lock a city into a single supplier's technology because IP allows the owner of the IP to set the terms of access and interoperability. As anyone who owns a Mac or PC knows, this control can make switching to other technologies prohibitively costly, even if your current system is sub-par. Control over IP matters, and what IP you don't control can be used against you.[2]

IP now matters to more people in more ways than ever before. Its importance extends to the heights of the global economy. As far back as 1998, economist David Teece argued that 'intangible assets' (which includes IP) had become 'the main basis for competitive differentiation in many sectors' (Teece 1998, 76; cited in Buckley et al. 2022, 2). In particular, changes to global IP rules have underwritten the transformation of the global economy from one based on international competition and free trade to one based on hierarchical global value chains (GVCs). In these GVCs, IP serves as a primary means of exerting control, appropriating the lion's share of value produced within these chains, with negative effects on productivity, income equality and economic growth (Schwartz 2021). Control over knowledge, in other words, is now a primary way in which economic control is exercised.

In this chapter, we describe both the nature and some of the most important effects of the current global knowledge-feudalist IP regime. We argue that in our current context, IP is best understood as a system of control designed not to encourage innovation but to extract economic rents – that is, payments above what would be realized in a competitive economy. Responses to this knowledge-feudalist regime tend to take the form of a digital economic nationalism in which countries and companies attempt to break into the monopolistic IP game but at the cost of replicating the same negative effects on economic growth and access to information that plague the current knowledge-feudalist regime.

This chapter is structured as follows. For most people, IP remains unnecessarily shrouded in mystery. We attempt to cut through the conceptual fog in our first section, which defines and describes IP. The second section describes how the inclusion of IP in trade agreements has transformed the global economy along the model of the franchise (think McDonald's). The third section pulls our focus back out to consider the larger policy implications of basing an economy on the monetization and control of knowledge as IP.

UNDERSTANDING INTELLECTUAL PROPERTY

IP 'is a type of property regime whereby creators are granted a right, the nature of which is entirely dependent on the nature of the creation on the one hand, and the legal classification of the creation on the other' (Dutfield and Suthersanen 2008, 12). IP regimes are enacted via domestic laws that are embedded within regional and multilateral agreements. Increasingly, IP regimes are also interpreted and enforced by private actors via contracts and, in many cases, via digital locks: computer programs that restrict, for example, who is allowed to watch a film on their computer or read an ebook.

Generally, IP discussions tend to focus on four primary forms of legal protection. Copyrights are the legal protection provided to creative works such as books, music, motion pictures and – in an accident of history – computer programs. Patents, meanwhile, typically cover industrial processes, such as drug formulas and – in another accident of history – living organisms. Trademarks are the legal protection provided to identifying symbols, such as McDonald's golden arches. Trademark protection has also been extended recently, in the United States, to scents like Play-Doh's (Siegel 2018). Finally, trade secrets are commercially valuable knowledge whose value is derived from their secrecy. Trade secrets encompass not only well-known examples like the formula for Coca-Cola but also Google's proprietary search algorithms. While copyrights and patents typically take pride of place in IP discussions, trade secrets are becoming increasingly important. It's not too much of a stretch to say that Google's status as one of the world's most valuable companies rests on its trade secret–protected search engine.[3]

As this very brief description suggests, the seeming solidity of the aforementioned four categories belies the reality that these labels cover ever-expanding and ever-changing types of knowledge. As Dutfield and Suthersanen note, the concept of IP 'is in a state of constant evolution and reconsideration' (2008, 14). Copyright regimes, for example, originated in England in the 1700s and patents in Venice in the 1400s. 'However', they also remark,

> the first English and Venetian laws were public in nature, a means of harnessing foreign technologies, or of regulating and censoring domestic printing. But by the nineteenth century, IP had become classified as a type of private law, conferring private property rights on the few. (Dutfield and Suthersanen 2008, 12; see also May and Sell 2006)

The content and functioning of these labels are more reflective of legal convention and historical chance than any hard-and-fast rules. In practice, legal IP categories are remarkably malleable. For example, what copyright law covers has expanded dramatically since the original copyright statute, Britain's 1710 *Statute of Anne*, and not always in ways that make intuitive sense. Computer programs – which are as much tools as they are forms of expression – are now covered by copyright, but recipes and fashion designs are not. While computer programs are covered by copyright, they are also increasingly being patented, thus offering another example of the fluidity of these legal categories.[4]

The seemingly discrete and limited nature of these categories is reinforced by a vast legal literature discussing what is the appropriate length of protection for a book, or whether a scent can be trademarked. In reality, IP can be

extended to cover any form of knowledge. A society such as ours, in which economic power derives from the control over knowledge, will face inexorable pressure to commodify and extend this type of coverage to as many forms of knowledge as possible.

IP as Incentive

There are two stories we can tell about what IP is and how it functions. We can focus on IP's role in economic and cultural development. The second, and more contemporarily relevant, story, meanwhile, focuses on IP as a means to exert control over the economy, creativity and innovation.

Knowledge is the foundation of economic growth and cultural and social development. All innovation builds on previous ideas and innovation. Coming up with a good idea and putting it into practice can be expensive in terms of time and money but copying is often quite inexpensive to do. The film *The Last Jedi* may have cost US$317 million to make, but in the shadier parts of the internet, you can download it at no marginal cost to you. IP rights provide the copyright holder with monopoly rights to control who is able to do what with their intellectual creation and to sue those who violate these rights. In doing so, IP creates a legally enforceable scarcity in this creation that the holder can use to profit off the creation without being worried about being undercut by low-cost copiers. The exact terms and scope of IP protection vary depending on the relevant law.

Like all monopolies, though, this protection comes at a cost. As we highlighted in chapter 1, the creation of new knowledge requires access to existing knowledge. However, the protection provided via IP restricts the dissemination of existing knowledge. In the case of Star Wars, copyright law gives Disney a veto over who is allowed to tell Star Wars stories to a large audience. We can repeat the same exercise with any form of knowledge. As economists Michèle Boldrin and David K. Levine note, patent protection provided to James Watt, inventor of the steam engine, allowed him to block socially beneficial innovations to his invention for years, imposing a material cost to society from the benefits that would have been reaped by the earlier deployment of a better engine (Boldrin and Levine 2007, 1–5).

This tension creates what political scientists G. Bruce Doern and Markus Sharaput refer to as the 'production-dissemination paradox': the monopoly protection provided by IP is justified as a means to increase knowledge production, but this very protection reduces the dissemination of the knowledge needed to create new knowledge (Doern and Sharaput 2000). As a result, all IP laws include limitations of these monopoly rights, be it in duration (e.g., general copyrights are limited in Canada to the life of the author plus 70 years – after that, the works are considered free for all to use), by activity (e.g., patent laws often allow for the mandatory licensing of drugs during national

emergencies) or the knowledge allowed to qualify for protection (e.g., recipes tend not to qualify for copyright protection).

The production-dissemination paradox highlights an important truth: that IP policy necessarily involves making a trade-off between providing protection for knowledge and encouraging its dissemination. Unfortunately, there exists no single socially optimal balance between protection and dissemination. As we noted in chapter 1, any balance you come up with will encourage some forms of knowledge production and discourage others. Returning to our example from that chapter, requiring that musicians license samples effectively killed off sample-dense music within the commercial music industry. However, these rules can also push musicians who can no longer afford to create sample-heavy music towards other forms of expression. Different people can have legitimate disagreements over whether these new rules were socially beneficial and more generally over where to draw the line between protection and dissemination.

The story of IP as an incentive takes for granted that IP is necessary to incentivize creation and innovation. In practice, this is not always the case. As economist Mariana Mazzucato and others have noted, the most economically risky research tends to be undertaken by governments, not private actors, and is not incentivized by the existence of IP. Instead, she argues that IP represents a privatization of the rewards related to this earlier, foundational research (Mazzucato 2018; see also Towse 2013). Similarly, looking at the historical record, economist Petra Moser has shown that 'in countries with patent laws, the majority of innovations [occur] outside of the patent system'. Meanwhile, 'Countries without patent laws have produced as many innovations as countries with patent laws during some time periods, and their innovations have been of comparable quality' (Moser 2013, 40).

Regardless, IP remains a dominant form of knowledge regulation. That there is no socially optimal balance between protection and dissemination means that IP is fully embedded in the world of politics. The balance struck in any given treaty or law tends to reflect the balance of power between the interests of those actors that already control significant economically valuable IP (they want greater protection) and those who depend on access to IP for their livelihood, such as start-up companies or farmers, or for their lives, such as those at risk of Covid-19 or AIDS (they want/need greater access to existing knowledge). That IP law reflects political, not technocratic, logics also means that IP law is characterized by a significant degree of arbitrariness, both in terms of what is or isn't protected and the scope of protection provided.

IP as Instrument of Control

Copying others is the essence of development and cultural creation. Today's advanced industrialized economies, including the United States – the leading

state proponent of ever-more-protectionist IP laws – developed by copying others' technologies (Chang 2002). That these same states promote historically strong global IP protections that restrict the type of copying that has underwritten their development strongly suggests that IP is best thought of not as an instrument to encourage development but as an instrument of control, 'kicking away the ladder' so that developing states cannot follow the well-trod path of innovation through copying.

IP functions as an instrument of control in that it provides those who control the IP with the power – limited by exceptions – to control who is allowed to use the knowledge protected by the IP rights in question. This right can involve denying or allowing use or requiring payment for the use of IP. These rights are almost always limited by exceptions designed to encourage knowledge dissemination in particular circumstances. This is why patents and copyrights are limited in time before they become open to everyone to use. It's also the justification for exceptions in many copyright laws for uses such as research, education or parody.

However, the more that IP laws tend towards the protection side of the protection-dissemination paradox, the more that IP functions as an instrument of control. As an instrument of control, IP law allows IP owners to engage in what economists call rent-seeking: economic activity that does not contribute to economic productivity. Since the 1990s, the current global IP regime has tilted increasingly towards the protection side (Durand and Milberg 2020, 410–12), in ways that stifle innovation and economic growth through the control of key, economically valuable knowledge (Mazzucato 2018). As Dutfield and Suthersanen argue:

> A case could be made for arguing that we in the developed world are not becoming knowledge-*based* economies as quickly as we are becoming knowledge-*protected* economies, or even – and this is a bit more worrying – knowledge-*overprotected* economies, in which the dominant industries maintain their market power by tying up their knowledge in complex bundles of legal rights and instruments such as patents, copyrights, trademarks and restrictive contracts and licensing agreements. (Dutfield and Suthersanen 2008, 8–9; emphasis in original)[5]

Moser, as well as Boldrin and Levine (2007), goes even further, arguing that the patent regime presents a structural disincentive to innovation. Again, looking to the historical record rather than (inconclusive) economic theory, Moser remarks that 'as early as the 1850s, patentees who did not produce anything were able to hold up entire industries because they had been issued broad patents that had been affirmed in court' (Moser 2013, 39).

Attempts to maintain market power through IP take many forms. Companies can create a 'patent thicket', filing or purchasing bundles of patents, say, in the mobile phone industry, in order to deter new entrants. Another strategy is for a company to buy existing patents, not with the intention of producing something but of suing those who are already producing the thing in question for violating 'their' patent. Whether it's a patent troll or an incumbent company deploying a patent thicket to stifle competition, the result is the same. Because the creation of new products, almost by definition, relies on existing, monopolized knowledge, newcomers must either pay to play by licensing the patents, thus giving the incumbents a piece of their action, or live in fear of an economically ruinous lawsuit. That the standards for what can be protected by IP laws have declined over the past several decades to a point where, for example, even some scents can be legally protected as trademarks only increases this fear.

This combination of patent thickets, patent trolls and the like represents an unproductive drain on the economy in terms of legal costs, the retention of lawyers to prosecute or defend against these lawsuits, higher costs due to decreased competition and the loss to society of never-realized innovations. Beyond lost innovation, Brander (2007) notes that the desire to construct defensive patent thickets can lead to a 'patent race' that can actually result in 'excessive investment in innovation and excessively early implementation of innovations in an effort to pre-empt others' (Brander 2007, 203; see also Hoen 2009).

The Social Construction of Intellectual Property

All societies have their own rules and norms governing what they see as valuable knowledge. Drawing on legal scholar Miranda Forsyth's research, Forsyth and Haggart (2014) discuss the confusion over a copyright treaty during negotiations between the United States and the Pacific island nation of Vanuatu. Vanuatu was interested in signing a treaty with the United States in part because they believed that it would provide protection for the bungee jump, whose origins can be traced to there. To be clear, nothing in copyright law, and especially not in this treaty, allows for IP protection of the bungee jump. In this case, as Forsyth and Haggart argue, Vanuatans and Americans both had different conceptions of what types of knowledge deserved protection. Vanuatans saw the bungee jump as a valuable form of knowledge that deserved protection and the United States did not. Only one view – the US perspective – of what counts as valuable knowledge deserving protection prevailed: not because Vanuatans were 'wrong' in thinking that the bungee jump was valuable knowledge, but purely as a result of US structural power to determine what counts as valuable knowledge.

Different societies regulate knowledge in ways that reflect the dominant (and sometimes conflicting) values of the society within which these rules

are created. IP rights are no different: they are socially constructed, reflecting historically specific biases and interests, and favouring certain groups and outcomes. Consider how the legal distinctions between copyright and patent laws in Canada fail to recognize the essence of Indigenous knowledge:

> For example, a patent, a trademark, or a copyright cannot adequately protect a ceremony that uses striking sacred-society symbolism to communicate empirical knowledge of medicinal plants. The medical knowledge may be patented, but the patent will expire in a matter of years. The text and music for the ceremony can be recorded (or 'fixed') and copyrighted, but only the recorded version will be protected and only for the lifetimes of the performers plus fifty years. The symbols can be protected as trademarks forever, but their significance will be diminished when they are taken out of context. (Battiste 2005, 8)[6]

Both IP and Indigenous knowledge systems as described here are interpreting the same underlying reality – medicinal knowledge, cultural expressions, symbols – but in different ways and with different objectives. These different ways of seeing the world derive from each perspective's fundamental assumptions and values.

Understanding the foundational values underlying the institution of IP, and their contingent nature, helps us understand that IP is only one possible way of regulating knowledge. Recognizing this, in turn, can help keep our minds open when considering ways to reform the global IP regime, including alternatives that exist outside the current regime.

Bias towards the Individual

Like all forms of knowledge regulation, IP reflects its historical origins. Current IP rules have two primary characteristics: a bias towards individual control over knowledge and its status as a means to commodify knowledge. These two characteristics reflect IP's European origins and its links, respectively, to European individualism and the Enlightenment, and the development of capitalism. Intellectual property, as well as individualism and capitalism, spread, via conquest and colonialism, to the rest of the world (see, e.g., Bannerman 2013 on the colonial origins of copyright).

The first characteristic of IP deals with *who* is allowed to control knowledge. Here, IP demonstrates a bias towards individual control over knowledge. While there exist various philosophical justifications for the creation of IP (see Drahos 1996), they all involve justifications for individual control of knowledge. The idea of the individual author is so deeply engrained in our individualist society that we often lose sight of the fact that this type of attribution is highly unnatural, in the sense that it only captures a part of the reality of how knowledge is actually created. Knowledge creation is a cumulative

process. Our names are on the cover of this book, but it is built on the work of hundreds of previous authors, to say nothing of our conversations over decades with innumerable colleagues that we've internalized.[7] Losing sight of the reality that this focus on the individual author is merely a 'conceit' (Litman 1990) and not an accurate description of how actual creation happens can lead to problems in crafting an IP system that does not stifle creation and innovation. Specifically, the emphasis on the individual author biases IP policy towards the protection side of the protection-dissemination paradox.

IP politics is a contest between those that favour stronger protection – generally speaking, those companies and individuals that control significant IP portfolios – and those that favour greater access rights – generally speaking, those companies and individuals that don't hold significant IP or that depend on access to knowledge in order to function (such as libraries, consumer electronics makers and generic drug companies, as well as net IP-importing countries such as Canada). Left out of this debate are actors, such as Indigenous groups, whose concept of knowledge governance doesn't follow the individualist, commodity-control focus of an IP knowledge-governance regime.

Commodification of Knowledge

The second important characteristic of IP is that it commodifies knowledge, turning it into a product that can be bought and sold. All knowledge-governance regimes reflect the society in which they exist, and IP is no different. Alongside the individualist heritage of the Enlightenment, IP reflects 'the political, philosophical and economic history of modern capitalism', with attempts to control 'valuable knowledge and information' stretching back to before the development of a 'formal legal definition of intellectual property' (May and Sell 2006, 4). This link to capitalist processes takes the form of the *commodification* of 'knowledge resources' (May 2010, 13), designed to turn these abstract concepts into property that can be bought and sold in the marketplace. These rights give IP owners (who are not necessarily the actual creators of the knowledge in question) several benefits: '(1) the ability to charge rent for use, (2) the right to receive compensation for loss, and (3) the right to demand payment for transfer to another party through the market' (May and Sell 2006, 7). This commodification means that the rights to a form of knowledge (say, a book) created by one individual can be sold to another, who then effectively controls it. There are caveats and limitations to these rights, but that's the general principle.

In other words, and as we discussed in chapter 1, IP is an example of what Karl Polanyi called a fictitious commodity, one that has an existence and purpose outside the market (Polanyi 2001; see especially Jessop 2007). As Polanyi noted, forgetting that fictitious commodities have alternate

purposes, and treating them as means towards (market-based) ends, risks social ruin and societal collapse.

Strip mining the environment for 'natural resources' can destroy the biosphere upon which our very existence depends. The same goes for knowledge and IP. When IP protection is extended too far, it stifles the processes by which knowledge is actually created. More terrible societal outcomes await when we forget that IP is a fictitious commodity and that the value of knowledge cannot be reduced to a market price. Patent laws and treaties, for example, stand near the centre of the weak global response to the Covid-19 pandemic. Current IP treaties allow for vaccine patents to be waived in emergencies, but countries have proven remarkably unwilling to take such a step even after millions of deaths worldwide (Amnesty International 2021). For example, in 2021, in the depths of the Covid-19 pandemic, Germany rejected calls to waive patents on Covid-19 vaccines, because, in the words of a spokesperson for the German government, 'The protection of intellectual property is a source of innovation and must remain so in the future' (Reuters 2021). Left unacknowledged was the reality that 'the vaccines benefited from unprecedented public funding' (Mazzucato and Ghosh 2021). This reluctance mirrors previous attempts by patent-dependent pharmaceutical companies to resist compulsory licensing for life-saving AIDS drugs (Drahos and Braithwaite 2002).

We see similar resistance with respect to the even-more-existential crisis of climate change. Regulatory scholar Peter Drahos, for example, argues that the zealous protection of IP rights in clean technology is one of the most significant impediments towards the rapid spread of the technologies needed to combat a climate disaster that could upend human civilization across the entire planet (Drahos 2021). In both cases, the fictitious commodification of knowledge – which treats knowledge as a wealth creator rather than the know-how to save human civilization – trumps the actual purpose of knowledge, to enrich human life.

Because IP is a human-created form of knowledge governance, its characteristics can be challenged, modified and altered. Even within the institution of IP, instruments like the concept of the public domain – which comprises intellectual works, like Shakespeare's plays, that are no longer subject to IP protection – can effectively decommodify a creative work. However, IP's roots in Enlightenment individualism and market capitalism are deep and resistant to change.

HOW IP TRANSFORMED THE GLOBAL ECONOMY

In the introduction to this book, we mentioned briefly how enthusiastic Canadian politicians, from the prime minister down to Toronto's mayor, were for the Toronto Quayside project. Part of Sidewalk Labs' allure for Canadian

politicians was the promise that it would turn Toronto into 'a global hub for urban innovation' to create and test smart-city technologies that could then be marketed throughout the world. This hub would be 'anchored by a new Google campus, a new applied research institute, and a new venture fund for Canadian companies' (Sidewalk Labs 2019a, 425).

This type of play – inviting a large, typically US, company to set up branch plants in Canada as a means to spur economic growth and prosperity – is common throughout the world. However, it has a special resonance in Canada, whose industrialization and manufacturing sector – particularly its auto industry – were built largely by the American branch plants that were encouraged via government policy to locate here (Williams 1994; Yates and Holmes 2019; Melanson 2009; Helleiner 2019). On the surface, courting Google to set up a branch plant in Toronto fits perfectly with this tried-and-true economic-development strategy.

Times have changed, however. Google is a very different company from General Motors (GM) or other large manufacturers, and economic development in our knowledge-driven economy does not happen the same way as it did in the 1880s, let alone in the 1960s and 1970s. Strong IP rights – and the control of commodified knowledge generally – is a large part of the reason for these differences. In a knowledge-driven economy, the employment and economic-development pay-offs to both manufacturing and having a large company present in your community are much lower than they were previously, and the path to prosperity runs a much different course.

The Awkward Fit between Trade and Intellectual Property

One of the ways that we can identify whether a particular structure has become dominant in society is the extent to which its logic, policy tools and key actors have reshaped the other structures. Trade agreements, for example, used to be concerned primarily with lowering tariffs and other barriers to trade among countries. This policy – the foundation of the post–Second World War international economic order – was based on the theory of comparative advantage. This theory, subject to many caveats (Rodrik 2011), holds that lowering barriers to exchange can increase economic activity in trading countries because it forces them to specialize in the production of what they're relatively best at (technically speaking, what they're relatively least bad at) and trade for what they're not great at producing.

Since the 1990s, as a result of US pressure on behalf of its IP industries (such as pharmaceuticals and motion pictures industries) (Drahos and Braithwaite 2002; Sell 2003), IP rights have become a mainstay of these agreements, but not because they encourage free flows of knowledge. Successive generations of trade agreements have ratcheted up levels of IP protection,

specifically to control knowledge flows. The stronger the rights, the more controlled the dissemination and the greater limits placed on knowledge spillovers that can lead to the creation of new knowledge and innovations. In free-trade circles, protectionism is a bad word, but strong IP rights are protectionist by definition. They protect the IP owner from competition and innovation while delivering them excessive profits, creating 'a kind of globalized guild system . . . a curious throwback to the early-capitalist era of mercantilism' (Dutfield and Suthersanen 2008, 11). As such, IP rights are something of a free-trade free-rider: accepted as part of these trade agreements even though they do not follow a comparative-advantage logic.

This guild system benefits, and was designed to benefit, those actors possessing large stocks of economically valuable IP. The inclusion of IP within the international trade regime, particularly through the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS, discussed in chapter 2) was the result of a strategic, concerted effort by successive US administrations dating to the 1970s to insert IP into the trade regime at a time when it was worried about losing its economic dominance to Asian upstarts (Sell 2003).

From the Liberalized Economy to the Franchise Economy

The inclusion of IP rights in trade agreements matters to more people than just IP and trade lawyers and the companies that love them. IP and other 'intangible assets' such as goodwill and tacit knowledge – essentially different forms of commodified knowledge – account for a larger proportion of the economy as a whole. Measuring the economic value of such intangibles is currently more of art than science (see Haskel and Westlake 2017, 5–7), but we have reached a point where investment in intangible assets now accounts for a higher share of sector value added than tangible assets (Haskel and Westlake 2017, 25). The 'proportion of corporate market value accounted for by' intangible assets 'is coming to dominate the value of many leading global firms' (Bryan et al. 2017, 60). 'For many high-tech and pharmaceutical companies, intangible capital now represents well over 90%' of market capitalization (Bryan et al. 2017, 61).

These numbers tell us that intangible assets, including IP, matter financially to companies. However, IP is even more important as a transformative form of control, an instrument of structural power. Globally strong protection of IP rights has given rise to the phenomenon of 'manufacturers without factories' (Bryan et al. 2017, 57). Consider the company, Nike. Ostensibly a shoe company, it does not actually manufacture shoes: it hires another company to do that. Or Apple, which may design computers, but which leaves its building to other companies. This control, over enormous distances and across international boundaries, is made possible by the existence of strong IP and

contractual rights. In the absence of strong IP and contractual rights, this type of control simply would not be possible, as there would be little stopping the contracted or outsourced manufacturer from copying and competing with the 'original' product.

The global economy is best understood now in terms of GVCs. GVCs are relationships between ostensibly independent companies in different countries that cooperate across borders to produce goods and services (Gereffi 2011, 2014). According to the World Bank, about half of world trade is comprised of trade within GVCs (World Bank 2020, 19). The expansion of GVCs, which took off in the 1990s, is closely related to the implementation of monopolistic global IP rights via trade agreements (Durand and Milberg 2020, 405).

If you're trying to visualize a GVC, it might be helpful to think of something a bit more familiar: a franchise, like McDonald's. As International Political Economy (IPE) scholar Herman Mark Schwartz remarks in an article that ranks as one of the most insightful analyses of the IP-driven global political economy, both GVCs (which he refers to as global commodity chains) such as the one run by Nike and franchises like McDonald's work on the same principle. A franchise-based company like McDonald's or the Hilton hotel company does not tend to directly own many restaurants or hotels. Instead, they use their IP rights, including its trademarks and trade secrets and contractual agreements to ensure that franchisees run their franchises just as the parent company desires while providing the head office with a significant piece of the action. From this perspective, there is little difference between Apple and McDonald's or the Hilton chain of hotels. As Schwartz notes:

> Qualcomm's [a US-based semiconductor company] 5% royalty on the sale price of smartphones, a fast-food franchise royalty of 6% of gross sales and Hilton's 5% royalty rate on gross room revenue are all the same strategy; Apple's near fanatical control over all aspects of its commodity chain parallels the de facto control fast food and hotel franchisors exert over their franchisees. (Schwartz 2021, 15)

This degree of control, and the control afforded to the lead companies in GVCs, would not be possible without globally enforceable IP rights. As Durand and Milberg note, 'GVC trade and stricter IPRs are mutually reinforcing' (Durand and Milberg 2020, 412). The protectionist global IP regime has allowed for the disaggregation of vertically integrated firms into formally disaggregated GVCs, in which control rests with the lead firm(s) and profits accrue primarily to those lead companies that control and license their economically valuable IP. This form of industrial organization reflects a 'franchise structure', in which the paradigmatic firms are McDonald's and Hilton hotels as much as Apple (Schwartz 2021).

The Global Economic Hierarchy

This GVC world is hierarchical. Schwartz (2021) divides this world into three layers. At the top of the hierarchy are those companies that control economically valuable IP. Such companies, such as Nike, perform very little manufacturing themselves. Instead, they coordinate production with other nominally independent companies by relying on their IP and contracts to set manufacturing conditions, taking a fixed percentage of the profits in return. IP-rich companies are thus able to shift fixed physical capital and labour costs onto other companies while using their IP defensively (e.g., via patent thickets) to pre-empt competition (Schwartz 2021, 3).

In the second layer, companies profit based on their control over physical capital-intensive assets and/or the possession of tacit knowledge that gives them an advantage over their competitors. Finally, at the bottom layer are companies engaged in labour-intensive manufacturing and services. With few barriers to entry, they seek profits through the hyper-exploitation of labour. Firms within a GVC, far from being independent, 'are often linked in a de facto integrated production process' across these three layers (Schwartz 2021, 16). IP-controlling companies tend to be in the driver's seat.

Winner Takes Most

This form of industrial organization has a significant effect on employment, income inequality and economic growth that is much different from the vertically integrated oligopolies of the production-focused 'Fordist' model. Where firms from this previous era (think automotive manufacturers) faced strong incentives both to invest and share that profit with their large labour forces, the franchise model of industrial organization does neither. Leading IP-based firms, with relatively small workforces, are largely content to reap IP-based monopoly profits while deploying the same IP to dissuade competition (e.g., through the possession of patent thickets, and using monopoly profits to buy up potential future competitors). As the proportion of IP-intensive firms at the top of the US economy has risen, measured by their share of gross profits, the capital expenditures of the top companies as a share of gross profits – the investments that fuel future growth – declined over that period from 74.5 percent in 1961–1965 to 45.8 percent in 2014–2018 (Schwartz 2021, 18, table 2). Second-tier firms themselves seek to achieve horizontal monopolies and avoid risks associated with excess capacity, also deterring investment. Meanwhile, third-tier firms are not able to produce either high-paying jobs or the investment needed to spur significant future growth. Taken together, 'this largely legal fissuring of industrial organization creates a vicious cycle in which weak investment inhibits growth, in turn dissuading firms from new net investment with strong multiplier effects' (Schwartz 2021, 3).

IP-intensive companies that drive the economy employ relatively fewer people. Mirroring the decline in capital expenditure as a share of gross profits, as the US economy has become more IP intensive, the share of employment of the top publicly listed companies in the United States (by gross profits), declined between 1961–1965 and 2014–2018, from 55.0 percent to 44.2 percent (Schwartz 2021, 18). Where previous forms of industrial organization, which were hierarchical and centred around manufacturing, invested heavily in the labour and capital expenditures that drove economic growth, a franchised-based economy does not. Taken together, these outcomes, which are often collectively described as 'secular stagnation', suggest that the global strong-IP regime is at least a partial driver of this phenomenon (Schwartz 2021; Döttling and Perotti 2019; Haskel and Westlake 2017, 91, 101).

The benefits from this form of industrial organization are unevenly distributed, accruing primarily to those companies in the first tier. IP-rich firms capture 'the lion's share of US and global profits' (Schwartz 2021, 2; see also Pagano 2014). More generally, the stronger IP regime has favoured the Global North, particularly the United States. According to Durand and Milberg, the United States in 2015 accounted for 38.4 percent of total international IP receipts. In 2016, meanwhile, industrial countries' IP receipts were over 100 times greater than those accruing to low- and middle-income countries (US$323 billion vs. US$3 billion) (Durand and Milberg 2020, 13).

Clearly, in this three-tiered IP-driven franchise model of industrial organization, it is better to control IP than not. As business professor Peter J. Buckley and his co-authors note:

> If some . . . GVC activities are owned or controlled by foreign MNEs [multinational enterprises], then a proportion of the value-added will not be retained in the countries in which it is generated but will accrue to the home countries of the MNEs (either as repatriated profits, or as management fees, transfer payments, royalties, etc). (Buckley et al. 2022, 11)

However, a community that merely hosts the branch office of a tech firm will not enjoy the same positive economic spillovers of, say, a manufacturing plant, for several reasons. First, while tech companies tend to pay their specialists very well, they also tend to employ fewer people than manufacturers. Income inequality becomes a problem as the tech sector accounts for a higher proportion of economic activity (Schwartz 2021, 17).

Second, IP turns knowledge into a proprietary asset. In doing so, it restricts the ability of others to use it to innovate – that is, it reduces the chances of the 'spillovers' that drive innovation when knowledge is allowed to spread, represented by the dissemination part of the production-dissemination

paradox. As former Blackberry co-CEO and prominent Quayside critic Jim Balsillie noted, 'You can only commercialize IP or data when you own or control them' (Balsillie 2018). What's more, IP-dominated firms themselves have a low marginal propensity to invest because IP can be used to stave off potential market entrants (e.g., via patent thickets), allowing them to collect monopoly rents via licensing and to use these rents to buy up nascent competitors (Schwartz 2021).

Third, because IP is an intangible asset, profits associated with it, such as licensing fees, can be easily transferred to the home jurisdiction or to a low-tax country (Linsi and Mügge 2019, 373; Durand and Milberg 2020, 422–23). As Haskel and Westlake note, intangibles like IP are 'often mobile; they can be shifted across firms and borders, which makes it harder to tax. Since capital is disproportionately owned by the rich, this makes redistributive taxation to reduce wealth inequality harder' (Haskel and Westlake 2017, 143).

Limited Understandings and Power Plays

For a policy instrument that has been around for centuries, the empirical record supporting strong claims that IP contributes to economic development or even the promotion of knowledge creation is inconclusive at best (e.g., Mazzucato 2018; Moser 2013; Boldrin and Levine 2007; Plant 1934; Towse 2013). What's more, even the logic of IP as a spur to innovation breaks down when IP protection is too easily granted or lasts too long. The TRIPS Agreement, for example, mandates a general minimum copyright term of the life of the author plus 50 years; in some countries, it's much longer (Mexico leads the world with a term of life plus 100 years). It's safe to say that hardly anybody makes decisions about anything, let alone whether they will write a novel or pen a song, based on what will happen 50 years after they're dead. Not only that, but most knowledge has a very short effective shelf life. After a certain point, expanding IP protections becomes ridiculous as an incentive to individual creation. They serve only to restrict dissemination in the interests of those who control existing economically valuable IP while impeding the creation of new knowledge by new inventors and creators.

We observe a similar situation with respect to patents. Summing up the research on the extension of patent monopolies – that is, making it easier to obtain patents – Breznitz notes:

> The results are clear and tragic. Patents tend to slow down innovation. That is, the more patents there are (especially patent 'families' that allow you to completely block competition in specific technologies by creating 'patent thickets'), the less innovative a technology becomes. This especially hurts new companies that try to work on follow-up innovation (which, we should remember, is the

> main way in which innovation positively affects welfare and increases economic growth). (Breznitz 2021, 142)

The situation, he adds, is not helped by the reality that patenting activity by all major patenting offices around the world exploded in the 2000s, to say nothing of the proliferation in trademarks, which set aside phrases, colours and even scents for the commercial use of individual actors, thus removing them from our common, uncommercialized repertoire (Breznitz 2021, 143). In other words, we are witnessing the equivalent of a land grab for knowledge of the kind we would expect of a knowledge-driven society.

We see similar issues with respect to the perverse effects of IP on international economic development. Recent research, for example, suggests that the long-assumed contention that strong IP attracts foreign direct investment (FDI) may be nothing more than a 'placebo effect' (Gold et al. 2019, 108). When it comes to attracting FDI, legal scholar E. Richard Gold and his co-authors find that one cannot determine the direction of the causal relationship between IP and FDI. That, almost 700 years after Vienna started issuing patents, 300 years after the first copyright statute and over 25 years since strong IP became a global standard in trade agreements, we remain highly unsure even about the direction of causality between economic development and IP laws, to say nothing of their actual effect or necessity as a spur to innovation, is a remarkable state of affairs.

THE BIGGER PICTURE: DIGITAL ECONOMIC NATIONALISM AND DECOMMODIFICATION

Even as trade agreements have become about much more than trade in goods, governments and trade experts continue to assess such agreements using computer models that are incapable of evaluating IP policies (Haggart 2022). This lack of quantification is one reason why highly protectionist IP continues to be a free-trade free-rider; its spread helped along by its association with the concept of free trade underlying international trade agreements.

The current global IP regime reflects a knowledge-feudalist logic. Knowledge feudalism is a dominant-state strategy preferred by those countries and businesses that already control significant economically valuable knowledge/IP. Unlike trade theories based on the principle of comparative advantage, IP is not designed to promote economic development but to capture economic rents and maintain control over economic activity. It is thus no surprise that the United States and its IP-based companies have been both the most vocal proponents and largest beneficiaries of the international strong-IP regime. Strong global IP rights have been a part of the official US National Security

Strategy since the mid-2000s, alongside such issues as nuclear weapons and military readiness (Halbert 2016). The United States sees strong IP rights as a primary means to ensure its role as the world's dominant economic power. This is not to say that the United States and US companies are the only actors pursuing a knowledge-feudalist logic. European countries, for example, have been the most vociferous proponents of geographic indicators as a way to insist that, say, carbonated wines produced outside of a tiny region in France can't be called 'Champagne'. In a knowledge-driven society, states and businesses have a strong incentive to seek to maintain and extend control over knowledge against any and all competitors.

It's certainly true that the effects on economic growth and innovation of intangibles like IP are very difficult to model (Dobson et al. 2017). The economic effects of IP are highly dependent on fundamental assumptions, such as a country's economic structure (Towse 2013).[8] The assumptions we make about them – for example, is research and development an investment or an expense? – will shape both policy and economic activity (Mazzucato 2018).

That trade-focused economic models can't accommodate IP is a reason to find new forms of measurement, not to ignore the problem. Thinking about IP in terms of its contribution to cross-border royalty flows – or transfers outside of a community – is one way to measure and assess over-dependence on IP controlled by other actors. In fact, this was the approach taken by the Canadian government up through the 1970s. Because Canada was a net-IP importer, Canadian officials looked with suspicion on proposals to strengthen IP. They saw stronger IP rights as a drain on the economy, payments to foreign companies that were not balanced off by relatively smaller IP royalty inflows (Haggart 2011, 241–42; Knopf 2018, 5–6). Alternately, governments' evaluation criteria could be even more blunt, focusing on who will control IP developed in a jurisdiction and the extent to which domestic individuals/businesses/governments will be able to access it.

IP rights – who controls them and who benefits from them – are not just about creating a revenue stream: they shape future growth and innovation possibilities. Care must be taken to not give away these resources at a discount.

Digital Economic Nationalism

In chapter 2, we noted that the main decisions facing the information-imperium state – that is, the key government and non-state (primarily business) actors as they relate to knowledge-governance policy – concern how to regulate the creation, dissemination and use of knowledge, including across borders. As one of the main tools regulating knowledge, IP rights are front-and-centre.

For knowledge feudalists who already control economically and socially valuable IP, the policy challenge is straightforward: to maintain their advantage by maximizing global IP protections and their enforcement.

Returning to our *leitmotif*, the Toronto Quayside project can help illustrate the difference between a knowledge-feudalist and digital economic nationalist approach to IP. Among other things, Waterfront Toronto and Sidewalk Labs wanted Quayside designed to serve as an incubator for smart-city IP that could be sold to customers around the world.[9] The hope of Canadian leaders, from Prime Minister Justin Trudeau on down, was that this development would put Toronto on the urban tech innovation map. Meanwhile, Sidewalk Labs, a spin-off of a company whose unmatched success is due to its control over intangible, commodified knowledge, fully appreciated the benefits to be had by controlling the IP that was to be developed using Toronto as a testbed for smart-city products and services.

Strong IP rights, however, can also lock people and companies into dependent relationships. Smart cities that run on proprietary, patent-protected technology risk this kind of lock-in, making it difficult to switch over to another technology, even if their current setup is sub-par. Strong IP rights of the type favoured by knowledge feudalists also restrict the knowledge spillovers that drive actual innovation. Stated most directly, people learn and innovate by building upon previous knowledge (i.e., by copying), and the greater the restrictions created by IP protections, the less that copying happens. From the IP owner's perspective, this reduced copying is a feature, not a bug, because the owner is then in a position to collect monopoly profits from those with whom they choose to share their proprietary knowledge. If you control economically valuable knowledge, it is in your interest to act like a knowledge feudalist, maximizing control and limiting dissemination.

In contrast, the digital economic nationalist response involves a coordinated attempt to generate economically valuable IP and to create first-tier companies capable of competing globally (and thus avoid being relegated to the lower tiers of the global economy). This effort can occur at the subnational, national or even regional level, as with the European Union. As we noted in the previous chapter, the digital economic nationalist response is a follower's response to knowledge feudalism, undertaken by actors who do not currently possess sufficient economically valuable IP.

In Quayside, Sidewalk Labs attempted to act like a knowledge feudalist, aiming to control as much Quayside-related IP as possible. This position was evident in a leaked design-procurement document in which Sidewalk Labs asked potential partners to sign over to Sidewalk Labs all rights to their technology designs' IP, including the right to commercialize that work worldwide (O'Kane and Bozikovic 2018). Where transferring IP was not possible,

Sidewalk Labs asked for 'an exclusive, royalty-free, worldwide license to use it' (O'Kane and Bozikovic 2018).

Quayside's critics, meanwhile, took a digital economic nationalist position. In terms of the protection-dissemination paradox, they were more concerned with disseminating knowledge, with securing access to economically valuable knowledge, than its protection.

Toronto's tech community and Canadian IP experts recognized that actors lacking significant stocks of economically valuable IP face the challenge of either breaking into Schwartz's IP-dominated top tier, otherwise adapting to the knowledge-feudalist regime, and/or working to shape the underlying rules. Toronto developer Julie Di Lorenzo, who resigned in protest from Waterfront Toronto's board in 2018 over its handling of the Quayside project, argued that Sidewalk Labs' language was 'completely inconsistent' with claims that the local tech industry would benefit from the project and was 'not conducive to innovation' (O'Kane and Bozikovic 2018). Similarly, 'prominent IP experts warn[ed] that Waterfront Toronto is not fighting hard enough to ensure that Toronto, Ontario and Canada get a fair share of the rights to Quayside's innovations' (O'Kane and Bozikovic 2018). Far from sharing in the Quayside bounty, the local tech industry feared they would essentially be relegated to piecework labour while Sidewalk Labs assumed a place in the top tier of the global knowledge economy.[10]

Digital economic nationalist policies, in general, tend to encourage sharing and a relatively less-protectionist approach to IP rights based on sharing *within* national borders, ensuring that, for example, the benefits of IP created in Canada remain in the country and do not flow to actors outside Canada. As the name suggests, such efforts are almost entirely national (or in the case of the EU, regional) in scope. For example, China, as the primary challenger to the United States' dominance, has been attempting, with what Buckley and his co-authors call 'remarkable' success, to move 'upstream' in GVCs, increasing its 'appropriation of intangible asset rents . . . from 6% of the global total in 2000 to more than 19% in 2019' (Buckley et al. 2022, 6).

Although it involves greater sharing of knowledge and openness to weaker IP rules, the objective of a digital economic nationalist strategy is the same as a knowledge-feudalist's: to ensure that a country's companies are as high up in GVCs as possible, creating a country of franchisors, not franchisees. However, as Breznitz (2021) notes, getting to the top of this mountain is immensely difficult, requiring skill, resources and the ability to overcome an IP regime designed to ensure that the summit cannot be conquered. His primary recommendation is that rather than chase the first-tier dream exclusively, communities should figure out how to innovate at the various levels of the global economy (which he defines somewhat differently from Schwartz (2021)) in ways that play to their strengths. Breznitz is certainly correct that

companies, regions and countries can successfully innovate even though the deck is stacked against them, but, as Schwartz notes, not all returns on innovation investment are equal.

Decommodification and the Limits to Digital Economic Nationalism

Digital economic nationalism is a logical response to knowledge feudalism's zero-sum game. It fails, however, to challenge knowledge feudalism's underpinnings, aiming instead to create the next generation's leading IP-based companies. At best, intra-country sharing of knowledge offers the possibility of domestic knowledge spillovers as local companies take advantage of easier access to knowledge to create more economically valuable knowledge. But it does nothing to address the disparities inherent in a knowledge-driven economy, nor does it do anything to address the resulting international disparities: it's an every-country-for-itself policy that can only recreate existing international inequalities.

For both the digital economic nationalist and the knowledge feudalist, the goal is to amass as much commodified knowledge as possible, with the digital economic nationalist also seeking to become a dominant IP power. As we noted earlier in the chapter, the IP regime is characterized by its commodification of knowledge. However, as Karl Polanyi reminds us, bad things happen if we forget that IP rights are a fictitious commodity: it turns the knowledge that is necessary for human existence itself into a product that can be ripped from its context.

Movement is possible: in May 2021, the United States, the dominant IP power, put its weight behind compulsory licensing for the Covid-19 vaccine. However, as Adyasha Samal, an IP expert remarked, 'Compulsory licensing cannot be seen as a tool so rare and exceptional that it takes 3 million deaths across the developing and the developed world to justify its use' (Samal 2021). At any rate, as of January 2023, entering the fourth year of the global pandemic, the issue remained unsettled.

In these challenges, however, we can perhaps see a way forward. The primary roles of the information-imperium state involve not only determining who can control knowledge but what limits must be set on this control. This second role recognizes Polanyi's key point about fictitious commodities: left to themselves, they will have pernicious effects on society. With reference to IP, these negative effects can take the form of stifled innovation or, more accurately, innovation that responds to the pre-existing, parochial interests of those who already control economically valuable knowledge. In culture, it can make it more difficult for artists, fearful of being sued, to create.

Unfortunately, the trend in IP policy internationally has been almost completely in one direction: more commodification of knowledge and higher levels of protection. Continuing this ratchet could well end in physical disaster. Even absent such apocalyptic scenarios, national responses to knowledge feudalism merely replicate and reinforce the geopolitical divisions that themselves contribute to an inability to confront global problems, like climate change.

Limits need to be placed on the further extension of IP rights. As we have noted, the evidence for their effects on economic growth and even creative output is surprisingly limited for policies that have been in place for centuries, to say nothing of the contribution of the currently high levels of protection to secular stagnation.

For all but the most dominant IP-based countries and companies, the fundamental interest in IP policy should be in limiting and rolling back protectionist IP rules or, at the very least, not expanding them. Such a move is, without question, a tall order. Strong IP rights, and the individualist, commodified ideology underlying them, are firmly embedded not only within international IP agreements but also within the trade agreements that underlie the global economy. The world's most dominant country, the United States, sees them as a matter of national security. Still, it remains that strong IP rights are a political, not natural or technological, creation. They are created by politics and can be undone by politics (Schwartz 2021).

We end this discussion about IP by highlighting how change could happen, both conceptually and concretely. Conceptually, one way forward involves re-emphasizing the dissemination side of the protection-dissemination paradox, rebalancing IP to make it less of a tool of the rent-seeking that is so harmful to economic growth, innovation and creative invention.

Another would be to look beyond IP to other forms of knowledge governance, which interpret this paradox in different ways, empowering different actors as possessors of knowledge, as well as promoting different values and outcomes. These include Indigenous forms of traditional knowledge (Desai 2007; Kansa et al. 2005; Rimmer 2015) that have been displaced by hegemonic IP discourses and practices. These also include knowledge practices within Western society: universities, for example, are devoted to the creation and sharing of knowledge. Different ways of regulating knowledge are possible.

Concretely, decommodification of knowledge could involve recognizing and taking seriously the idea that some forms of knowledge should not be commodified. Allowing for compulsory licensing of medical goods during a pandemic is an example of this thinking. However, as noted earlier, such licensing should be more routine and easier to achieve. Climate-change mitigation technologies are another specific area where dissemination should trump protection interests (Drahos 2021). Rather than hoard planet-saving

technology behind patents, countries could agree to make cleantech patents available via a compulsory licence available at a reasonable rate. That way, innovators would get paid and those who need the tech would be able to access it. Treating climate change–related patents as a global commons, meanwhile, would help mitigate digital economic nationalism's reproduction of the harmful geopolitical divisions that reduce our ability to cooperate internationally to address climate change.

CONCLUSION

IP rights have emerged as a significant form of structural power in the global economy. Consistent with what we would expect from the rising dominance of the knowledge structure, production outcomes are now largely determined by IP rules – that is, knowledge regulation. Whether one is negotiating the IP chapter of a trade agreement or the licensing terms of a municipal smart-city project, IP treaties, laws and agreements shape communities' future economic prospects, and their ability to access the technologies and knowledge needed to develop cities and communities in ways that allow individuals to reach their full human potential. The first step toward more-human IP rules involves recognizing the importance of IP and acting accordingly.

NOTES

1. Legal scholars will note that, formally, IP protects the expression of an idea rather than the idea itself. We contend that, in practice, this is usually a distinction without a difference: forbidding someone from copying a drug formula or a movie is tantamount to restricting the circulation of the ideas contained within the work in question.
2. Breznitz (2021) forcefully makes this very point.
3. Provisions criminalizing trade secret violations that were included in the 2018 revisions to the North American Free Trade Agreement among Canada, Mexico, and the United States further attest to their rising importance. Trade-secret violations tend to be seen as civil matters. Their elevation to the level of a criminal act, in what is regarded as the current bleeding-edge IP treaty (de Beer 2020), suggests that trade secrets are being taken very seriously indeed.
4. Thanks to Herman Mark Schwartz for this point.
5. This section focuses primarily on economic control but copyright can also be weaponized to limit the dissemination of speech that the rights holder disagrees with for non-economic reasons. As Halbert (2019) documents, in the United States, copyright law has been used to remove hate speech on YouTube that, while offensive, is not illegal under US law.

6. In 2005, Canada's copyright term was life of the author plus 50 years. In 2022 it was extended to life plus 70 years as required by the 2018 United States-Mexico-Canada trade agreement.

7. For example, our framework combining Strange and Cox is based on a suggestion found in May (1996) that such a combination could be fruitful.

8. Here Towse is speaking about copyright, but her point holds for IP generally.

9. As Sidewalk Labs CEO Daniel L. Doctoroff noted in testimony before the Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics, 'we'll hopefully develop a small group of products that would be operational here, which we think have the potential to be taken beyond Toronto into other markets around the world' (Doctoroff 2019).

10. Serving as a reminder of the politically contested nature of IP rights, near the end of the Quayside project's troubled life, as Waterfront Toronto and Sidewalk Toronto attempted to negotiate a way forward in what had become a difficult relationship (O'Kane 2022), the two organizations agreed in November 2019 to share a 'to-be-determined percentage of revenues' from technologies piloted in Quayside. It also would have granted 'Canadians access to Sidewalk patents registered globally, instead of just those registered in Canada', as originally proposed. This concession would have meant that local companies could have built upon Sidewalk innovations without fear of facing infringement claims (O'Kane 2019b).

While this digital economic nationalist–friendly concession would have at least somewhat thwarted Sidewalk Labs' knowledge-feudalist ambitions, and while they were welcomed by local IP experts (O'Kane 2019b; 2020), they came very late in the game, following pressure from activists and experts.

Chapter 4

Demystifying Data

The knowledge economy relies fundamentally upon the ubiquitous surveillance of people, objects and their environments, based on the idea that the more detailed data amassed, including personal data, the more value accrued. In fact, anything less than total surveillance is seen as a deviation from the logic of the market since data that is not observed and measured cannot be monetized. (The same logic holds for states that pursue ever-greater surveillance in the name of security.) Corporate actors have commercial interests in extracting insights from data that they perceive may have economic value. Governments collect and interpret data from state bodies, including statistical organizations, security intelligence agencies and health departments, and purchase data insights from companies that are intended to facilitate the delivery or management of government programmes. Civil-society groups also accord value to data, for example, undertaking campaigns to crowd-source data to identify government corruption, organizing population counts of wildlife or using sensors to measure pollution or industrial noise levels. The economic, social and political value that governments and non-state actors, both companies and civil society, accord to data is emblematic of the information-imperium state, for which control over knowledge is central to the exercise of power. Those who wish to lay claim to this power, however, must possess the resources and capacity to collect and interpret data, which typically requires technical expertise to deal with large volumes of data.

In our knowledge-driven society, the word 'data' is almost talismanic, often evoking fear and awe more than understanding. It doesn't help that there remains great confusion about how data should be treated. As political scientist Dan Breznitz remarks,

> The reality is that we do not even have a decent understanding of how data should be used, who should use it, what technologies it might spawn, who

> should regulate it, who it should be regulated for, or how it should be regulated. (Breznitz 2021, 175)

This chapter is designed to clarify some of the foundational concepts needed to think through Breznitz's questions and to understand the data-driven economy and society that we explore in the remainder of the book. Much of this chapter follows from what we discussed in chapter 1, since data is merely a particular form of knowledge. However, that the concept of data has begun to assume almost mystical powers makes it necessary to describe and define data directly. In particular, we highlight how control over data is a key means of exerting power in a knowledge-driven society.

The economic and social importance that the information-imperium state accords to interpreting data and companies' search for commercially valuable data are evident, to take one example, in the wide variety of fitness and health apps and data-collecting wearables that measure nutritional intake, exercise, sleep and heart rate. Commercial actors that design hardware and software to capture and quantify bodily data promise users accurate, reliable and, crucially, actionable health knowledge that users may employ to address current medical conditions, as well as detecting and perhaps deterring future health problems. Digital sociologist Deborah Lupton (2016) and others refer to this phenomenon as the 'quantified self'. With the real-time monitoring of bodily data, the thinking goes, people will be able to better understand and manage their health. Users are encouraged to take charge of their bodies, changing diet, exercise and health management based on tips from the apps or wearables. However, these individual-level choices of modifying diet or stress levels are often wholly inadequate for people facing complex or chronic health problems, those without access to health professionals or those who face structural obstacles of poverty, racism and discrimination (see, e.g., Lupton 2017).

The commodification of bodily data is particularly evident in the 'femtech' market, a broad array of apps and services devoted to monitoring fertility, menstruation and pregnancy, as well as nutrition, fitness and sexual wellness (see, e.g., Thomas and Lupton 2016; Corbin 2019). Menstrual-tracking apps, such as the popular Flo, Glow and Clue apps, ask users to record their sex drive, diet, moods, the state of their skin, workouts, constipation, cervical mucus quality, masturbation frequency and basal body temperature to identify ovulation. If users become pregnant, they are encouraged to enter details of their sleep, diet, emotional state, weight, the appearance and colour of their cervical fluid, and even when and in what positions they have sex. Information collected on birth includes birth type, length of labour, birthing complications like haemorrhage and in the case of pregnancy loss, the date and type of loss, like whether the baby was stillborn (Harwell 2019). Data collection intensifies after birth as parents can monitor babies and children throughout their

childhood, including using sensor-embedded clothing to monitor infants' respiration, pulse rate and blood oxygen levels and set alarms to detect any irregularities to heartbeats or breathing (Bonafide et al. 2017).

Health technologies like fitness or menstruation apps can be useful tools, but our point is that the purposes and processes of data-collection matters: not all data-collection efforts are necessarily beneficial. In the case of data-driven health technologies, for instance, the shift towards quantifying health has introduced 'a host of new challenges and limitations, such as new selection and other types of biases' (Sharon 2018, 2). Wearables, for example, have had difficulty measuring heart rates in people with darker skin as the optical sensors work better for paler skin (Hailu 2019). Apps and wearables may not be able to capture measurements precisely or universally, and ordinary users may not appreciate the difference between advice from qualified medical professionals and app-derived health advice. There are also critical questions of privacy and individual consent, as some companies like Amazon are requiring employees to use wearables to track worker productivity in warehouses or, in the case of the trucking and construction industries, worker safety. The data economy's imperative is to exploit data, even sensitive health data. This practice is evident in the US Federal Trade Commission's finding in 2021 that the fertility app Flo misled users about its disclosure of users' health data to Facebook (Federal Trade Commission 2021b). The commodification of health data poses additional security risks in the wake of the US Supreme Court's overturning of *Roe v. Wade* and subsequent criminalization of abortion in many states as privacy experts warn that law enforcement could use app data to identify users within or even transiting through the United States whose pregnancy starts and then stops (Hu 2022).

Data is a core constituent element of 'smartness', whether for health technologies, the algorithm-driven gig economy or smart cities. In the case of smart cities, data is integral to delivering the seamless integration of digital and physical infrastructure and the responsive delivery of services like transit, energy, waste disposal and communications. To integrate infrastructure and provide essential services, data-collecting sensors enable 'ubiquitous trackability' of people and objects within the urban environment (Koops 2014; cited in Edwards 2016, 39). For those with a technological solutionist mindset, data is also regarded as an essential component to solving even intractable complex social problems such as unaffordable housing or deteriorating infrastructure (see Kitchin 2014b; Morozov and Bria 2018).

Technology vendors tend to portray smart cities as a way to 'rationalise the planning and management of cities' (Shelton et al. 2015, 13) through the pervasive accumulation and application of data (see Kitchin 2014b; Sadowski and Bendor 2019). In the designs for the ill-fated Quayside neighbourhood that was pitched as the most advanced form of the smart city, for example, Sidewalk Labs proposed heated sidewalks, autonomous vehicles, self-driving

garbage bins and package-delivering robots. These plans were data intensive. Sensors in sidewalks would be responsive to weather, activating heaters when cold wet weather is detected. Self-driving garbage bins' volume sensors would detect when bins should be emptied, while their optical sensors would enable them to move to disposal centres to empty themselves (Sidewalk Labs 2019d, 79). Another set of sensors, designed to regulate mobility within the neighbourhood, would collect data on the presence of pedestrians and cyclists, vehicle and bicycle volume and speed, with real-time monitoring of the locations of app-connected taxis, ride-hail vehicles, bicycles and electric scooters to optimize transit usage and provide real-time information on weather and traffic conditions (Sidewalk Labs 2019d, 50).

Data collection and even surveillance are natural human activities necessary for any functioning society, whether in addressing transit problems or improving maternal health. Problems arise, however, depending upon how surveillance is undertaken and by whom, how the data is treated and who benefits from the surveillance activities and who bears the risks. Public health surveillance undertaken during the Covid-19 pandemic, for instance, again demonstrated that racialized people and those who are marginalized often experience disproportionate levels of state surveillance in comparison with other populations with similar behaviour. In the United States, studies of those arrested for violating Covid protocols, such as social distancing requirements, found that those arrested were disproportionately Black or Latinx (Sundquist 2021).

Data is necessary for sound policymaking, but accessing data in a usable form can be challenging, not just technically but also politically. This challenge was evident in a legal battle over health data between the provincial government of British Columbia, on Canada's west coast, and a coalition of Indigenous Tribal Councils. Indigenous leaders from these councils demanded access to Covid-19 datasets collected by provincial health authorities pertinent to their territories so that they could determine the necessity of stay-at-home orders and resource sharing with other Indigenous nations, arguing that without detailed case counts and locations they 'are working blindfolded' (Slett and Sayers 2020). The province repeatedly denied these requests, stating that sharing the data would violate privacy laws (The Canadian Press 2020). This case clearly shows the power of being able to control, interpret and make decisions using data. In this case, Indigenous leaders claimed that the BC government's actions reflected 'a colonial refusal to share information' (Slett and Sayers 2020).

Data, as these examples show, has emerged as a flashpoint for widespread concern over governmental and corporate power. To explore how data has become a means of exerting power in a knowledge-driven society, this chapter first offers a definition of data as an entirely human-constructed form of knowledge. It then briefly considers two different types of data, personal and

non-personal. Then, it offers a sketch of our current data-driven economy and society. Building on the eight ground rules for understanding knowledge that we explored in chapter 1, it highlights eight key characteristics, and one inconvenient truth, of the data-based society as it currently exists.

DEFINING DATA

As chapter 1 laid out, data is a form of knowledge. Often, data is used interchangeably with 'information' or is treated as a building block for knowledge, which is seen as involving a deeper, more complex understanding of the world. Our decision to equate data with knowledge is designed to highlight the fact that data itself is created by human action. It involves an interpretation of an underlying or not-wholly-accessible reality, which we term information, the real 'raw material' from which data is created.

Data can never give us a full picture of reality. It is always and everywhere shaped by our necessarily limited modes of perception and our decisions about what aspects of a particular phenomenon to observe, capture (as data) and interpret.

More precisely, data is the knowledge that data collectors perceive as somehow valuable, interesting or worthy of collecting and using. Makers of fitness wearables, for example, decided that measuring users' sleep patterns and daily activity levels provides useful data about users' health. However, many wearables and fitness app companies initially did not capture data about pregnancy or nursing, an oversight that likely reflects the male-dominated software development industry, but also aptly highlights how data creation is a partial representation of reality (Conditt 2019). Because human decisions about the value of certain information result in the generation of data, there is no such thing as 'raw data' (Gitelman 2013, 2). Data must 'be imagined as data to exist and function as such' (Gitelman 2013, 3). In other words, data does not exist independently from human actions, and once collected, data must be interpreted for it to have meaning and value.

Two Types of Data: Personal and Non-Personal

Personal data generally attracts the greatest media and policymaker attention, as evidenced by the recent spate of data-protection laws in countries worldwide in the last several years. This attention is unsurprising considering the harm that can result from the leaking or theft of people's sensitive personal data, but personal data is only one category of data, the other being non-personal data. Non-personal data covers things such as data observed from industrial processes like the manufacture of pharmaceuticals or commercial

buildings' tracking of energy and water consumption and presents its own set of policy challenges.

Personal data relates directly or indirectly to an identifiable individual. The EU's General Data Protection Regulation (GDPR), which came into force in May 2018 and which is generally seen as the world's most developed form of data regulation, defines personal data as 'a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (European Parliament 2018 Art 4(1)).

Personal data is a category that includes data from a variety of sources. A primary source is user-submitted data (often referred to as *volunteered* data) that people generate when they use fitness wearables, gig economy applications like Airbnb or Uber, or social media platforms, or when they access online government services. 'Volunteered' is something of a misnomer, as people may have few options but to provide personal data to access necessary products and services.

Personal data also includes *observed* data, which captures individuals' actions and behaviour, such as the collection of geolocational data from public transit use or from cell phones. Even more indirectly, personal data can be *inferred* by analysing other data to create inferred data. Credit scores are a common – and highly consequential – form of inferred data. Financial institutions construct credit scores by analysing an individual's income, spending habits, debts and other information to build a profile of their creditworthiness (Lauer 2017).

In a society in which data is a commodity that can be bought and sold, it is very difficult – and in the absence of regulation practically impossible – for individuals to understand how the data that they volunteer, or that is collected via observation, is used. Data freely given for one purpose – for example, data collected in the course of a job application or a DNA test to trace one's family tree – can become inferred data used for different or previously undisclosed purposes, such as whether an individual (or others deemed via data analysis to be like them) qualify for life insurance.

In contrast to personal data, and as noted earlier, non-personal data is a category that covers a vast range of information, including weather and environmental conditions, as well as industrial activities. The gas and oil industry, for example, relies upon sensors to detect pipeline leaks, and shipping companies track vehicles and packages in real time. Similarly, medical systems may rely upon internet-connected monitoring, diagnostic and treatment devices to share data among healthcare providers and insurers (DeNardis and Raymond 2017). From an industry perspective, data-driven tools like the sensors discussed here are perceived to be essential to making businesses more effective and productive as they can capture data that may be

used to reduce waste in production processes or identify possible new product lines (see Srnicek 2017).

While personal data raises privacy concerns, non-personal data presents a separate set of policy challenges, primarily related to data control and ownership. Entities, usually corporations, with the technical and commercial infrastructure to collect and extract meaning from data can leverage the skills to dominate industry sectors or to make a private corporation that collects this data indispensable to, say, a municipal government that wants to understand traffic patterns for planning purposes. For example, as chapters 6 and 7 explore, companies may establish data monopolies designed to crowd out other actors that depend on access to data for their own activities. A growing business for big agricultural firms like John Deere is capturing farm data – from sensor-studded tractors driven by farmers – and then selling to farmers insights such as soil or harvesting conditions. Traditionally, farmers painstakingly collected this information themselves, viewed it as a form of traditional knowledge about their lands, crops and livestock, and treated it as proprietary property important to farming as a business. In the data-driven economy, however, companies, not farmers, largely control agricultural data at the cost of farmers' autonomy and in a manner that increases the structural power of big agri-data firms in the agricultural industry over other industry actors, as chapter 7 explores.

Addressing these challenges, including whether to promote such monopolies for favoured domestic industries and how to limit the harms resulting from such control, is a key challenge for the information-imperium state.

The Datafication of Everything

It's readily apparent in everyday life that more types of data are being collected from people, objects and the built environment than at any time in the past. Two key drivers of this phenomenon are digitization and datafication. Digitization is the conversion of information into binary code readable by computers. Datafication, a term popularized by scholars Victor Mayer-Schönberger and Kenneth Cukier (2013; see also van Dijck 2014), entails capturing a phenomenon in a quantified data format so that it can be recorded, analysed and accorded value. Datafication 'necessitates a desire to quantify and to record' (Mayer-Schönenberger and Cukier 2013, 78) a wide range of phenomena that formerly weren't captured or measured as data. Locations of people and objects are now routinely tracked: for example, internet-connected thermostats gather data on the detected motion within a residence, ambient light levels, temperature, humidity, heating and cooling usage, and carbon monoxide and smoke levels. Human experiences and interactions are a particular focus, as datafication also involves the process of

quantifying social interactions into data to make inferences about behaviour, largely for commercial purposes (see van Dijck 2014).

Just as more phenomena are being datafied, there is a growing array of actors involved in the collection, storage and use of data. Intensive data collection used to be the exclusive purview of states through tools like the census. Now, however, civil society, for example, can work with governments or industry or act alone to collect data on any number of issues, from pollution levels, populations of migrating birds and incidents of government corruption to the number of children travelling to school by bicycle.

Some data may be shared between governments and the private sector, but there are often legal restrictions on sharing specific state-collected data, especially data in sensitive areas like health, taxation or security. This, however, is not always the case. As we discuss in chapters 6 and 8, companies and governments have become increasingly interdependent in their data practices. This interdependence is captured by the concept of the information-imperium state which involves both state and non-state actors as key decision-makers who not only compete but also cooperate in the exercise of structural power. With different actors involved in the collection, processing and use of data, it can be difficult to distinguish public-sector data from private-sector data, further complicating data governance.

The growing centrality of data to the global economy is evident in what scholars alternatively term 'data capitalism' (West 2019), 'surveillance capitalism' (Foster and McChesney 2014; Zuboff 2015), the 'information-industrial complex' (Powers and Jablonski 2015), 'platform capitalism' (Srnicek 2017), 'informational capitalism' (Cohen 2019) and the 'sensor society' (Andrejevic and Burdon 2015). Common to these concepts is the identification of a massive expansion of surveillance systems and data-collection practices, as well as a focus on control over data. For corporate actors, datafication typically results in business models built upon the commodification of data, undertaken through contractual terms-of-service agreements and under the protection of intellectual property (IP) laws. Companies prefer to treat the data they collect as proprietary, from which they will extract value, even when the data originates in the public realm. Companies' practices of capturing the lion's share of accrued value over data can be understood as what Science and Technology Studies scholar Kean Birch terms 'data rentiership', which entails the transformation of data into an asset, that is, the 'assetization' of data to extract value from data (Birch 2020). Concepts like data rentiership and assetization are part of a broader scholarship that emphasizes the proprietary control over the accumulation, ownership and interpretation of knowledge, including IP (see, e.g., Drahos and Braithwaite 2002). Before being monetized, however, actors must identify and capture as data the information that they believe is of potential economic or social value, as we describe further next.

Data Is Political

Data does not exist independently of people. The processes by which information is conceptualized as data to be collected, stored, processed and used are inherently political. A full understanding of data requires a focus on human actors and the power relationships at play in how we understand and use data. Decisions about the production and use of data are subject to power struggles. Equally importantly, 'data is generative of new forms of power relations' (Bigo et al. 2019, 4).

Decisions to collect and use data are undertaken within specific thought systems that set out what data is determined to be valuable and what devices and technologies will capture that data (Kitchin 2014b, 9). In other words, how we understand data is 'framed technically, economically, ethically, temporally, spatially and philosophically' (Kitchin 2014a, 3). As Science and Technology Studies scholar Yanni Alexander Loukissas (2019, 14) notes, data is not universal. Data does not necessarily 'travel' well: data practices and data themselves differ from one context to the next. Tech companies that operate transnationally, for example, may also transfer or store data outside the country in which it was collected. Governments, however, may want to have data stored and governed within the jurisdiction of collection for reasons of national security or to boost the domestic data economy, thereby conflicting with big tech companies. In response, tech companies like Tencent, Alibaba, Amazon, Microsoft, Google and Facebook have heavily lobbied countries, including India or Indonesia that were considering rules that would require data to be stored within the country of collection (i.e., data localization rules) that would conflict with companies' preferences on transnational data flows (see, e.g., Basu et al. 2019). As debates over data localization (a topic we explore in more depth in chapter 9) show, local context matters. There are always a politics and a culture at play.

DATA'S EIGHT CHARACTERISTICS

Data requires human deliberation to conceptualize the collection of particular information as valuable or important, such as people's gaits, facial expressions or real-time locations of public transit vehicles. In other words, data is subject to politics, and the laws and norms shaping the identification, collection and use of data reflect the historical, social, political and economic influences of the era. Our current data-intensive economy and society are no different, reflecting specific state- and market-based interests and rationalities driving and shaping the mass accumulation and the use of data. With this in mind, we now turn to data's eight characteristics and one inconvenient truth.

Characteristic 1: Data Is Not Neutral

One of the most pernicious assumptions at play in policy circles is the idea that data is objective, untainted by human norms or bias. Relatedly, technicians and engineers who design and build data-collection and data-intensive technologies often portray themselves as somehow separate from how their creations are used and from the ensuing consequences.

As we explained in chapter 1 and as scholars from critical data studies and Science and Technology Studies have long pointed out, data is not neutral (see e.g., Kitchin 2014b). How we understand and treat data, including decisions to monetize personal data, reflect specific social, economic, legal and technological ideas within particular societies (see Kitchin 2014a). As the following chapters discuss, states and private actors, particularly large corporations, understand and treat data in ways that reflect specific mindsets.

Bias can be entrenched within the design and operation of technology, thereby affecting what information is considered data and how it is used and valued, as well as what populations are deemed more necessary for intensive monitoring. Scholars and activists have long highlighted bias and discriminatory features designed into software, particularly anti-Black racism (Daniels 2013; Noble 2018). For example, automated speech recognition systems developed by companies like Amazon, Apple and Google have been found to be more accurate in identifying voice commands from native English speakers in the United States than speakers with non-native English accents, and the assistants also have a racial bias in understanding African American speakers compared with white speakers (Koenecke et al. 2020). This 'accent gap' (Harwell 2018) highlights a lack of diverse voice data in training datasets. More broadly, software accuracy problems and lack of training dataset diversity reflect institutional decisions about what data, populations and technologies are considered more commercially important than others.

Characteristic 2: Data Is a Product

The collection and use of data are fundamental to the proper functioning of software-facilitated products and services. Automatic thermostats, for example, can only work if they can measure the temperature in your house; sensors designed to measure soil moisture need to detect moisture levels. Such data is valuable, and not only because it allows the thermostat to regulate the temperature. Data has become valuable, in and of itself, as a product separate from its purely instrumental purpose. Business models built upon data extraction have become increasingly common, collecting and parsing vast amounts of data from their users. The 'platform' – companies such as Uber, Google, Facebook and even industrial companies like Rolls-Royce, which embed sensors in their

products to track their usage – are designed explicitly around the imperative of collecting as much data as possible (Srnicek 2017).

From the user's perspective, utilizing 'Google maps or hitting the "like"-button on Facebook . . . are not motivated by the intention to produce data, but rather to get directions and to signal approval respectively' (Grabher and König 2020, 105). This is not how companies see things. As Andrew Ng, founder of Google Brain project and former chief scientist at China's Baidu, explains, in a data-driven economy, tech companies 'launch products not for the revenue but for the data' and then 'monetize the data through a different product' (Lynch 2017).

Data, for them, is a fictitious commodity, to use Polanyi's term. Data is not 'produced for sale', but is 'brought to market' (that is, commodified) by companies. The problem with data as a fictitious commodity is not the fact of data collection – you need to provide your location to get Google Maps to get you to your destination, after all, and we want our sensor-operated thermostat to turn the furnace off when our room reaches a certain temperature – but rather when it is repurposed away from the reason for which it was produced. This repurposing is done not in the interest of the individual, but of the actor employing the data for another product or service. By commodifying their users' personal data, companies produce 'surveillance assets' to generate revenue with the goal of influencing and predicting consumer behaviour (Zuboff 2015, 81; see also West 2019). Seen in this way, Google Maps is not a map app but a data-collection mechanism that looks like a map (Zuboff 2019). The purpose of the app is to collect data; the service delivered is a means to an end. Music-streaming services like Spotify deliver 'listening as a service' in which the listening audience is commodified. Nor is this data-based platform economic model limited to the online space. For example, an executive with Vizio, a California-based television manufacturer, said that customers can opt out of data collection, but that if they did so, companies 'would have to charge higher prices for hardware if they didn't run content, advertising, and data businesses' (Patel 2019). Commodifying data, as this statement makes clear, is at the heart of the Vizio business model.

Characteristic 3: The Centrality of the Proprietary Control of Data

Closely aligned with the treatment of data as a commodity is the impetus to retain proprietary control over data – to keep it within the organization, so that the organization can extract the maximum amount of value. Simply put: 'Whoever controls data, controls the world', an oft-quoted statement popularly attributed either to Jack Ma – former chair and one of the founders of

Alibaba Group, a tech giant in China – or Masayoshi Son, CEO of the Japanese internet, energy and financial conglomerate SoftBank Group (Pfluger 2019). The business models of traditional manufacturers are shifting to emphasize monetizing data. John Deere, for example, is not only one of the largest manufacturers of agricultural equipment. It is also a data analytics company that sells access to data on soil and crop conditions.

Typically, proprietary control over data is contrasted with open-data frameworks, in which data is publicly accessible for anyone to use. However, open-access policies are not a panacea when it comes to issues of control. It takes skill and resources to process and use data, no matter the sources. Larger companies, with human resources and advanced technical infrastructure, including data analytics capacity, possess advantages over start-ups lacking these capacities. Google, Facebook, Amazon, Tencent and Alibaba are amongst a new generation of actors whose business models focus on the accumulation and monetization of data. Those who 'are able to collect data from multiple sources, aggregate it, and do innovative things with it' (Mayer-Schönenberger and Cukier 2013, 135) benefit economically from data and, equally importantly, the authority to create rules regarding the use of the data.

Beyond companies, states have long sought to monopolize data collection, analysis and use relating to the populations within their territories, linking the control over data with state sovereignty and, thus, control over their territory (Kitchin 2014a; Ruppert et al. 2017). State monopoly on data production, however, has been increasingly challenged by companies active in data collection and analytics. As chapter 8 explores, states may work with private actors who provide the hardware, software or data expertise to monitor populations or deliver services such as social assistance or protection of at-risk children. In other situations, governments may have interests in maintaining a 'monopoly of interpretation' (Baack 2015, 4), in areas of strategic interest to the state, such as national security.

Characteristic 4: The Surveillance Imperative

Data must be observed to be created and collected. The rising importance of knowledge in the form of data to the economy and all facets of social life necessitates constant surveillance of people, objects and their environments, whether to maximize state or personal security or to maximize profits. While individuals, companies and states have always engaged in data collection, the ubiquitous nature of surveillance has changed its goals and effects. Traditionally, surveillance has been understood as 'purposeful, routine, systematic and focused attention' intended to control or manage specific individuals or populations, such as who pose a risk to public safety (Lyon 2015). Now, however, surveillance is increasingly being broadened from focused attention on targeted individuals to systems of pervasive continuous surveillance.

The objective of surveillance in such a 'sensor society' is to capture 'a comprehensive portrait of a particular population, environment, or ecosystem (broadly construed)' (Andrejevic and Burdon 2015, 23) to enable the identification of patterns in data to understand and, more importantly, anticipate actions to predict consumer behaviour and, for state actors, to monitor and control populations.

Both states and corporate actors in the knowledge society are driven by the ubiquitous surveillance imperative. From social media platforms and smart cities to software-enabled Internet of Things (IoT) products, companies have increasingly adopted business models reliant upon the normalization of pervasive, continuous surveillance of consumers, as chapters 6 and 7 explore.

With respect to national security, while China is the paradigmatic example of state surveillance with its systems of online and real-world surveillance, all states have interests in surveilling and controlling their populations, as chapter 8 argues. As the US global surveillance system revealed by Edward Snowden demonstrated (Schneier 2015; Lyon 2015; Greenwald 2014), such surveillance is not unique to authoritarian countries but is evident in all countries that define security in terms of the amount of data to which one has access – that is, countries that embrace the logic of the information-imperium state.

Characteristic 5: Data Collection Is Speculative

The drive towards total surveillance is complemented and reinforced by the assumption, or belief, that the value or use of some data may only become clear in the future. Such data is seen as useful not only for the development of new products or services but also in terms of safeguarding national security. This perspective introduces, in turn, a bias towards data overcollection, lest you miss out on data that later turns out to be valuable. Or, worse, that someone else collected that now-useful data.

As a result, data-intensive companies tend to operate with a 'collect-it-all' mentality, with the goal of generating 'new patterns of correlation' that can be repurposed indefinitely (Andrejevic and Burdon 2015, 23–24). This data-maximalist attitude is complemented by a drive to maximize surveillance, to minimize privacy and to engage in expansive data-collection practices that amass more data than required for the effective operation of current products and services, often without the knowledge or consent of customers. Data-maximalist mindsets are evident in Silicon Valley's 'move fast and break things' ethos, which condones, among other aggressive business practices, the all-encompassing collection of data even without users' permission with the idea that specific uses will be determined later.

Google's attempts to map the world offer a particularly egregious case of this collect-it-all (no matter the legality) mentality. Between 2007 and 2010,

Google deployed Street View mapping vehicles around cities worldwide, capturing panoramic digital images of neighbourhoods and collecting Wi-Fi network data to provide location-based services like mapping (Federal Communications Commission 2012). Google also illegally captured the content of internet communications, including email and text messages, and passwords. Over a dozen countries investigated Google for violation of their privacy laws. Google belatedly admitted to the US Federal Communications Commission that the illegal data collection was a 'deliberate software-design decision' made by Google engineers working on the Street View project (Federal Communications Commission 2012, 2). Illegal data collection in this case was not a bug; it was a deliberate decision to collect potentially valuable information to create new products.

As chapter 8 examines, states also exhibit data collection–maximalist tendencies typical of the information-imperium state. Recall that the information-imperium state is characterized by an overarching emphasis on the capture and control of knowledge, in this case data. National security is a particular focus of states' speculative, future-oriented, data-driven surveillance. US national intelligence agencies, for example, call upon the private sector for ways to improve facial-recognition technology, especially by strengthening identification with other technologies, including 'whole-body identification, gait recognition and/or anthropomorphic classification (e.g., height, gender)' (Kimery 2019). The drive towards ubiquitous data collection is not just a characteristic of state security services but of the state as a whole, in the name of delivering services like health, immigration and social assistance programmes.

The speculative, data-maximalist approach characteristic of the information-imperium state and the data-driven society stands in stark contrast to calls for a 'data-minimization' approach to commercial and state activities. Such an approach calls on organizations to collect, use or share only the personal information that is necessary for the purpose at hand and not to collect and use personally identifiable information if other information could serve the same purpose (Cavoukian and El Emam 2014, 4). While the data-minimization approach is intuitively appealing because it is designed to maximize user privacy, its implementation, like the exhortation to reduce IP protections to encourage innovation and cultural creation and consumption, is a hard sell in a world in which the control over data is a key element of political, economic and social power.

Characteristic 6: The Presence of Asymmetries of Knowledge

Anyone who has been surprised by the Instagram ad that appeared in your feed advertising a TV show that you'd been talking about with your friends

or felt queasy about the data profiles that data-hungry social media platforms have created about you intuitively understands the chasm between ordinary users and data collectors. This gap, which some scholars term 'asymmetries of knowledge' (West 2019; Zuboff 2015, 2019), refers to the difference between what data companies know about their users and how little people know about how these companies use their data. 'Data-poor' actors have little understanding of the inner workings of data actors' data-collection capabilities, how or where data is stored and used, and the short- and long-term consequences of data commodification and monetization (Andrejevic and Burdon 2015). Even when data may be freely available, such as when a city provides open data on public transit, data-poor actors often do not have the expertise or resources to make sense of or use such large volumes of data.

Here, it's important to understand that bits of data on their own – say, data collected on an individual – have little value. It's only when that data is collated with many other data points into large datasets that it becomes valuable.[1]

'Data rich' actors, in contrast, are large commercial, academic and government bodies, including security and military agencies, with the resources to exploit the opportunities afforded by big volumes of data, notably to operate costly data infrastructures, especially the development and application of machine learning technologies to deal with large datasets (Andrejevic and Burdon 2015, 21). In short, these actors have the necessary infrastructure, expertise and technologies to analyse large swaths of data, including open data (Andrejevic 2014). Those who can control data are understood to wield 'new kinds of informational power' (West 2019, 22), equivalent to Strange's concept of structural power in the knowledge structure: the ability to set the rules under which others – that is, data-poor actors – operate.

As a quick example, consider the ride-hailing company Uber. Uber's control over its drivers exemplifies the knowledge – and power – asymmetries in the gig economy. The gig economy can be thought of as digital piecemeal work. Lacking the long-term stability, protection and benefits offered by traditional employment, gig workers get paid depending on how many tasks they complete – in this case, taxi rides. Meanwhile, ride-hailing companies use data-driven algorithms to control the working conditions and pay of drivers, often in exploitative unfair ways (Calo and Rosenblat 2017). Uber's algorithms, for example, sometimes conceal from their drivers their fares per trip, thereby pushing drivers into working longer hours for less pay (see also Rosenblat 2018). That drivers don't have access to this data or the algorithm that shapes their working lives marks them as data-poor and solidifies their structural disadvantage when dealing with Uber, their de facto employer.

Characteristic 7: Claims of Predictive Accuracy Are Overstated

Another foundational faulty assumption underlying the data economy is that human behaviour can be objectively and accurately quantified, understood and predicted through data, an ideology termed 'dataism' (van Dijck 2014), which we will discuss in greater detail in the next chapter. A core claim of dataism is 'veracity through volume' (Crawford et al. 2014, 1667), meaning that mass amounts of data ('big data') are understood to produce valuable expert knowledge.

A core ideology of the information-imperium state, dataism holds that data-intensive processes, including regulation via algorithms, are perceived to be more effective, accurate and efficient than non-big-data human-centred ways of doing things. Even in light of data-driven debacles such as algorithms that unfairly deny people public services to which they are entitled, including housing and child protection (see Eubanks 2018; Hintz et al. 2018), the legitimacy and predictive accuracy that industry accords to algorithms can be 'seductive' for policymakers (Crawford et al. 2014, 1667).[2] Algorithms, in other words, promise straightforward technological fixes to complex social problems. However, not only are these promises faulty because algorithms cannot achieve their designers' lofty goals, but adopting data-driven processes to deliver government programmes can further entrench biased and discriminatory practices.

A dataist mindset typically assumes that data collection is comprehensive and reliable and that the gathered data is accurate and fully represents the phenomenon being examined. Not all information, however, can be translated into data, as aspects of the original phenomenon can become lost or be untranslatable (Loukissas 2019). Dataism also tends to also overlook the reality that datasets can be incomplete. Design anthropologist Sarah Pink and colleagues contend that data can be 'broken', necessitating 'repair and maintenance' work before data analysis can take place, meaning that actors may manipulate and process data in certain ways to make it 'useful' or valuable for certain purposes (Pink et al. 2018, 3).

The assumption that data can speak for itself also ignores a key insight of sociologists of knowledge: because data itself is a human product, it will necessarily never be objective. The concept of broken data, meanwhile, reminds us that instead of assuming data completeness and accuracy, we should be attentive to the ways that data collection, storage and analysis are partial and can be faulty or disrupted, while also recognizing the human labour involved in repairing data to render it valuable.

Algorithms, which are a set of instructions designed to generate a specific desired outcome, are central to efforts to monitor and predict behaviour and events, typically through automated decision-making. Similar to the

economic, political and social power we have accorded data, algorithms are commonly framed as having significant power and legitimacy, offering the 'promise of algorithmic objectivity' (Gillespie 2014, 179). Communications scholar and Microsoft researcher Tarleton Gillespie notes that this objectivity is a 'carefully crafted fiction' intended to portray algorithms' outcomes as 'fair and accurate, and free from subjectivity, error, or attempted influence' (Gillespie 2014, 179).

Characteristic 8: Individual Consent Legitimizes the Data-Driven Society

The data-driven economy is founded upon the myth of individual informed consent. The idea of voluntary informed consent holds that personally identifiable information should only be collected, stored and used once individual consent is secured, namely with 'the consent being specific, freely given and based on full and adequate information' (Taylor et al. 2017b, 6). Much of the Quayside debate turned on the question of how Sidewalk Labs could (or should) get individual consent for the surveillance throughout the urban landscape that would be necessary to make their plans work.

As we will see in chapter 9, there are two key issues with using individual consent as a regulating principle when it comes to data governance. First, it is problematic to assume that individuals can provide any form of meaningful consent for the collection of their personal data. Individuals are usually deemed to have provided consent through the terms-of-service that pop up whenever one uses software or an online service. In the United States, the dominant perspective of privacy since the late 1990s assumes people act as rational consumers who read (notice) and then give an informed consent (choice) to privacy policies (Cranor 2012, 304). This notice-and-consent approach has been exported globally through US-based internet companies in their terms-of-service agreements that are the legal authority for their data-intensive business models.

Anyone who has ever come across one of these terms-of-service agreements will understand the problem immediately: most people neither read nor understand these often-massive and often-impenetrable documents (see Bakos et al. 2014; Obar and Oeldorf-Hirsch 2020; Tene and Polonetsky 2013). In fact, the standard phrase, 'I agree to these terms and conditions' has been called, without exaggeration, 'the biggest lie on the internet' (Obar and Oeldorf-Hirsch 2020, 130). Even if people painstakingly poured through their terms-of-service agreements, they would need 'ubiquitous omnicompetence' in order to understand how their data may be collected, used and shared, particularly how it may be 'repurposed and sold by every application,

commercial organization, non-commercial organization, government agency, data broker and third-party' (Obar 2015, 4).

Second, it is problematic to view consent solely (or even primarily) as an individual responsibility. The idea of voluntary informed consent is deeply embedded in Anglo-Saxon conceptions of privacy as an individual right (see, e.g., Taylor et al. 2017a). In this understanding of privacy, one individual's disclosure of personal data to an entity does not affect the privacy of another.

This is not always, or even usually, the case. With the rapid growth of social media platforms and the expansion of corporate databases, disclosure of personal data by one individual may result in knowledge of the personal data of others linked to this person. For example, as law enforcement increasingly turns to consumer DNA ancestry sites as an investigative tool, genetic data shared by one person for a specific purpose – to trace a family tree – may be used for other purposes not intended or likely anticipated by the donor. What's more, most individuals' data only has value when combined with others' data, for example, in constructing credit risk standards against which others are judged (and possibly denied access to credit). In those situations, one person's individual consent, even if fully informed, can end up harming other people.

In both cases, it is clear that individual consent–based privacy is too narrow a conceptual lens to use when setting policy. Instead, as we argue in chapter 9, a broader, more collective human rights–based approach to privacy is necessary (see Dencik et al. 2016; Taylor 2017a). Human rights–based approaches, which argue for the importance of protecting individual rights while also establishing or expanding collective rights in the data economy, tend to favour measures that restrict some types of data collection and limit data commodification. We discuss this decommodification approach as an alternative to the information-imperium state in the conclusion.

AN INCONVENIENT TRUTH: THE FALSE PROMISE OF ANONYMIZATION

Concerns about individual privacy (to say nothing of collective privacy) present probably the most significant roadblock towards the construction of an efficient data-based economy. That ubiquitous surveillance and privacy fit poorly together has not stopped industry, government and policy entrepreneurs from attempting to find privacy workarounds that would allow the data-driven economy to flourish. Technical infrastructures based in part on greater individual control over their data, such as data trusts, which we discuss in chapter 9, are efforts in this vein.

De-identified (or anonymized) data represents a similar attempt to maximize data collection while minimizing privacy risks and concerns. Data

de-identification is a technical process that 'strips' or 'scrubs' personally identifiable information from a dataset, such as names, addresses or birthdates (see, e.g., Lubarsky 2017). By stripping personal identifiers in a robust fashion, the idea is that the data can no longer be traced back to identifiable individuals, and therefore can be broadly used, stored and shared without typically being subject to the same privacy regulations as personally identifiable data.

Data de-identification treats privacy as something that is only relevant to individuals. While many debates on privacy and surveillance in the data economy focus on individuals being tracked, amassing and processing data is often about groups (Taylor et al. 2017a). Aggregate data refers to group-level data that has been created by combining individual-level data, often in anonymized form, for example, to predict trends in energy consumption or health. Governments and companies are interested at the level of the group in terms of forecasting, tracking and influencing behaviour, which is typically undertaken using automated data tools. As such, data de-identification schemes do not do much to address the harms from collecting group-level data.

Putting aside these group-level concerns, data de-identification is often portrayed by companies as a solution to address public or regulator concerns about data security, privacy or the misuse of data, as well as the possible sharing or sale of personal data with third parties. Data de-identification, however, is not a foolproof solution. Over the last decade, a growing body of scholarly research by computer scientists and mathematicians demonstrates that it is increasingly possible to re-identify, or, put it another way, to de-anonymize data (see, e.g., de Montjoye et al. 2013; Narayanan and Shmatikov 2008). Data re-identification is the process of discovering 'the identity of an individual who contributed data that subsequently had anonymization techniques applied' (Curzon et al. 2021, 102). In fact, as research by computer scientist Yves-Alexandre de Montjoye and colleagues shows, it is 'increasingly difficult, if not impossible, to anonymize a dataset' (Montjoye et al. 2012; cited in Kammourieh et al. 2017, 46). Data de-identification advocates, however, argue that sufficiently robust de-identification techniques, combined with proper data-protection practices, minimize the risk of de-identification (see, e.g., Cavoukian and El Emam 2014, 2).

Actors can re-identify data when de-identification practices are flawed or are insufficient to prevent re-identification or when actors combine datasets that were meant to be kept apart (see Lubarsky 2017; Ohm 2010). Combining a small number of attributes extracted from various datasets, such as gender, data of birth, postal code and marital status, is often sufficient to re-identify individuals with a high degree of confidence (see Rocher et al. 2019). What's more, these attributes need not relate to personal data, as re-identification can also be undertaken by combining personal data with non-sensitive,

non-personal data, such as movies watched, locations visited or web browsing histories (Narayanan and Shmatikov 2019). Every data point, even those revealing something seemingly innocuous 'abets further reidentification' (Ohm 2010, 1705). As de-identification attacks are improving over time, computer scientists Arvind Narayanan and Vitaly Shmatikov argue that de-identification techniques 'should rest on provable guarantees rather than the absence of known attacks' (Narayanan and Shmatikov 2019, 1).

A full account of the technical processes of de-identification and risks of re-identification lies outside the scope of this book (but see Lubarsky 2017; Ohm 2010). What's important to our argument, however, is that corporate claims about the effectiveness of de-identification practices reveal a fundamental truth about data: 'Data can be either useful or perfectly anonymous but never both' (Ohm 2010, 1704). While perhaps an overstatement, what this means is that data utility and privacy are 'intrinsically connected' because 'as the utility of data increases, the privacy decreases' (Ohm 2010, 1705–6). There is therefore an incentive for actors to re-identify data, either for their own use or to sell to others.

Here, again, we see a fundamental tension between privacy and the collect-it-all mentality characteristic of our data-driven society. Actors reliant upon pervasive data collection are understandably resistant to the argument that de-identification does not effectively protect privacy as there are strong financial incentives to safeguard the 'simplicity of the de-identification paradigm' (Narayanan and Shmatikov 2019, 2).

Aside from the data-maximalist attitudes of various states and companies, fundamental changes in the data economy have contributed to the risk of data re-identification. The number of datasets, both public and private, has grown, meaning that there is a risk that datasets may be combined (Kammourieh et al. 2017). Here, the risk is that disparate data sources may not individually reveal personally identifiable information but their combination may do so (Curzon et al. 2021, 7). The growing data broker industry, moreover, has as its primary purpose to amass, link and combine datasets from consumers, companies and even governments to uncover potentially valuable patterns in data of use to those interested in forecasting or influencing behaviour. New data sources in the last two decades also provide richer data, such as genetic information, fitness wearables, social media and mobile phone data (Taylor et al. 2017b, 3). Further, technological advances enable the collection and processing of mass amounts of data that, as noted by the British Academy and the Royal Society, 'generate unexpected patterns or insights which go far beyond the original intended purpose of data collection' (The British Academy and the Royal Society 2017, 34; cited in Rinik 2020, 347).

CONCLUSION

The eight characteristics (and one inconvenient truth) outlined in this chapter describe how data 'works' in our own historically contingent knowledge-driven society. A knowledge-driven society is naturally predisposed to favour ubiquitous surveillance and control over knowledge (in this case, data) because this control is seen as a fundamental element of political, economic and social power. The particular form of this control is, in turn, linked to the interests of the actors involved. For the information-imperium state this means commodified data for market-based actors (i.e., companies), while for states, it entails data that serves state goals of protection/security (as with the system revealed by the Snowden leaks) and the delivery and management of public services. It is the logic to which state and non-state actors – digital economic nationalists and knowledge feudalists, whether authoritarians or democrats – must respond.

Chapters 6 through 9 explore how private actors and governments are increasingly amassing and using data in order to wield economic and political power. In particular, this book studies the accumulation and, importantly, the interpretation of data as a key power vector in the global economy and also considers those who benefit and those disproportionately affected by the rise of a data economy. In short, how can (and how *should*) data be governed, by whom and for what purposes?

None of this should be read to imply that there is either anything natural or inevitable about ubiquitous surveillance or data commodification. One of the lessons we can draw from Karl Polanyi's discussion of fictitious commodities is that the harm caused by treating human beings or nature as commodities can be reduced or eliminated. Policymakers can, in the name of human rights, limit the economic and social pressures of a data-driven society by restricting data commodification – think data-minimization efforts or exempting children from online data-collection efforts – and ubiquitous surveillance.

We would be remiss not to acknowledge that enormous pressures against such efforts are, to an extent, built into the system. These are evidenced most directly by the ongoing charade that terms-of-service agreements are anything but 'the biggest lie on the internet' (Obar and Oeldorf-Hirsch 2020), as well as by the faith that has been placed in de-identified data to square the surveillance-privacy circle. As we will see in the next chapter, the biggest obstacle towards more humane data and IP policies is not material power but ideology. The emergence of a knowledge-driven society has not only reshaped the economy and foundational institutions like private property but also how we think about the world itself.

NOTES

1. We purposely avoid using the term 'big data' because, as boyd and Crawford (2012, 663) remark, 'big data' involves not just the ability to collect and analyse large datasets but also the 'belief that large datasets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy'. We explore the implications of this belief in chapter 5.

2. See chapter 5 for a more in-depth discussion of dataism and chapter 8 for a discussion of how governments are both using automated data practices to deliver public services and battling data companies to access the data necessary to regulate sectors like housing and transportation.

Chapter 5

Ideology, Dataism and the New Experts

> Oh my God! We've been selected. Now, it's our turn.
> *Alphabet executive chair Eric Schmidt, on hearing that Sidewalk Labs had been selected to plan the Toronto Quayside neighbourhood*. (Dingman 2017).

Why would anyone think that Google could build a smart city?

The question seems to be too obvious to even ask. After all, Google is one of the biggest, most iconic companies of the modern age. It dabbles in almost every industry under the sun, from healthcare to thermostats. If Waterfront Toronto, the quasi-government organization that we mentioned in the introduction, was interested in building if not a smart city, then at least a smart neighbourhood, wouldn't it make sense to tap a Google company, Sidewalk Labs, for the job?

Smart cities, after all, are built on data and mass surveillance. What better company than Google – the master of online search and data collection – to make a smart city happen? Especially one that was to be planned 'from the internet up' to quote Sidewalk Labs CEO Daniel L. Doctoroff (2016). And in addition to being backed by Google, Sidewalk Labs capitalized on Doctoroff's pedigree as a former deputy mayor of New York City (from 2002 to 2008), responsible for Economic Development and Rebuilding.

Regardless of Doctoroff's deputy mayor credentials or the urban-development experts the company had on staff, Sidewalk Labs was almost certainly in the game because it was a Google company. At the official partnership announcement in October 2017, Canadian prime minister Justin Trudeau remarked that 'Eric and I have been talking about collaborating on this for a few years now', the Eric in question being Alphabet (Google's holding company) executive chair Eric Schmidt (O'Kane 2019a). Behind the scenes, as the Ontario auditor general's scathing 2018 report into Waterfront Toronto

revealed, Waterfront Toronto's board was placed under 'intense pressure' (Goodman and Powles 2019, 459) from all three levels of government to approve the Sidewalk Labs partnership (see also Auditor General of Ontario 2018, 691). From the prime minister on down, the province's and city's leaders all believed that Google could build and potentially operate digitally enhanced municipal infrastructure.

But consider the question from another angle. Consider this proposed smart neighbourhood, not as a tech project but as an urban-development project, one designed, as Waterfront Toronto's original Request for Proposals (RFP) made clear, to tackle issues like climate change and affordable housing (Waterfront Toronto 2017). As an urban-development project, Quayside would have been an enormous undertaking. Sidewalk Labs estimated it would cost CDN$39 billion to implement their plans (Sidewalk Labs 2019a, 215). Nor was this some out-of-the-way development on a patch of Arizona desert (Borland 2020): Quayside sits on some of the most economically valuable real estate in North America – prime underdeveloped urban waterfront in the city of Toronto (Cardoso and O'Kane 2019).

This was a big project, both for Waterfront Toronto and the city as a whole. One wonders if Quayside had been seen primarily as a multi-billion-dollar urban-development project, whether Waterfront Toronto would have sought a company and partner with a more-established track record in development. When Waterfront issued its RFP in March 2017, Sidewalk Labs had never tackled a project anywhere near this big and complex. Google created Sidewalk Labs in 2015, its entry into the bourgeoning smart-city market that had already been established by powerhouses like IBM and Cisco (Lohr 2015). By 2017, the only completed project Sidewalk Labs could point to was the advertising LinkNYC street kiosks in New York City (Sidewalk Toronto 2017), which were designed to blanket New York with Wi-Fi. Even this relatively small project later ran into trouble. In 2020, New York accused the consortium behind LinkNYC of failing to pay the city millions of dollars of advertising money it was entitled to, even as the 'kiosks . . . have fallen short of their original lofty goals'. What's more, the LinkNYC project had run into its own particular set of problems. As *Politico* reported, 'In 2016, officials announced that the administration would be pulling internet access in response to the volume of pornography that was being viewed al fresco on city sidewalks.' All while 'critics . . . questioned the information collected from passersby' by these kiosks (Rubinstein and Anuta 2020).

Quayside, needless to say, was to be a project an order of magnitude more complex than LinkNYC. It was going to involve much more than wiring and networking a small neighbourhood. Sidewalk Labs' eventual proposal, the 4-volume, 1,500-page Master Innovation and Development Plan (MIDP), released in June 2017, laid out plans not only for timber skyscrapers but also

for an entirely new Canadian lumber industry, not only smart thermostats but also a revolutionary new power grid. The entire document is littered with similar grandiose schemes.

Which brings us back to the key question, phrased a bit differently: Even without the benefit of hindsight, why would any government think that Sidewalk Labs had the expertise and experience needed for a $39 billion, once-in-a-lifetime urban-development project?

We return to Quayside because the project reveals an important aspect of the knowledge-driven society. The seeming obviousness of the answer to the question of why anyone would think that Google could build, or even lead the construction of, a neighbourhood points to a fundamental change in the way we understand society and the world around us.

As we noted in chapter 2, power in the knowledge structure consists of two parts. The first is control over how knowledge is created, disseminated and used. We call this the knowledge-regulation part of the knowledge structure: it addresses control over things such as intellectual property (IP), data governance laws, internet governance and other communication systems and rules. This is the most easily studied part of our knowledge-driven society: What outcomes do IP laws favour? How do governments and companies use surveillance systems? Who controls data? Who benefits? Who bears the risks?

But there is another, more important part to the knowledge structure: the power to determine what we consider to be knowledge in the first place and what we consider to be socially and economically valuable knowledge. It's one thing to be able to control knowledge flows, but being able to convince people that you possess the type of knowledge they need? That's a form of structural power on a whole other level. It's the type of power that determines who we consider to be experts, who we turn to for guidance. We refer to this part of the knowledge structure as knowledge-legitimation power.

In Europe, the Enlightenment marked a significant change in the knowledge-legitimation part of the knowledge structure (Strange 1994, 124; on knowledge-legitimation, see chapter 2). Previous to the Enlightenment, the Church was the dominant European knowledge institution, with religious (Christian) knowledge – particularly of how to get to heaven – being the dominant form of knowledge and religious orders being the keepers of this knowledge. The Enlightenment dramatically reduced the Church's influence to the extent that science became the new dominant source of legitimate knowledge, the standard against which truth claims are judged. Scientists supplanted priests as the dominant legitimate knowers. Religious belief, of course, has not vanished. However, it tends to play a secondary role to science in today's world. The existence of Creation Museums in the United States demonstrates the extent to which even fundamentalist Christians believe they must frame their mythical origin stories according

to the forms of science, a museum being nothing less than a temple to science itself.[1]

Today, however, the question of who should be considered a legitimate authority and what counts as expertise is very much an unsettled issue. Worries about the rise of misinformation and fake news, fears, particularly in the United States, that we no longer share the same reality, and doctors concerned about the number of people who refuse to acknowledge the reality, that Covid-19 vaccines are a safe and proven technology, are all expressions of this fundamental conflict (Benkler et al. 2018; Ecker et al. 2022).

That Google's Sidewalk Labs, an untested company, won this valuable *land development* contract[2] because of its association with Google's surveillance (data collection) and data processing capacities is revealing for what it tells us about what counts as legitimate knowledge and who we accept as experts in general. Sidewalk Labs' and Google's success in landing this project reflected a widely held belief that technical proficiency in surveillance and in collecting and processing digital data translates into expertise in any public-policy area.

Faith in technical skills related to data collection – that Google could indeed build a smart city 'if someone would just give us a city and put us in charge', as Schmidt once said (Dingman 2017) – to allow us to undertake socially complex projects that involve much more than data processing is not unique to Prime Minister Trudeau, Waterfront Toronto or urban development as a field. It has become an omnipresent feature in society. Tech companies like Apple and Google have moved into finance and healthcare (Powles and Hodson 2017; Cross 2022). Tech start-ups are entering the criminal justice field, offering software that promises to identify crime 'hotspots' or rank offenders by their perceived risk of recidivism (see, e.g., Brayne 2020). There is hardly an area of society that has not been 'disrupted' by companies promising to leverage the power of data to do things better (see, e.g., Eubanks 2018; Sharon 2020; van Dijck et al. 2018; Vaidhyanathan 2012; Morozov 2014).

The belief in tech companies as experts outside of their narrow, technical domains is rooted in a belief in the power of data itself, particularly digital data, to allow us to understand and interpret the world. This belief enables such actors to influence meaning itself, in ways that express social, economic and political structural power. Facility with data has become synonymous with all-purpose expertise, displacing old-fashioned subject-matter proficiency. If you understand data, you can understand the world.

It is this shift in belief as to what constitutes legitimate knowledge that represents the fundamental, defining characteristic of our knowledge-driven society and of the information-imperium state. The knowledge-driven society is not defined primarily by the presence of ubiquitous digital communications systems like the internet or by the ability to digitize ever-increasing swaths of

experience. Rather, our current moment is defined by the belief that mastery of data and digital technology gives one privileged, uncannily accurate insights into how the world works. This belief is what media studies scholar José van Dijck (2014) and others refer to as 'dataism'. In a marketized society, this belief in data is tightly linked to the commodification of knowledge. Much as IP commodifies various other forms of knowledge, data is not just a type of knowledge, but is something to be bought and sold.

Changes in what constitutes legitimate and valuable knowledge are important because they also change our ideas about who we should think of as experts and what constitutes good and desirable policy and social outcomes. Our understanding of what legitimate knowledge is privileges some groups, ideas and outcomes while marginalizing others. In this case, dataism is the belief that the quantification of human activity can reveal previously unattainable truths about existence and that human interactions, beliefs, emotions, and so on, can be accurately and valuably quantified to provide useful insight into human behaviour (van Dijck 2014). (If you think this sounds uncomfortably close to long-discredited approaches like phrenology and other pseudoscience theories about quantifying human behaviour, you're not wrong (Kaltheuner 2021).)

Dataism is linked to what tech critic Evgeny Morozov calls 'technological solutionism' – the idea that 'all complex social situations' can be recast 'either as neatly defined problems with definite, computable solutions or as transparent and self-evident processes that can be easily optimized' by (digital) technology (Morozov 2014, 5). Dataism as an ideology stands in contrast to a scientific view of the world, which prioritizes deep understanding and embraces complexity. Authority under dataism is based not on the contextual understanding of specific fields such as economics, health or urban design but on the ability to operate the machinery capable of collecting and collating enormous amounts of digital data. It is a technician's authority.

As our brief discussion of the contests between religion and science and between science and misinformation suggests, specific knowledge-legitimation regimes rarely exist uncontested. While dataism and technological solutionism are the signature ideologies of our current knowledge-driven society, they are constantly challenged by a number of different actors. The smart-city debate over Quayside, for example, was as much about the limits and drawbacks of dataism as a guide to public policy as it was about material interests.

In this chapter, we outline the meaning and consequences of dataism and technological solutionism, what norms they promote and which actors they favour. We then explore the tensions between dataism and the scientific form of knowledge through an extended case study focused on the development and deployment of Canada's Covid Alert contact-notification app. The app's development bears all of the marks of commodified dataism that we also see

in Waterfront Toronto's embrace of Sidewalk Labs: a belief that technology companies can deliver health policy and a subtle redefinition of the problem in question (in this case, how to stop a pandemic) in ways that undermine previous (successful) techniques and policies.

THE SCOURGE OF DATAISM

In its original definition, dataism refers to 'a widespread belief in the objective quantification and potential tracking of all kinds of human behaviour and sociality through online media technologies' (van Dijck 2014, 198). However, the dataist mindset reaches far beyond personal data, encompassing all forms of data collection, personal and non-personal. Dataism, in other words, reduces the entire world to the data that can be digitally collected about it via surveillance and assumes that the solutions to the world's problems are encoded in this data.

Central to dataism as an ideology is the assumption that there is 'a self-evident relationship between data and people' (van Dijck 2014, 198). This assumption is closely related to the claim that data is a neutral representation of reality. Consequently, so the dataist argument goes, data aggregated into 'large datasets offer a higher form of intelligence and knowledge' (boyd and Crawford 2012, 663). As Microsoft researchers danah boyd and Kate Crawford highlighted in a groundbreaking 2012 journal article, 'Big Data' doesn't just propose a new methodology. It 'changes the definition of knowledge', reframing 'key questions about the constitution of knowledge, the process of research, how we should engage with information, and the nature and the categorization of reality' (boyd and Crawford 2012, 665).

That it embodies a 'higher' intelligence, so the argument goes, means that big data can be used to 'generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy' thanks to the remarkable computing power we now have at our fingertips (boyd and Crawford 2012, 2). The delivery of a 'higher form of intelligence and knowledge' is the promise of every artificial intelligence (AI)-branded start-up and the entire personalized advertising industry that underwrites our current commercial internet (Hwang 2020).

As we noted in the previous chapter, the promise of dataism is nothing less than the ability to predict the future. In his study of the data analytics industry, sociologist David Beer argues that companies promise results from data analytics with 'prophetic properties' (Beer 2018, 473). Companies sell the idea that it is possible and desirable to anticipate future events and act accordingly as 'data analytics are conjured as being the desirable direction for all organisations' (Beer 2018, 473). Data-focused business models 'are presented as a competitive necessity' (Beer 2018, 476). In turn, power in the

data-driven economy rests 'firmly in the hands of those who are able interpret or tell stories with the data', giving 'a unique primacy to those who are in a position to engineer those revelations' (Beer 2018, 465). Those who interpret data exert power 'in shaping what is said, made visible or known through data' (Beer 2018, 466).

The dataist belief that every aspect of human experience can be transformed into quantifiable data, and that this data can be used to predict human behaviour, is nothing if not expansive. It forces back the 'data frontiers' that mark the limits of what can be datafied, encompassing ever-more social areas like education or healthcare (Beer 2018, 467). Quantifying human emotions? Spotify, the music platform company, claims that it can tell what you're feeling by how you use its platform, knowledge it can use to decide which songs to suggest to customers or sell to marketers who share its dataist mentality (Savage 2021; Mahdawi 2018).

The promise that data can predict the future has a long pedigree: selling predictions about the future is nothing new. Advertising, for instance, has long claimed to anticipate consumer desires, while the insurance and financial industries are built on forecasting events and calculating associated risks (see, e.g., Lauer 2017). Assessing the rise of Silicon Valley's hype of the predictive nature of data analytics, historian Jill Lepore notes that, at least in the United States, calling something AI, data science or predictive has become a way to raise venture capital funding, a surefire profit model underwritten by a credulous press and facilitated by the US government's reluctance to exercise effective oversight over the digital tech industry (Lepore 2020). This business model remains seductive, despite a decades-long history, detailed by Lepore, of companies making dubious claims of predictive capability that often end up being limited in scope and discriminatory in application.

Dataism and Algorithms

The belief in data as a higher form of knowledge is mirrored in the belief that algorithms deliver unbiased, objective and accurate outcomes. Like 'data', the idea of the algorithm has attained an almost mystical quality in our datafied world. Like the Greek gods, they are the mysterious and unknowable cause of and solution to all our problems. Like all things mystical, they empower those who claim the ability to interpret them. It is no accident that Science and Technology Studies scholar Malte Ziewitz describes algorithms as a 'modern myth' (Ziewitz 2016, 3).

Algorithms, he notes, are commonly portrayed as 'powerful and consequential actors in a wide variety of domains' (Ziewitz 2016, 5). Industry actors and policymakers alike embrace their wisdom and utility in addressing a wide range of social and economic issues, from determining the eligibility

of 'potential immigrants' or prisoners up for parole to allocating public services like housing or social assistance (see Eubanks 2018).

Of course, algorithms are nothing more than a set of human-created rules that are applied over and over again to a situation. That they are processed within a computer and potentially contain many different and recursive steps doesn't make them any different than the procedures used by individuals, organizations and bureaucracies from the dawn of civilization to decide who qualifies and who should be denied for a service, a pension or a job. As a human creation, algorithms are no better than the people who create them. Garbage in, garbage out: it was always thus.

Algorithms are central to data-driven efforts to monitor and predict behaviour and events, particularly on a mass scale. When someone is talking about automated decision-making, machine learning or predictive analytics, they're discussing algorithms. Some algorithms use machine learning, which involves 'parsing large datasets to detect patterns, commonly "training" on one half of the data, with ongoing refining occurring on the remainder (and then progressive adaptation to fresh data)' (Carney 2020, 4). The objective in machine learning is to enable the algorithm to classify and 'generalize beyond the examples in the training set', for example, identifying faces that are not in a facial-recognition training database (Domingos 2012, 79; cited in The Citizen Lab and International Human Rights Program 2018, 9). Advanced automated decision-making involves 'making more complex decisions involving a discretionary element' that leaves little space for context or complexity (Carney 2020, 2). For example, advanced automated decision-making can be (and is) used to determine who is eligible for government services or determine an individual's risk level for recidivism, as chapter 8 explores.

Regardless of the mundane reality of what algorithms are (automated rules) or how they work (by iteratively applying rules), what is most consequential is the belief that has sprung up around them, in the algorithm as a font of legitimate, superior knowledge. Those who create and use algorithms have imbued algorithms themselves with a degree of agency: 'they "adjudicate", "make mistakes", "exercise their power & influence"' (Ziewitz 2016, 5). Although they are designed by humans and reflect human goals, the human agency involved in creating and using them is minimized. This minimization of human agency effectively shifts the responsibility for the effects of this automated regulation away from algorithm creators and the organizations that use them. Mystification in action.

This was the case in the Stanford Medical Center in California that used an algorithm in early December 2020 with the aim of prioritizing Covid-19 vaccinations amongst frontline medical staff. When it was revealed that only a handful of frontline staff had been prioritized for vaccinations and that the list of priority staff included administrators and doctors working

remotely, employees protested. Hospital administrators blamed 'a very complex algorithm' for the debacle (Guo and Hao 2020). Blaming the algorithm draws attention away from the human decisions embedded in the algorithm: in this case, the determination of specific demographic and workplace variables that the designers contended calculated risk levels for the disease.[3]

'Big Data' and the End of Theory

Whether we're conscious of it or not, we move through the world by relying on theories of how the world works. Theories are lenses that we use to understand the world. This understanding extends to what data, or facts, about the world we consider to be most important to understand a particular issue.

These assumptions, in the scientific way of thinking about things, are necessary because as we discussed in chapter 1, the world is infinitely complex: making sense of it requires such assumptions. Because the world is complex and theories are always partial, people with different theories and interpretations of the world – interpretations that themselves are socially constructed – will see the world differently. This is what it means when we say that there is no such thing as raw data (Gitelman 2013): our theories of the world inform our choice of what we define as relevant data, and our data informs our theories of the world.

Dataism rejects this complexity. Dataism as an ideology believes that data gives us a neutral depiction of reality, and if we analyse a complete-enough dataset, we will be able to fully understand the world. All we need to do is identify the correlations in the data. These assumptions in turn lead to claims that the era of 'big data' has brought about the 'end of theory' (Anderson 2008). If data can speak for itself, and correlations are all that is needed for understanding, then we don't need to indulge in elaborating theories on how states interact or what drives suicide rates. This dataist approach amounts to a rejection of a key principle that we discussed in chapters 1 and 4, that 'raw data is an oxymoron' (Gitelman 2013). For dataists, data is a raw material, just hanging around, waiting to be collected, an objective representation of the world.

Grasping the implications of this point – that data is not neutral – is important for understanding arguments against algorithmic governance. Many, if not most, of the critiques levied against, for example, search engine algorithms that systematically return racist results (e.g., Noble 2018) or algorithms that discriminate against groups in the delivery of government services (e.g., Eubanks 2018) are not just attacks on poorly designed algorithms. By highlighting the biased nature of algorithms *in general*, critics are arguing against the dataist worldview that big data and algorithms can be neutral at

all. These are not just attacks on the improper use of big data; they are part of a larger debate over what it means to conduct scientific inquiry.

Dataism, then, is the belief that it is possible and achievable (and desirable) to collect and process all the data and that problems with data reliability and accuracy can be overcome. If you collect enough data and have enough computer-processing power, you'll be able to understand the world using nothing more than the ability to spot correlations in the data. No theories of the world are needed because all that data can speak for itself. The ability to collect and aggregate data becomes synonymous with understanding, or knowing, the phenomena from which the data is being extracted. No subject-matter expertise is needed.

Redefining Expertise

It has become a running joke among those who follow the digital technology industry that Silicon Valley companies have an uncanny knack for 'inventing' goods and services that already exist. Over the past few years, the brightest minds of their generation have invented the city bus (the Lyft Shuttle), 'being thirsty' (the Hidrate Spark, a Bluetooth-enabled chip with 'a glowing light that tells you to drink, and must be plugged in and recharged periodically or it stops working') and powdered food (Soylent) (Spencer 2017), as well as vending machines (Bodega) (Ohlheiser 2017). As we write this particular paragraph, in January 2022, Bitcoin bros and Non-Fungible Token evangelists are busy reinventing the Ponzi scheme and the Dutch Tulip bubble, respectively, for the digital age.

While this almost-wilful ignorance of history is alternately amusing and frustrating, the tendency to reinvent already-existing goods and services is more than just techbro ignorance and marketing hype. It also reflects a dataist ideology that refuses to see any meaningful distinction among different areas of expertise. Seeing the world as data leads to a tendency to treat all data as interchangeable, no matter in what nominal area it is collected or for what purpose.

Traditionally, expertise has been associated with a deep understanding of a specific subject area, be it medicine, law, economics and so on. At the so-called End of Theory, however, such knowledge is perceived to be of secondary importance to the ability to collect, collate and technically analyse data. As Beer puts it, 'Algorithms [driven, we should note, by data] produce outcomes that become or reflect wider notions of truth.' Power becomes 'operationalised through the algorithm, in that the algorithmic output cements, maintains or produces certain truths' (Beer 2017, 8). Communications scholar and Microsoft researcher Tarleton Gillespie puts it even more poetically:

> The algorithmic assessment of information, then, represents a particular knowledge logic, one built on specific presumptions about what knowledge is and how one should identify its most relevant components. That we are now turning to algorithms to identify what we need to know is as momentous as having relied on credentialed experts, the scientific method, common sense, or the word of God. (Gillespie 2014, 168)[4]

This understanding of knowledge as context-free data has placed companies like Google, Facebook, Tencent, Apple and other digital-focused companies in positions of significant influence in areas far outside their nominal competencies (advertising, social media, etc.). Dataism, as a dominant ideology, has also served as an impetus for non-digital companies to reorient their activities towards greater data collection (Srnicek 2017) or at the very least to be seen as 'tech companies'. There are solid material incentives for this self-identification. Companies able to pose as 'technology' companies can command higher market valuations than those that are seen as labour-dependent firms and thus less likely to be hit by higher labour costs as company revenues increase (Irani 2015a, 231).[5] Within the state, dataism potentially empowers statistical agencies, security services and those organizations designed to surveil, collect and process data. It encourages other areas of government to incorporate surveillance and data-collection practices, and data-collection companies, into their activities, including the delivery of services (Eubanks 2018; The Citizen Lab and International Human Rights Program 2018).

The conflict of expertise with dataism could be seen even within Sidewalk Labs itself. *Globe and Mail* reporter Josh O'Kane (2020) highlighted tensions within Sidewalk Labs between 'Google-style technologists' and 'urban-affairs experts' in the company's early days. In particular, he noted that the 'technologists wanted to get some kind of product to market quickly – possibly in a standalone community – while urbanists treaded more slowly, cautioning about the slow pace of city building'. To an outsider, the scope and audacity of Sidewalk Labs' plans suggest that the final proposed project leaned closer to the technologists' vision than that of the urbanists.

Tech companies reinvent the city bus – and they are listened to when they propose these schemes – because understandings of what counts as knowledge are changing, and when it comes to the new knowledge, they are accepted as the experts. This faith in technologists and dataism even, or especially, extends to the question of how to fix the myriad problems caused by Silicon Valley. The number and diversity of references that we've drawn on to write this book highlight how there is no shortage of people who understand tech, data and Silicon Valley. However, their voices tend to recede into the background in policy debates, which are often dominated by what tech

policy writer Maria Farrell calls 'the Prodigal Techbro' (Farrell 2020). These are former (usually male) tech executives who, having 'experienced a sort of religious awakening . . . reinvent themselves as experts on taming the tech giants'. While one can claim expertise in something, one's status as an expert is bestowed by others: it is a social phenomenon. This is why the prodigal techbro's pivot in and of itself is much less interesting than what Farrell calls 'the mantle of moral and expert authority' that they have been accorded by society. They have received this expert status precisely because of their position as dataism's high priests and the belief of others in the promise of dataism. Small wonder, as Farrell notes, that the prodigal techbro shies away from structural change: 'He's invested in the status quo, if we can only restore the founders' purity of intent.'

TECHNOLOGICAL SOLUTIONISM

If dataism is the dominant ideology of the information-imperium state – that is, of dominant business and government agencies – technological solutionism is its policy programme. For the prescient tech critic Evgeny Morozov, who coined the term in his 2014 book *To Save Everything, Click Here*, technological solutionism treats all social problems as digital-engineering problems. Solutions to engineering problems, Morozov notes, tend to value efficiency, optimization and speed over all other objectives. Implicit in this formulation is the assumption that speed and real-time data collection facilitate problem-solving and that deliberative decision-making by humans is necessarily ineffective. Technological solutionism reduces problems to what can be measured and assumes that what can be quantified represents an unbiased and complete representation of the underlying phenomenon. In doing so, technological solutionism more than adopts a different way of solving an issue; it redefines the underlying policy problem in narrow technical terms.

Technological solutionism offers a seductive way of thinking about the world, particularly in an era in which the computer operating system has become an omnipresent metaphor for human society and reality itself. However, there is at least one flaw at the heart of the idea, even overlooking the points we made in chapter 1, that all datasets are necessarily biased and incomplete and that perfect knowledge is an unattainable pipe dream. The fantasy that there are 'definite, computable solutions' or 'self-evident processes that can be easily optimized' (Morozov 2014, 5) ignores the reality that reasonable people have often-radically different opinions about both the appropriate means and just ends of nearly every social problem. Should education focus on self-esteem and socialization of students or the memorization of facts and history? What principles should undergird a city's transportation system: a

preference for mass transit or for individual freedom (i.e., buses or cars)? Simply looking at the data can't answer these questions because they require consensus on what the problem is and what values should shape the problem and the solution. Optimal solutions are a technocrat's dream, but we live in a world of politics, where honest people legitimately disagree about almost everything.

Sidewalk Labs' approach to addressing Toronto's transit challenges offers us a useful example of technological solutionism in action. Toronto's transportation system is rife with problems in need of solutions. Its subway system is overburdened, its streets are clogged with cars and traffic fatalities are unacceptably high (Spurr 2018, 2021).

Sidewalk Labs' proposed solutions focused on enabling private ride-hailing programmes and autonomous vehicles, as well as a demand that Toronto fast-track a rail link to its neighbourhood (Sidewalk Labs 2019b, 40; 102–145). Putting aside the rail link, Sidewalk Labs made a specific choice to define Toronto's problems in ways that played to its own interests. It didn't frame Toronto's transit woes as a problem of underfunded, crumbling infrastructure. Instead, it framed the issue as one of ineffective coordination amongst mobility options and insufficient monetization of public spaces, whether for cultural events or package delivery. Unsurprisingly, the solution that it proposed to these problems would have been digital-data-driven: for example, creating flexible-use street curbs and a real-time data-based mobility system that would have coordinated and managed all traffic within the district. Framing the problem and solution in this way allowed Sidewalk Labs to position itself as uniquely qualified as an urban developer, to digitally map and monetize curbsides for more effective use of ride-hailing services, package delivery vehicles and other entities, like taxis or buses, using street curbs in ways that would 'solve' Toronto's transportation crisis. The answer to inadequate transit infrastructure is digital and would require a company like Google, which is an expert in collecting and interpreting data through mass surveillance of people and objects.

DATAISM IN ACTION: PANDEMIC SOLUTIONISM

Responses to the Covid-19 pandemic were rife with technological solutionism that can help us to further appreciate the dynamics and consequences of seeing the world through a dataist lens. In this section, we highlight how dataism contributed to the embrace of tech companies as credible health-policy actors by governments and publics alike. This embrace, in turn, has allowed these actors to redefine fundamental public-health concepts, notably 'contact tracing' and 'privacy' in ways that reflect their interests and values as technicians rather than subject-matter experts, most notably in the global embrace of Covid apps as a (failed) way to mitigate the pandemic's effects.

Tech Companies as Credible Policy Actors

As law and technology scholar Linnet Taylor and her colleagues argue in a 2021 book on the pandemic, the pandemic saw the 're-purposing' (or re-packaging) of existing technologies from various sectors to track and predict Covid-19 (Taylor et al. 2021, 11). When the global Covid-19 pandemic began in earnest in early 2020, it was not long until dataism's telltale faith emerged in the notion that tech companies are well-suited to addressing all matters of policy challenges, not just as supporting players but as leading actors.

In the United States, Facebook CEO Mark Zuckerberg stated in an April 2020 *Washington Post* op-ed that data is 'a new superpower' to counter Covid-19. Zuckerberg argued that there are opportunities to use 'aggregate data [from social media platforms] to benefit public health' (Zuckerberg 2020). In the policy realm, US president Donald Trump announced on 13 March 2020 that Google was building a national Covid-19 screening and test-scheduling website. Unsurprisingly given the source, it quickly turned out that the announcement was typical Trumpian bluster: the Google sister company in question, Verily, 'had only begun working on a small pilot of the website to begin screening people in the Bay Area' (Lerman 2020). Nonetheless, this blind faith that Google was the appropriate actor to conduct such tracing has all the hallmarks of dataism and technological solutionism.

While Verily was quick to ramp up its efforts, almost two months after the announcement it became clear that it was failing to make any difference to the US testing effort (Lerman 2020). By the end of 2020, the Google tool had contributed to less than 1 percent of all US tests (Abril 2020). The Verily project, however well intentioned, lacked deep experience in the field. Analysts attributed its failure to the fact that Verily 'has roots in technology and research, not clinical medicine' (Lerman 2020). The site – which required users to have a Gmail account to access – also ran into privacy concerns that individuals' health data would be harvested by Google (Abril 2020). Also important was the fact that Verily is 'reliant on partners – it doesn't conduct its own tests or process the results, and many patients have never heard of it' (Lerman 2020). In short, in terms of the initial faith placed in it, a lack of actual experience or embeddedness in the notoriously complex American healthcare field mattered much less than the fact that Verily could bask in Google's data halo: the very embodiment of dataism.

Remaining in the healthcare sector, in Canada, Switch Health, a company that went from five employees and no healthcare clients 'in early 2020 to over 1,200 full-time and part-time employees one year later' (Cooper and Bell 2021), offers a small example of how appeals to data and tech operates with respect to building legitimacy. An April 2021 investigation by Canadian news outlet Global News noted that 'there is limited public information

available about Switch Health and its founders' and that 'the company was formally registered in April 2020' (Cooper and Bell 2021).

Switch Health's innovation, according to media reports, was to administer Covid tests remotely, with tests delivered and picked up by couriers, including Uber. In early 2021, it received a contract 'worth nearly $100 million to manage hundreds of thousands of coronavirus tests for travellers arriving in the country at land-border crossings and at airports in Toronto, Montreal, Calgary and Vancouver' (Cooper and Bell 2021) (the government also awarded contracts to other providers, although Switch Health seems to have garnered the most headlines [O'Connor 2020]).

In their report, Global News raised several questions and concerns about Switch Health, particularly numerous complaints of unsupervised swabbing, long wait times and an inability to book tests within fourteen days (at the time, negative tests were required to leave the mandated fourteen-day quarantine) (Cooper and Bell 2021).

In a response to these reports, Switch Health told Global News that 'it has scaled up its operations and continuously hired new employees to upgrade its systems and reduce wait times, but said it was going through some "growing pains"'. In the same report, then-federal Conservative party leader Erin O'Toole called their failure rate 'unacceptable' (Hill et al. 2021).

From the perspective of this book, less interesting than Switch Health's record is how it presented itself and how others saw the company. A glowing profile in Canada's *National Post*, published in September 2020, portrayed CEO Dilian Stoyanov as 'a techie with a background in big data and health-care solutions'. The future, as they saw it:

> Testing at home, using kits and advanced software so that, for example, Joe Blow, with the sore throat, won't necessarily have to go sit in a doctor's office for an hour to have his heart listened to and blood pressure checked, only to then be informed that his next stop is the pharmacy to fill a prescription for strep throat. (O'Connor 2020)

In the same profile, Rona Ambrose, a former Conservative health minister who sits on Switch Health's board of directors, highlighted the tech-based appeal of Switch Health, commenting 'I am a big believer in the need for the health-care system to be disrupted by technology' (O'Connor 2020).

Such is the mystique of 'big data' and 'disruption'. At the end of 2021, Switch Health continued to receive government contracts, including a contract of up to $440 million to provide testing services in Ontario, Alberta and Atlantic Canada (The Canadian Press 2021).[6]

The transformative powers of 'tech', 'big data' and 'disruption' are routinely invoked by entrepreneurs wanting to establish themselves as serious players. Such was the case in Philadelphia in the United States, where city officials put an untested nonprofit run by a twenty-two-year-old graduate student in charge of its entire vaccine-distribution effort. As *Bloomberg* reporter Dayna Evans recounts, Andrei Doroshin had caught people's attention when his group of Drexel University students, Philly Fighting Covid (PFC), 'volunteered to make 3D-printed face shields for undersupplied hospital workers' and later conducted 'Covid tests in a parking lot outside a temporarily shuttered Fishtown music venue' (Evans 2021). This was enough to convince the city to give Doroshin, who otherwise had a 'total lack of medical experience', the contract to be Philadelphia's first vaccine provider (Evans 2021; Feliciano Reyes et al. 2021).

The result was a disaster, with PFC appearing 'to be motivated primarily by self-aggrandizement and cash' (Evans 2021). In the resulting fiasco:

> PFC's chief medical officer (its only licensed doctor) quit and alerted the health department that the operation had quietly reincorporated itself as a for-profit called Vax Populi. The whistleblower also warned the department not to trust Doroshin or his ability to handle vaccinations. (Evans 2021)

Further questions were raised when 'Doroshin added a line to the site that suggested people who signed up with sensitive medical information for their testing clinics could have their data sold', and it was revealed that Doroshin had brought vaccine shots 'home with him to administer to his friends' (Evans 2021).

As reporter Dayna Evans notes, 'Doroshin's bro-y clown show might have been amusing if it hadn't distracted Philly from hiring real experts.' These included Dr. Ala Stanford, 'who was also running testing clinics through her Black Doctors Consortium' and who, as one observer noted, has 'been a doctor longer than [Doroshin's] been a person' (Evans 2021).

Doroshin, in other words, was pitching textbook technological solutionism and dataism, in the *lingua franca* of the ideology. In an interview, Doroshin remarked:

> We don't think, like, institutional. You know, we're engineers, scientists, computer scientists, cybersecurity nerds. . . . We think a little differently than people in health care do. We took the entire model and threw it out the window. We said to hell with all of that. (Evans 2021)

Doroshin's statements were the opposite of disqualifying. Everything pitched by Doroshin sounds like a feature, not a bug, if your audience has a dataist and technological-solutionist mindset. This ideology makes one

vulnerable to the charms of a '22-year-old whiz kid' with no formal training in the field he's seeking to upend (Feliciano Reyes et al. 2021).[7] The grandiose promises, the trumpeting of ignorance of healthcare practices while playing up claims of being 'cybersecurity nerds' were not disqualifying. In a dataist world, they actually positioned this non-expert as more qualified to address the pandemic than a doctor with over two decades of experience. This is the embodiment of dataism. Philadelphia eventually cut ties with Doroshin, with Mayor Jim Kenney admitting that 'working with Mr. Doroshin and Philly Fighting Covid was a mistake' (Feldman 2022). According to the *Philadelphia Inquirer*, some wondered if the decision to go with Doroshin rather than the group Black Doctors Covid-19 Consortium (which was run by actual medical doctors) was due to systemic racism (Feliciano Reyes et al. 2021).

Changing Beliefs: How Covid Apps Redefine Contact Tracing Downward

Power in the knowledge-legitimation part of the knowledge structure flows from the ability to designate who is considered to be a legitimate expert or authority. Expertise is not neutral; how society responds to a problem depends in large part on who is defining the problem and how it is defined (including whether or not something is really a problem).

The widespread global embrace of contact-tracing and contact-notification apps to combat the Covid-19 pandemic offers a textbook case of how dataism redefines who we consider to be experts and how a change in what we consider to be legitimate knowledge affects how we respond to crises. Embraced enthusiastically by governments in many countries, the apps largely failed to live up to their initial hype.

These failures are not in and of themselves an indictment of the idea of contact-tracing apps, and we should take care to avoid hindsight bias in judging failures such as these. Not every idea works out, especially when working under conditions of high uncertainty. Nor should these failures be treated as evidence that technology writ large has no place in healthcare or any other area. Vaccines are a technology, as are N95 masks. So, for that matter, are the computer systems that crunch the data needed to produce vaccines and to evaluate possible policy responses.

The problem, rather, lies with the dataism and technological solutionism behind the design and implementation of these particular pieces of technology.

Technological Solutionism: Redefining Contact Tracing

Consider the case of app-based contact tracing during the Covid-19 pandemic. Proposals to use apps to track, trace and mitigate the disease's spread

appeared early on. Like many technological-solutionist ideas, the notion that one could use a smartphone app to track and trace Covid-19's spread is plausible on its face. It also seemed to respond to a real problem: how to best track and mitigate the spread of Covid-19 in the most-efficient possible way, given the intensive nature of manual contact tracing.

An early article in *Science* by several Oxford University academics contended that because that the virus could be spread by 'presymptomatic individuals', it would be 'infeasible' to control 'the epidemic by manual contact tracing' (Ferretti et al. 2020). In contrast, a smartphone app, they argued, could offer 'instantaneous contact tracing'. Their claims for such an app resembled something you might read in a press release from any number of Silicon Valley start-ups: that, if used by enough people, such an app could 'be sufficient to stop the epidemic' (Ferretti et al. 2020).

Covid apps differ amongst themselves in how they function and their explicit purposes. Some are full contact-tracing apps, while others, such as Canada's Covid Alert app, are designed for contact notification, alerting a user's other contacts upon notification of a positive test result. That said, all Covid apps work roughly the way these Oxford academics envisioned: 'Proximity events between two phones running the app are recorded. Upon an individual's Covid-19 diagnosis, contacts are instantly, automatically, and anonymously notified of their risk and asked to self-isolate' (Ferretti et al. 2020).

As the companies that control the two dominant smartphone-operating systems, Apple (iOS) and Google (Android) played a central role in shaping both the discussion and development of many of the resulting apps. Their control over their operating systems amounts to a form of structural power, that is, the ability to dictate what other actors can do with and through their phones. Their 'almost complete monopoly on smartphone operating systems enabled them to channel information about the location of, and contacts between, almost all the world's smartphone users to anyone building an app' (Taylor 2021, 898). As Taylor and her co-authors note, their collaboration for a Covid app standard was a textbook case of 'crisis entrepreneurialism', an attempt to reach further into the multi-billion-dollar global healthcare market (Taylor et al. 2021; see also Sharon 2020).

To understand why Covid apps are an example of technological solutionism, we need to compare it to its manual analogue, manual contact tracing.

As the phrase suggests, technological solutionism assumes that solutions that involve technology – especially digital technology – are inherently superior to other possible solutions. Here, the main alternative to Covid apps would have been an expansion of manual contact-tracing regimes. However, at the beginning of the pandemic, as far as we are aware, no governments embraced supplementing their existing contact tracers with suddenly idled university students or laid-off workers. Such a move would also have had

the knock-on effect of better integrating people into their communities rather than isolating them at this time of crisis. Instead, to solve their problem, governments looked to technology.

Technological solutionism also reduces and redefines social problems according to the data that can be collected on the issue in question, prioritizing quantification, efficiency and the pursuit of precision.

For Covid apps, this involves defining a 'contact' based on a time and distance rule. Canada's Covid Alert app, for example, defines an exposure (or contact) as occurring when someone (or rather, a smartphone) is 'within two metres of someone [or rather, another smartphone] with Covid-19 for 15 minutes or longer', as determined by the two phones' Bluetooth signals (Health Canada 2020a). Efficiency, optimization, speed: the hallmarks of technological solutionism (Morozov 2014).

The precision offered by these apps is, to a significant extent, illusory. Bluetooth technology is inaccurate when it comes to estimating distances. It can't account for the size of the room, if the phones are separated by a wall, whether the contacts took place outside (lower risk) or inside (higher risk) or even the relative distance of the phones to each other (Romm 2020; Sharon 2020). Beyond these individual challenges, smartphone-based apps – which were never going to achieve universal uptake – were always destined to shut out lower-income (often racialized) individuals, the same individuals whose need to keep working made them most susceptible to catching Covid in the first place and who are least likely to be able to afford a smartphone (Haggart 2020b; McDonald and Wylie 2020). More generally, in Brazil, for example, the government's Monitora Covid-19 app, created 'in a partnership between public and private institutions', was 'underused in impoverished areas due to a lack of economic access to the technology and wireless network' (Lemos et al. 2022, 84).[8]

Making the efficiency claims for these apps (Ferretti et al. 2020) requires adopting this new, degraded definition of 'contact'. People are notified of something more quickly than they would be otherwise, but 'what constitutes a "contact" for a smartphone does not always have epidemiological value' (Sharon 2020, 551) precisely because it cannot evaluate the context within which the contact occurs.

Efficiency involves using fewer resources to obtain the same, or more of, a particular outcome. However, Covid apps' efficiency gains are also not as clear-cut as one might think. Beyond the false positives, the apps also shift the physical and emotional labour characteristic of manual contact tracing away from frontline public-health officials and onto individual app users and behind-the-scenes officials whose unseen labour allows the app to function.

This downloading of responsibility onto users is itself typical of how solutionist tech companies operate. It is characteristic of how companies like Facebook depend on its customers to police others' actions on its platform

(Crawford and Gillespie 2016). In the case of Covid apps, it is up to untrained (and likely frightened) users, rather than trained professionals, to follow the steps needed to make even this degraded version of contact tracing work. For example, the Canadian Covid Alert app requires that individuals

- download the app (not everyone will);
- carry their phones everywhere (granted, most people probably do this);
- run the app in the appropriate way (not everyone will);
- upon notification of a positive test, receive a code; and
- those with codes must upload them (not everyone will).

Furthermore, those receiving an alert must

- pay attention to it (which they won't if they're receiving too many false positives or don't understand where they were exposed);
- seek out legitimate information about what to do (which they might not do); and
- follow through on this advice (actions that will be contingent on their ability and willingness, say, to isolate).

Nor are these systems as automated as they appear. What we think of as automated systems tend to be backed in practice by scores of often-low-paid workers needed to make these systems work (Gillespie 2018; Irani 2015a). In this case, beyond the user's labour, somebody has to run the tests and ensure they're sent to the correct people. Neglecting this behind-the-scenes labour is a key way one can make companies look like 'technology' companies and thus improve their market valuation (Irani 2015a, 232). From the perspective of investors, technology companies may be perceived as having large profit potentials but little operating costs, whereas 'labour-intensive companies, on the other hand, increase their labor expenditures as their revenue increases' (Irani 2015b). This obfuscation of the role of labour in the tech sector instead celebrates those who have become our de facto experts on everything from urban planning to healthcare: 'Programmers, innovators, lean startups, and IT managers reinforce their claim as the celebrated actors of knowledge-economy projects – the brains that drain, circulate, and congregate in centers of capital' (Irani 2015a, 232–33). Contact tracing, moreover, is not just about identifying infected individuals. As philosophy of technology scholar Tamar Sharon (2020, 551) notes, 'Much of the work of human contact tracers has to do with ensuring that people have the material conditions required to sustain a 14-day quarantine, including food in their homes, the ability to care for children who may need to be removed, how to isolate in small spaces and when to seek medical attention.' Access to food and childcare and proper isolation practices are effectively downloaded onto the infected (or presumed infected) individuals.

The Oxford University *Science* article, for example, proposes that these apps could 'serve as the central hub of access to all Covid-19 health services, information, and instructions, and as a mechanism to request food or medicine deliveries during self-isolation' (Ferretti et al. 2020), downplaying – as the Covid Alert app does – the bureaucracy and frontline workers (who would be required to put themselves in harm's way to collect and deliver these meals) necessary to make this solution work.[9]

'The App Probably Won't Help Us Hurt You': Covid Apps, Trust and Privacy

Covid apps also took a very different approach to trust and privacy than do manual contact-tracing processes.

Manual contact tracing is one of the epidemiology's main pandemic-fighting tools. The purpose of manual contact tracing with respect to infectious diseases is to identify infected individuals and the people with whom they have been in contact. This can be a delicate process. Transmissible diseases are often accompanied by feelings of shame, embarrassment or fear. Identifying potential disease vectors thus requires that public-health workers 'build a relationship of trust' with the people they are interviewing, notes Sharon (2020, 551). This trust is necessary 'so that people feel safe revealing personal details', including personal contacts, and allow the health worker to provide them with the 'targeted information' that they might need to deal with the infection, such as whether or not to quarantine (Sharon 2020, 551). Trust between public-health workers and infected individuals allows public-health officials to engage in the surveillance that is necessary to map and fight pandemics.

Contact tracing is a form of data collection. Like all forms of data collection, it involves surveillance of individuals and groups, in this case by health professionals, who usually are employed by the state. Implicit in this approach is the idea that the more data amassed, the better equipped a society will be to fight a pandemic. Manual contact tracing, as Sharon (2020) notes, requires that (trained) contact tracers work to gain the trust of the people they work with, often to supply very private information, such as sexual encounters.[10] That manual contact tracing is about building trust makes the (non) decision to forego a dramatic expansion in manual contact tracing even more disappointing, a lost opportunity to increase social cohesion at a time when social bonds were being placed under significant strain.

If manual contact tracing is designed to maximize trust and data collection, Covid apps such as Canada's were designed based on a requirement of minimal trust. From the beginning and almost without exception, the focus on these apps' privacy protections was relentless, by governments, activists and the media. Early in the pandemic, in what can be seen as an example of

a contest over structural power between private and state actors, the French government decided to implement a centralized Covid-tracking system. In this system, some data would be sent to a centralized system to conduct the contact matching (BBC 2020). France's decision to favour a centralized system giving health authorities access to data – an entirely defensible and even necessary approach, if you're most concerned with ending the pandemic – involved 'open confrontation' with Apple and Google, who had decided on a decentralized application programming interface (API).[11] Decentralized systems, in contrast, keep all data on the user's phone. In the ensuing public relations onslaught, the French government was 'portrayed in the media as caring less about privacy than the tech companies did' (Sharon 2020, 554). This reflects a central conflict within a society marked by dataism: the battle to position oneself – company or government – as trusted users/producers/stewards of data (van Dijck 2014, 202–3). Given the numerous data breaches suffered by all the global platforms, to say nothing of their poor reputation post-2018's Cambridge Analytica scandal, that the tech companies came out of this with burnished privacy reputations is an impressive feat.

When Canada unveiled its app on 31 July 2020, its government webpage[12] was long on how it protected individuals' privacy, including links to Canada's privacy regulator, the Privacy Commissioner of Canada, with its attestations to the same. This was an app designed to minimize data collection without requiring trust in anyone.

To its designers' credit,[13] the Covid Alert app appeared to be everything that privacy activists could have hoped for. Every part of its design betrays an obsession with delivering an app that would not compromise individuals' privacy. Officials decided to make it a contact-notification app rather than a contact-tracing app. This decision not only eliminated a potential means for the government to collect data but also hampered the ability of health officials to trace the disease's spread – one of the principal goals of contact tracing. Data was stored exclusively on the phone, avoiding the creation of a centralized database that could also be used to discover patterns in the disease's spread. The app, during the time it was active, did not experience any privacy-related breaches or other such stumbles.

For their laser focus on preserving privacy, the government and the app designers (including an external advisory council led by a privacy lawyer and the head of a then-Canadian tech company) were rewarded with the blessing of the Privacy Commissioner (Canada 2020) and exhortations to download the app from some of Canada's leading privacy activists and experts (see, e.g., Semeniuk 2020; Geist 2020a, 2020b, 2020c).

In Canada's case, prioritizing privacy alongside (or even ahead) of pandemic mitigation came at a particularly ironic cost. As it turns out, the Covid Alert app designers had made the app so airtight, so protective of individual privacy that they'd left themselves no way to evaluate the app's effectiveness

in mitigating the pandemic. After all, you need to collect data to see if something is working, and the only way to collect data is via surveillance. Sold by the government with the promise that 'the app probably won't help us hurt you', as Sean McDonald, an early critic of the app, wryly put it (McDonald 2020), the near-exclusive focus on and privileging of privacy turned the Covid Alert app into the ultimate black box.[14]

Interpretations of Privacy

The focus on privacy in Covid app policy debates not only effectively prioritized the protection of individual privacy over societal health outcomes. It also privileged a corporate view of privacy over what we could call the epidemiological view of privacy.

The benefits of privacy are highly contextual (Nissenbaum 2004); more privacy is not always better. In a pandemic, too-strong individual privacy rights can literally be a killer, making it difficult for health authorities to stop the spread of a virulent disease.

The Covid app privacy debate reflected the interests and relative power of Google and Apple, the duopolists who supplied the operating systems on which these apps would run (Android and iOS, respectively) and who also set the terms and conditions under which governments could use these systems. It surprised many when the two companies proposed a joint API that kept data on phones and out of government (including healthcare officials') hands, reflecting the concerns of digital privacy activists (Sharon 2020). Generally left unmentioned was that these APIs effectively created a latent capacity for surveillance by these companies: 'Embedding the contact-tracing functionality in the operating system layer creates a dormant functionality for mass surveillance, whereby the contact-tracing microdata are under the control of Apple/Google' (Sharon 2020, 548). In other words, while the two companies promised not to collect users' data in this case, there's nothing beyond their word to keep them from doing so in the future, using the system they designed. Apple and Google's actions can be understood as a means to realize long-standing ambitions to enter the health sector, leveraging 'their data expertise and the large amounts of data they already have access to' to become 'important facilitators, if not initiators of data-driven health research and healthcare' (Sharon 2018, 1; see also Lupton 2018; van Dijck and Poell 2016).

Google and Apple's control over the operating systems needed to run these apps provided the two companies with structural power to shape the actions of countries' pandemic responses. Their privacy gambits transformed the app contact-tracing debate into a contest over who could provide the most privacy (from government, at least) rather than which approaches would best address the pandemic. Nor does the question of these companies' fundamental

suitability for such a project seem to have been considered. If effective surveillance is essential to a sound epidemiological response to a pandemic, and we cannot trust the companies offering these services – in part because their businesses are built to a greater or lesser degree on surveillance and data collection – then one has to wonder why the app-surveillance model was even considered in the first place.

It did not seem to register with most politicians or reporters that the Covid app debate should (or even could) be about anything other than maximizing individual privacy against government and (for the moment) Apple and Google snooping. That governments might have a legitimate need to engage in surveillance in the midst of a deadly pandemic was a second-order issue. It was a given that *of course* the Covid app debate should focus on user privacy and not health effectiveness. That it just made sense to talk about the app from this perspective is a testament to the power of the dataist and solutionist perspective in society today. These tools were seen as digital technologies first and healthcare instruments second.

The Covid app story also reflects changing ideas of who we consider experts. These include not just Apple and Google but also the privacy-focused digital-rights activists whose opinions were sought by journalists and who tend to share these companies' framing of the privacy dilemma, even if they often oppose their actions in other areas. This is not to say that privacy considerations are unimportant. On the contrary, worries that what surveillance scholar David Lyon (2022) calls 'pandemic surveillance' will continue in non-health areas post-pandemic should be taken seriously (see also Lemos et al. 2022). Such concerns around surveillance, however, should have raised questions about the suitability of depending on commercial platforms to deliver such sensitive services at all and been evaluated in a context in which other options, most notably a massive expansion in manual contact tracing, were considered alongside them. Instead, the starting point was the tech, not the problem. Instead of focusing on the best way to mitigate the pandemic, instead of considering how to build the trust that is the lifeblood of any society, let alone during a pandemic, the main challenge became maximizing users' privacy against governments and companies.

The Covid app debate offers a warning about how shifting discussions from a health to a commercial tech frame involves taking on the ideological and political baggage of the larger commercial tech debate. Treating contact-tracing apps as primarily a technological rather than a healthcare issue can lead to the adoption of policies/apps that might have been rejected out of hand if they had been evaluated as a normal policy intervention. As one would expect from a technological-solutionist mindset, that it might be a bad idea to place two tech duopolists at the heart of contact-tracing efforts seems not to have been much of a concern.

Covid App Postscript

The record of Covid apps as tools to fight the pandemic is, to be kind, mixed. Probably the most favourable report came from researchers studying the United Kingdom's National Health Service Covid-19 app. In England and Wales, between 24 September 2020 and the end of 2020, they estimated that the app – 'used regularly' by 28 percent of the population of England and Wales – prevented a significant number of infections (Wymant et al. 2021; Lyon 2022). By late 2021, however, almost two years into the pandemic, many governments had concluded that Covid apps had not delivered on their promise. Canada's Covid Alert app remained operational through the end of May 2022. Even before it was retired in June 2022, it had been rendered almost completely useless by decisions made by various Canadian health authorities that made it more difficult to get the code needed to notify the app of one's status (Wylie 2022).[15] Meanwhile, a report from the US Government Accountability Office (GAO) could not find evidence of the effectiveness of Covid apps in general, in part because, for privacy reasons, officials and the companies involved did not allow the apps to collect enough relevant information to determine their effectiveness. The GAO also noted that technological limitations of these Bluetooth-based apps affected their accuracy (2021, 27), as well as the apps' low uptake and delays in receiving verification codes, a problem noted also in Canada. More data to assess the effectiveness of these apps, the GAO argued, is required (US Government Accountability Office 2021, 27–33, 40).

ROADS NOT TAKEN

The most consequential change of the past several decades has not been digitization or the rise of the internet, but that it is now commonplace to assume that those with an expertise in data and computers are de facto experts in every area of human society. That we believe that Google *could* build a smart city or that a twenty-two-year-old tech student without medical training *could* design a vaccine-distribution system or that smartphone-based contact tracing *was* a good idea: that is the actual revolutionary change.

The issue is not technology but our attitude towards it. Technology undergirds activities throughout society – throughout Strange's four structures of finance, security, production and knowledge. These structures are all interrelated. As we discussed in chapter 2, the knowledge-driven society is characterized by the dominance of actors and priorities associated with the knowledge structure, and in particular with the US tech sector, often shorthanded as Silicon Valley. We are witnessing the spread of an ideology

– dataism – that emerged from Silicon Valley and is being applied throughout the other structures and throughout the rest of society.

Accepting dataism and a dominant role for technologists takes us down roads that we might not have otherwise chosen to follow. Imagine for a moment if the question of whether to spend time and money on Covid apps had been placed within a wider policy context that prioritized health protection first and foremost. In such a world, health officials' priorities, not those of Apple and Google, would have dictated how these companies' systems would be used and adapted to reflect health officials' perceptions of health and privacy challenges, including the French government's demands for a centralized system. Or perhaps, given concerns about the corporate use of health data, the idea of asking private companies to facilitate the surveillance of entire populations might have been rejected outright and other alternatives sought.

If health officials had treated these apps as just one possible policy response among others, concerns about their relative effectiveness may have been closer to top of mind. Given the apps' inability to reach key populations and their inherent technical limitations, perhaps officials, unencumbered by dataism and technological solutionism, would have spent much less, if any, time taking the apps seriously.

There is usually more than one way to approach a problem, and scarce resources mean that not all alternatives can be implemented. Governments could have poured war-footing money into a technology that we know works: manual contact tracing. At least where we live, the Ontario provincial government (provinces are primarily responsible for healthcare delivery in Canada) certainly did not do that, and it does not seem like it was ever seriously considered. Instead, in February 2021, the Ontario government invested CDN$2.5 million in a small 'start-up that began as an "ethical" ride-hailing company' to produce 'wearable bracelets to fight Covid'. Perhaps unsurprisingly, the company has since been the subject of a scathing *Toronto Star* report that, among other things, quoted current and former employees arguing that the technology 'never fully worked like the company, or the government, claimed they did' (Warnica 2021).

Avoiding dataism does not require rejecting data-collection or data-driven policy. It also doesn't mean that digital technologies should have no role in addressing social problems. Data is merely knowledge, and we need knowledge of the world in order to function in it, just as technology, used well, can improve our lives. What matters is the starting point of our policy discussions. We should not assume that digital technology *necessarily* will give us the best way to address the problems that we are concerned with. The problems that Waterfront Toronto sought to address in its original Request for Proposals for a smart city – housing, hunger, climate change – are important and real. And

they require data and technology to tackle them. Where the organization erred was by taking a one-dimensional view of these issues. Instead of starting with the problem – how can we make streets safer? – they accepted a proposal that started with the (technological) solution that redefined the problems to fit Sidewalk Labs' digital data-driven solution.

The technician's expertise celebrated by solutionism is a mirage. Data and algorithms are not magic. Dataism promises what it cannot deliver, whether it is precision that obscures the messiness of reality or the neutrality of algorithms written by people and forcing order on a world that by definition data and algorithms will never be able to represent fully. As the following chapters illustrate, habits of dataism are both seductive and hard to break. For this reason, it is important to recognize that dataism is an ideology first and foremost and that the problems that arise from our knowledge-driven society are as much ideological as they are technical, if not moreso. Consequently, dealing with them requires adjusting our thinking. Unfortunately, ideologies tend to die hard.

NOTES

1. See, e.g., https://creationmuseum.org/ (accessed 3 August 2021).
2. More precisely, it won the bid to come up with a plan to develop the land, with the possibility of continuing as a developer.
3. A common challenge with analysing algorithms is their 'black box' nature (Pasquale 2015), meaning that designers may make it difficult for outsiders to see or understand the variables and rules that comprise the algorithm's decision-making processes. Those crafting algorithms also often invoke trade secrets to shield their algorithms from external scrutiny, while claiming protection for their valuable commercial intellectual property.
4. This chapter was written months before the much-discussed November 2022 release of OpenAI's ChatGPT bot, which produces legible, if not always accurate, responses to plain-language queries. We do not address ChatGPT in this book; however, everything we discuss can be applied quite straightforwardly to the hopes and controversies surrounding generative AI.
5. That tech firms are often labour-intensive enterprises is obscured by the emphasis on 'tech', as we will discuss later in the chapter.
6. For other reports on Switch Health, see La Grassa (2020) and Levitz (2021).
7. In February 2022, Doroshin was banned from doing government or health work in Pennsylvania for a decade and is at the time of writing facing a civil complaint seeking US$30,000 in damages alleging that he violated 'Pennsylvania consumer protection, charitable solicitation, and nonprofit corporation laws' (Feldman 2022).
8. The Monitora Covid-19 app 'provides specialist medical attention remotely (through messaging via the application and telephone calls), geo-location data,

individual monitoring of case evolution and secure consolidation of data about the pandemic'. As Lemos et al. note, it is 'the tip of a broad network of data monitoring and medical assistance' in Brazil, involving '"intelligent" surveillance as the treatment of digital data through the use of specific algorithms in public data banks, on one hand, and coordinated and effective action by participating public healthcare agencies for patient care on the other' (Lemos et al. 2022, 84).

9. In Canada's case, officials were careful to note that the app was not designed to 'replace medical advice or manual contact tracing by local public health authorities' (https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html, accessed 30 April 2022). At the same time, however, the app was not effectively or fully integrated into the Canadian pandemic response, while also imposing a very narrow definition of 'contact'.

10. For a more general discussion of ethics and digital health, see Shaw and Donia (2021).

11. APIs regulate the interoperability between computer programs. Control over the API allows one to determine which programs can interact, and under what conditions.

12. See https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html. Accessed 31 July 2020.

13. The Covid Alert app was originally developed, based on Google and Apple's framework, by volunteers at Shopify, the Canadian backend ecommerce platform (see documentation at https://github.com/CovidShield/mobile; and https://github.com/CovidShield/mobile, accessed April 22, 2022).

14. On 9 February 2021, over six months after the government launched the app, officials modified the app to collect app metrics for the first time, such as the number of active users; the number of users whose app changed to the 'exposed' state; and the number of app users who entered a key while in the 'exposed' state (Health Canada 2020b). Technical performance metrics included the number of new installs; the number of 'date of symptom onset' or 'test date'; and the number of app users who have agreed to various app permissions (Health Canada 2020a). Based on this data, in July 2021 the government concluded that the app 'did not meet expectations' (Saint-Arnaud 2021).

15. This difficulty was related to the increasingly lackadaisical response to the ongoing (as of January 2023) pandemic by Canadian health authorities.

Chapter 6

Power, Data and the Private Sector

One of the key insights that emerges from the work of Susan Strange and Robert W. Cox is that, alongside states, non-state actors are also potentially consequential regulators. The concept of the state-society complex highlights how regulatory authority is not limited to the state: it can be undertaken by non-state actors, sometimes in competition, sometimes in cooperation, with the state.

This chapter focuses on the private, corporate side of the information-imperium state and explores the emergence of private actors as consequential regulators through their control over data and data governance. The focus on data as a key source of power has led companies to adopt business models aimed at exerting control over knowledge by commodifying data and claiming intellectual property (IP) rights over data-collecting and interpreting technologies, including in ways that encroach on areas such as healthcare that are often thought of as belonging to the public sector. This process involves a novel business model, the platform, which is designed to maximize opportunities to capture and exploit data, both personal and non-personal (Srnicek 2017).

Companies are increasingly positioning themselves as consequential data governance actors capable of exerting what can be understood as private data power. This chapter argues that technology companies exert structural power through data in two main ways: by using automated data analytics designed to forecast future events and behaviour and, second, through data-driven standard setting.

In an economy centred around the control of data, power resides with those companies capable of harvesting and processing vast amounts of data. Further, as this chapter examines, power accrues to those with the (claimed) ability to make interpretations of data that produce authoritative knowledge of behaviour or events. Data-driven technology firms argue that their capacity

to elicit insights from data, including claims of accurate forecasts of future events and behaviour, whether at the level of individuals or groups, can create widespread benefits. These purported benefits include services and products tailored precisely to individuals, as well as greater knowledge of and intervention in areas of future risk, such as a propensity for specific diseases or likelihood of vehicle accidents. Knowing ourselves better through data, they argue, delivers concrete, actionable knowledge for businesses and governments alike, or so they claim. Despite these promises, using data to forecast behaviours and outcomes creates multiple problems, including in many cases overexaggerated claims of accuracy. In particular, employing automated data tools to quantify and predict human behaviour, whether at the level of individuals or groups, can exacerbate existing discrimination and inequality, shutting some people out from accessing core government services or unfairly intensifying surveillance on some populations.

Alongside their claimed capacity to make precise data-driven forecasts, companies also exert data power through standard-setting behaviours. While the standard setting is often associated with governments, private actors also play a key role in setting and enforcing standards (see Braithwaite and Drahos 2000). At their most basic, standards can be understood as the ways that things are done (see Bowker and Star 2000). A classic example is the 1980s videotape format war between Sony's Beta and JVC's Video High Density (VHS): despite being a technically inferior format, the latter won and became the unrivalled standard, at least until the introduction of DVDs (see Cusumano et al. 1992). In the data-driven economy, companies that offer key products and services can set the standard for how things work. For example, in China, Tencent's WeChat Pay, introduced in 2013, had become by 2015 a standard for how payments are made, through its role as an intermediary that brings together different financial entities in a commercial transaction through its QR codes, enabling people to seamlessly pay for goods and services with their phones (Plantin and de Seta 2019).

This chapter considers technology companies' efforts to exert power as standard setters by exploring their expansion into the healthcare field. Technology companies, including Amazon, Palantir, Facebook and Google are applying their expertise in data analytics to health datasets in order to build the next generation of diagnostic and treatment tools, as well as to manage the delivery of healthcare. In doing so, technology companies are endeavouring to set standards, through the creation of data-driven technologies, for how healthcare is delivered and, more broadly, understood as a service.

With private data power comes risks that large actors may be able to translate their capacity to amass, interpret and control insights from data into monopolies over data. Actors are able to create private data power through their capacity to maintain proprietary holds over datasets and capture a

significant share of economic value produced by data and to create advantageous data monopolies. The societal risks from data monopolies, like other monopolies, include stifled innovation, higher prices, greater barriers to entry and wealth disproportionately captured by 'data-opoly' actors. Further, as chapter 3 lays out, the knowledge underlying the creation of the data tools or technologies is typically held as proprietary knowledge and protected by IP rules, with the result that others may be locked out from accessing or building upon this knowledge.

To explore the private, corporate side of the information-imperium state, this chapter is organized into four sections. Building upon the central assumptions underlying the data- and knowledge-intensive global economy, discussed in chapter 3 with respect to IP, the first section describes the nature of this data-driven platform economy as well as its key actors, including the data broker industry.

The second section examines a key premise of the data-focused society – that actors capable of amassing and processing vast amounts of data using automated tools can forecast future events and behaviour by profiling individuals and groups. As we will see, however, companies' controversial claims of predictive power rest upon shaky foundations of data accuracy and the precision of automated tools.

Third, the chapter examines how private actors exert power through data-driven standard setting with a focus on technology companies' expansion into the health sector. Google, with its artificial intelligence (AI) company DeepMind and its 2019 acquisition of the wearable company Fitbit, epitomizes technology companies' expansion into healthcare and the consequent risks of data monopolies. Finally, the conclusion reflects upon the consequences of private data power, particularly in terms of anti-competitive effects and harm from biased, discriminatory data practices.

UNDERSTANDING THE DATA-DRIVEN ECONOMY: OF PLATFORMS AND DATA BROKERS

In chapter 3, we discussed how the franchise model of industrial organization captures a key element of how companies use control over IP rights to appropriate profits and exert control across global value chains (Schwartz 2021). When it comes to data, it is the platform that is becoming the dominant business model. Conversations regarding platforms require an extra degree of precision because, as discussed in the book's introduction, companies often strategically describe themselves as 'platforms' as a rhetorical ploy to obscure their economic power and disguise their data-extractive business models, as well as to stymie government regulation.

To define platforms, we draw on IPE scholar Nick Srnicek's insightful book *Platform Capitalism*. Platforms at their heart, Srnicek argues, 'are an extractive apparatus for data' (Srnicek 2017, 48). They have business models 'capable of extracting and controlling immense amounts of data' (Srnicek 2017, 6). Platforms do so by positioning themselves as two- or multi-sided markets capable of extracting data to use 'so as to optimise production processes, give insight into consumer preferences, control workers, provide the foundations for new products and services (e.g., Google Maps, self-driving cars, Siri), and sell to advertisers' (Srnicek 2017, 40–41). Two-sided markets place companies in a privileged position to shape both sides of the market, an advantage that accords the entities significant economic and social power, including the ability to act as regulators, over their users and the relationships between the suppliers and users on the different 'sides' of their business (Dunne 2021, 244, 248).

As international political economy scholar Martin Kenney and his co-authors note, the platform model has become increasingly prevalent and influential. They estimate that in the United States, '70% of service industries, representing over 5.2 million establishments, are affected directly or indirectly by one or more platforms' (Kenney et al. 2021, 1452). Platforms have also 'increasingly shaped' non-platform businesses, including 'how customers found and interacted with them, how they hired, handled paperwork (information and data), connected with customers, and shipped products' (Kenney et al. 2021, 1453).

Much of a platform's power comes from network effects: the more people or groups that use a platform, the more valuable and essential it becomes. The larger a platform and its user base become the more data, rent or value can be extracted, which also facilitates the company's expansion into different business sectors, thereby raising competition issues (Srnicek 2017; see also Hutchinson 2022). The structure and business models of platforms facilitate the creation of monopolies, or what Srnicek refers to as 'the natural tendency toward monopolisation' (Srnicek 2017, 45). Amazon, for example, capitalizes upon the data it collects from buyers and sellers on its massive marketplace to launch its own product lines, essentially exploiting third-party companies' data for its marketing research before undercutting them and promoting its Amazon-branded products (Khan 2019). Amazon's ability to expand its marketplace into shipping and logistics, cloud computing, a microwork platform (i.e., Mechanical Turk), content delivery and physical devices is based on its access to data across all of these disparate sectors (Kenney et al. 2021, 1470).

By bringing 'together different users: customers, advertisers, service providers, producers, suppliers, and even physical objects' (Srnicek 2017, 43),

the platform becomes 'the ground upon which [users'] activities occur, which thus gives it privileged access to record them'. This business model grants platforms not only access to data but also 'control and governance over the rules of the game' (Srnicek 2017, 44, 47) and enables privileged access to datasets that can be used to train algorithms (Hutchinson 2022, 14). Here we can see how data companies can raise concerns of monopolistic behaviour through their control over critical networks in the market, a problem intensified through their creation of proprietary ecosystems that lock out competitors, and their data capture of rivals' business practices (see Khan 2019). One solution to counter monopolies, anti-trust proponents argue, is a structural separation that prohibits dominant actors from directly competing with the businesses reliant on their services (Khan 2019; Rahman 2018). Structural separation would not allow, for example, search engines, social media, app stores or marketplaces to operate those services and compete directly with third-party businesses reliant upon those services (see also Wu 2018). To fully address anti-competitive behaviour, however, regulation that addresses the monopolistic control over data is also necessary, as dominant incumbents, such as Google Maps, have a significant advantage over other actors through their control over the underlying datasets (Khan 2019).

Data Monopolies

The platform model is designed to capture and exploit data, both personal and non-personal. Their business models operate by amassing as much data as possible from existing products and services, such as from sensor-studded tractors or web-based gig economy services like Airbnb. The more activities a company has – in products, services or other interactions with businesses or customers – the more data there is available to be extracted, the more value generated and the more future activities that may be accessed and thus new data acquired (Srnicek 2017, 45). This practice of data accumulation in which the value accorded to data increases as the amount of data grows facilitates data monopolies as companies centralize their troves of data. One way that platforms establish data monopolies is by crafting proprietary ecosystems that privilege their goods and services while excluding competitors (Srnicek 2017). Amazon, for instance, operates as a data monopolist in its operation of a dominant market platform and its provision of its own branded goods and services on that platform.

The 'tendency toward monopolisation is built into the DNA of platforms,' explains Srnicek (2017, 95), with network effects helping to ensure that the more users a platform has, the more data generated and the more valuable the platform becomes. Actors that control large datasets and have the

technical and commercial infrastructure necessary to analyse data, including algorithms, can further generate value from data by extracting insights that they calculate may have economic value, whether currently or at some future point (see Andrejevic and Burdon 2015). Those who possess large datasets and the means to interpret data are also better placed to offer predictions of future events and behaviour, a new source of data power that this chapter explores. Creating and controlling datasets, including that of proprietary data interpretations, can lead to 'new concentrations of power' (Crawford et al. 2014, 1667) that determine how data and digital technologies are used. Data monopolies, in other words, enable key data actors to shape the terms on which others are able to engage in the data economy.

Mapping the Data Economy

In a map of the global data economy, the poles of platform power are obvious and tilted nearly exclusively towards the Global North. Dominant platforms are largely based in the United States and, to a lesser extent, in China, with only a handful of major companies located outside these countries. These dominant actors extract the most value from the 'data value chain', meaning that they have the technical and commercial capacities to transform information into valuable, proprietary data insights that can be 'monetized for commercial purposes or used for social objectives' (United Nations Conference on Trade and Development (UNCTAD) 2021, 17).

Referring to this new global order, scholars use terms like 'platform imperialism' (Jin 2015) or 'data colonialism' (Couldry and Mejias 2019) to underscore the concentration of power amongst a small number of companies in a few largely Global North locations, with the rest of the world on the periphery, including nearly all of the Global South. This Global North/South dynamic is also evident in the data value chain where companies, generally in the Global North, dominate the high-value processes of amassing and processing data into a commercial asset. These dominant Global North data-driven companies are knowledge feudalists, disproportionately benefitting from the capture and interpretation of data. In this process, 'developing countries may find themselves in subordinate positions, with data and their associated value capture being concentrated in a few global digital corporations and other multinational enterprises that control the data' (United Nations Conference on Trade and Development (UNCTAD) 2021 xvi).

In addition to replicating the traditional colonialist Global North/South patterns of resource extraction in relation to data, the dominance of Global North companies also raises competition problems when these companies operate as data monopolists. Consider the example of Google. The company dominates the search and digital advertising industries, and, together with Apple,

Google operates a duopoly on operating systems and app stores (Nieborg et al. 2020). Google's prowess with data, specifically its data analytics capacity, enables it to move into other industries, from mapping and advertising to autonomous vehicles and healthcare.

In the data-driven economy, platforms headquartered in the United States play an outsized role.[1] Alongside Google, discussed previously, Meta, Facebook's parent company, plays a dominant role in the digital advertising industry, while Meta's companies – Facebook, Instagram and WhatsApp – are dominant players in social media. Meanwhile, Apple and Microsoft dominate popular hardware and software products, and Amazon, Microsoft and Google are amongst the largest cloud service providers.

China has worked to challenge the dominance of American platforms with its own 'national champions': Baidu, Alibaba and Tencent (Fuchs 2016; Jia 2021; Jiang and Fu 2018), all of which have global ambitions and are expanding rapidly outside of China. They offer mobile payment (Alibaba's AliPay and Tencent's WePay), search (Baidu), marketplaces (Alibaba's Taobao, Alibaba and Tmall), social networking (Tencent's WeChat, in addition to ByteDance's TikTok, which in China is known by the name Douyin) and various other services including cloud services, AI, video-on-demand services and video gaming (Chen et al. 2018; Shen et al. 2020). Although their revenue is still largely generated within China (Jia 2021), their emergence is in line with Chinese ambitions to become a knowledge-feudalist power, expanding globally its technology sector and, more broadly its technological power, touching on infrastructure projects in Africa and Asia, as we discuss in chapter 8.

How Companies Acquire Data: The Role of Data Brokers

In the popular imagination, the data economy is dominated by particular types of companies, such as online companies like Google and Tencent, gig economy companies like Uber and Airbnb and the data broker industry, which we discuss further next (Crain 2018, 2021). In reality, the data economy is far more pervasive. Traditional manufacturing companies, such as John Deere (agriculture equipment) and General Motors (automobiles), have adjusted their business models to capture value from collecting and parsing data from their users and production processes (Srnicek 2017).[2] As companies retool their activities to capture more and more data, it becomes more difficult to draw the line between the data economy and the economy as a whole.

A data-driven economy requires that actors have access to mass amounts of personal and non-personal data, while dataism supplies the ideology core to the information-imperium state that treats such large datasets as valuable forms of knowledge (chapter 4; boyd and Crawford 2012). Companies in a data-driven economy thus have a significant economic interest in amassing

and acquiring proprietary control over high-quality data, accessing or combining existing datasets, as well as in the data-processing capabilities that make large datasets useful.

Companies can acquire data in several ways. Most obviously, they can collect it themselves, such as Fitbit amassing health data from fitness wearables, or through Google tracking user searches and IP addresses. This is the basis of the platform business model. Companies can also use publicly available data (collected, say, by government bodies such as statistical agencies) or purchase access to datasets from other actors, including data brokers.

In an economy that runs on data, the data broker industry plays a central role. This industry is comprised of a vast array of companies that buy, license and resell personal information about consumers from a variety of public and private sources, largely without consumers' knowledge (Federal Trade Commission 2014, i). Within this industry, multiple layers of data brokers trade data with each other, making it difficult to gauge the size of the industry, either globally or within individual countries (Federal Trade Commission 2014, iv).

Although such actors use a number of different terms to describe themselves and their practices – marketing analytics, data analytics, data providers, database marketers (see Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic 2018) – they are best thought of as 'information resellers' (Kuempel 2016).[3] They are 'data intermediaries' (Beer 2018, 476), the 'invisible middlemen' (Kuempel 2016) in the data economy that sell data to government and law enforcement agencies, as well as to advertisers, marketers and political campaigns (see Christl 2017). From this perspective, we can consider a wide variety of actors to be data brokers, including major credit-reporting agencies such as Equifax, Experian and TransUnion; firms in the risk-analysis industry like PricewaterhouseCoopers; and significant players that are likely not household names, like Acxiom, Accenture, and Relx, which owns LexisNexis. Google and Meta, which make most of their money selling data-driven targeted ads, are also data brokers through their use of their proprietary datasets on their users' demographic profiles (Venkatadri et al. 2018, 1).

Data brokers function by obtaining consumer information, including purchase habits and web-browsing activities from diverse sources, including retailers, service providers like telecommunication companies and financial institutions, marketers and non-profits and charitable organizations that sell their membership lists (Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic 2018). Consumer data also includes information from software-enabled devices (which we will discuss in chapter 7), like smart televisions, thermostats, vehicles and fridges, that effectively grant brokers unprecedented access to people's homes and their private lives (Christl 2017; Christl and Spiekermann 2016).

Data brokers contend that their industry can, among other things, deliver effective customized advertisements to consumers and help companies avoid fraud by providing accurate financial profiles of customers. However, the industry's use of consumer data also poses risks, not least because it enables companies to target individuals and groups for less-than-noble purposes, such as marketing risky financial products to highly indebted people (see Federal Trade Commission 2014). Furthermore, while data brokers typically stress the accuracy and completeness of their data holdings, there have been multiple cases in the United States in which people were denied housing or rejected from jobs because they failed background checks due to inaccurate information passed along by data brokers (see Kirchner 2020).

Given these problems, and the data broker industry's notable opacity, governments and regulators in Canada (Canada 2014), Norway (Norwegian Consumer Council 2020), Australia (Australian Competition and Consumer Commission 2019) and the United States (United States Senate Subcommittee on Fiscal Responsibility and Economic Growth 2021), among others, have been active in studying the industry. Among other measures, these inquiries are examining whether – and, specifically, how – privacy or data-protection laws need to be amended to limit the trade in personal data. In the European Union, which is at the forefront of state efforts to regulate the data-driven economy, data brokers' activities are subject to the General Data Protection Regulation (GDPR), which requires individuals' consent before their data can be collected. Such restrictions, however, are somewhat mitigated by a loophole that allows for data collection to occur without consent if it is done 'for the purposes of the legitimate interests' of the actor doing the collecting or a third party (European Parliament 2016 GDPR Art 6(1)(f)).

How Companies Extract Meaning from Data

Single points of data do not have much value on their own. Rather, data acquires value as tools combine and interpret datasets to discern new patterns (Andrejevic and Burdon 2015). Being able to interpret data, specifically to extract meanings of importance to businesses or governments, is a source of social, political and economic power.

For example, data analytics firms, which are part of the broader data broker industry, exemplify the practice of generating economic value by processing and extracting meaning from data, for example, by identifying market demand for a particular product. Analytics firms market their data-derived insights 'in easy to consume forms that require little technical expertise' designed to 'reveal hidden value in the data, they shine a light on organisations and show things that were previously invisible' (Beer 2018, 476). They present their product as a 'competitive necessity' (Beer 2018, 476),

the implication being that actors not taking advantage of the knowledge that data delivers are squandering market opportunities, thus leaving them at a competitive disadvantage to those taking advantage of their services. This is the very essence of dataism.

To extract insights from large datasets, researchers commonly employ what is colloquially called artificial intelligence (AI). At its most basic, AI can be defined as computer programming that 'learns' from and adapts to data (Verdegem 2021, 5). Although computer scientists differentiate algorithms, machine learning and AI and define each precisely (see Koch et al. 2021), the concept of 'AI' has become a popular umbrella term describing a broad set of technologies that use statistical modelling to identify insights and make predictions (Jansen and Cath 2021, 184). The development of such tools typically requires large volumes of detailed, high-quality data to 'train' and test the tools before they can be commercially viable products (Koch et al. 2021).

DATA POWER THROUGH PREDICTION

Companies are shifting their business models towards a data-driven model that accords economic value to interpreting and commodifying data. Those who market themselves as being able to discern specific knowledge or truths from personal data, which is the key achievement of data brokers and platforms, also position themselves as sources of legitimate expertise, as chapter 5 explains. These claims to knowledge can be future oriented, such as revealing which job seekers might make better employees or which parolees might reoffend: assessments that are difficult – even impossible – to forecast accurately and can have significant ramifications when incorrect.

We've all likely had the experience of being followed by digital advertisements across the web or had an uneasy feeling when we learned that companies like Meta or Twitter have placed us in a particular marketing category because of our interests, demographic features or purchasing habits. Companies acquire data to profile us, to discern patterns that may indicate potential future behaviour or events. In the data-driven society, social and economic power is accrued not only by amassing and interpreting data but also by making claims that such data can deliver accurate predictions, whether through forecasting at the level of individuals or of groups. Data power, in short, goes beyond interpretations that produce knowledge of behaviour or events: power is also expressed via claims of knowledge of the future. Profiling is a type of future-oriented knowledge construction designed to discover or produce new information about groups or individuals through algorithms or other automated techniques (Hildebrandt 2008a, 17). Automated profiling is a type of forecasting or prediction in which 'the correlations stand for a probability

that things will turn out the same in the future' (Hildebrandt 2008a, 18). It is based on the dataist assumption that, with the proper application of automated tools to large datasets, accurate predictions are possible and, for industry, commercially valuable.

While the expanding scope and number of datasets and advancement in automated data-collection and processing tools have made profiling commonplace, attempts to quantify and forecast human behaviour through data are nothing new and long predate the computer. For example, the roots of contemporary data-driven surveillance practices within the financial system can be observed in the early commercial and consumer credit bureaus, with the latter emerging in the 1870s in the United States following the establishment of commercial credit rating systems (Lauer 2017). Similarly, insurance companies began offering life and disability insurance to Americans in the 1910s, necessitating the collection of detailed demographic and employment data, as well as health and mortality data, to create and manage insurance policies (Klein 2006). From the origins of the modern financial and insurance industries, tracking people through their data in order to forecast their clients and potential clients' creditworthiness or their potential for risky financial behaviour has been a standard practice.

Underlying companies' application of automated tools to large datasets is the dataist assumption that human bodies and social interactions can be precisely quantified and, with the proper application of data using automated tools, that one can produce accurate predictions of future actions (see chapters 4 and 5). Those creating and operating automated data tools to quantify and then predict human behaviour may emphasize the rigour of their analysis through claims that they are constructing accurate, unbiased datasets and using unbiased rules in building their algorithms. Claims of data accuracy, completeness and objectivity, however, are often unfounded and even impossible. More importantly, despite dataist claims of accurate measurements and forecasting given the right application of tools and large datasets, it is not evident that complex human behaviour can be predicted to the degree promised by these new digital tools. In short, promises of precise future-oriented knowledge may not match reality. This section examines how companies profile individuals and groups to forecast, track and influence behaviour, while chapter 8 examines the equivalent situation with respect to governments.

As chapters 1 and 4 point out, data is not neutral, and algorithmic bias is a long-recognized problem with serious consequences. For example, ten widely used health algorithms in the United States were found to have allocated greater healthcare resources to white patients with conditions like diabetes or kidney problems in contrast to Black patients with the same medical conditions (Obermeyer et al. 2019). Algorithms can be discriminatory in their

application because they were designed and trained on racially biased datasets, examples of which can be found in the financial sphere. For instance, Black borrowers of bank loans in the United States often continue to pay higher rates or are rated as higher-risk borrowers in comparison with white borrowers with similar financial profiles (Park and Quercia 2020). This discriminatory practice stems, in part, from the US-government-sponsored segregationist housing practice termed 'redlining' from the 1930s to early 1960s, in which financial institutions denied Black people loans and rated Black-majority neighbourhoods as higher risk than white-majority neighbourhoods (Park and Quercia 2020; Rothstein 2017). As a result, when algorithms are built using data based on racist policies, the resulting profiles can exacerbate existing discriminatory practices in which certain groups pay higher prices for financial services.

Despite the risks arising from erroneous, discriminatory predictions, and despite case after case of such discrimination, the use of algorithms to deliver data-driven predictions has become commonplace in a wide variety of areas, including the criminal justice system (Brayne 2020), health (van Dijck and Poell 2016), immigration (Kenyon 2018) and, probably the circumstance most familiar to people, advertising. Advertising enables the web's grand bargain: key services including search, social media, messaging and email, and mapping are offered free to the public in exchange for their personal data. Business models based on digital advertising – that is, based on using micro-level behavioural data to understand and predict people's interests and habits – form the economic foundation of the web (see Crain 2021; Hwang 2020; Wu 2016). Social media companies operate as digital advertisers, amassing, parsing and selling what they promise is their customers' accurately detailed demographic profiles, as do data brokers with third-party data they've acquired from other companies (see Crain 2021). What's being sold are predictions of consumer habits (Wu 2016).[4]

People are likely most familiar with data-driven predictions carried out at the individual level. In this scenario, data is collected on a single person to discover or create knowledge that, when algorithms are applied to discern patterns in data, can reveal information about specific individuals' future behaviour, interests or habits (Hildebrandt 2008b, 304). Companies may use this data to infer when people are at the cusp of major life changes like graduation, first-home purchase, pregnancy or retirement. Financial institutions use data-driven profiling to determine an individual's financial status as creditworthy or a credit risk based on spending behaviour and, increasingly, assessment of social data from people's social media networks. Likewise, insurance companies are increasingly basing their rates on data from customers who use self-tracking wearable technologies like Fitbits (Cevolini and Esposito 2020). Wearable technologies provide the insurers real-time data on individual behaviour, including sleep and fitness levels

(see Lupton 2017), with the idea that insurers can establish strong correlations between past and future behaviour to make individualized predictions of risk (Horan 2021).

Profiling does not just target individuals. Group profiles sort people into different 'groups', or 'clusters', or 'categories', to find shared features or to define categories of individuals sharing some properties (see Jaquet-Chiffelle 2008). The goal of group-level analysis is to make group-level inferences in terms of the interests, activities or propensities for certain health conditions or specific risky behaviours among members of that group. The aim here, which emerges directly from the dataist ideology discussed in the previous chapter, is to use the power of data to provide precise forecasts based on hidden correlations to enable someone to act upon the information (see Hildebrandt and Gutwirth 2008). Companies, for example, could market healthcare screening or preventative treatments to people at risk of developing certain diseases. More negatively, they can use such profiling to deny services or credit to members of a group with characteristics deemed to be undesirable.

Group profiling can involve identifying pre-existing groups, such as people who use fitness wearables, whose 'members' have self-selected by using wearables, even if they don't know other group members. These 'naturally' existing or self-defined groups differ from so-called algorithmically created groups. Algorithms may 'create' or 'discover' groups, newly created categories of people not drawn from a pre-existing group whose members may not be aware that they have been included in the group (Kammourieh et al. 2017). People who complete online health questionnaires or submit DNA swabs to ancestry sites, for example, may have consented to have their health information used for research purposes. However, they may be unaware that an algorithm has grouped them into a particular category, for any number of purposes, including having a predisposition to develop a medical condition, data that insurance companies could use to deny healthcare coverage.

Such practices are examples of data commodification. Data is transformed into a fictitious commodity (to use the language we introduced in chapter 1) when it is appropriated into a context beyond the intentions of the subject from whom the data was taken. People submit their DNA in order to find out something about their past, but this data can be sold and repurposed for many other reasons. For example, insurance companies could use this data to deny or limit coverage to people whose genetic tests find are predisposed to specific genetic conditions, a form of genetic discrimination (Tiller et al. 2020).

Algorithmic categorization based on genetic data can reveal information about entire families, raising concerns of genetic discrimination even for those 'who share a certain genetic architecture but are not aware of it' (Taylor et al. 2017, 229). This type of categorization raises significant concerns. It highlights a key power dynamic in the data-driven economy: individuals can lose control over their data, which can then be used in ways to which

the original data subject might object. These decisions can have effects that reach beyond the individual whose data is being repurposed. Brenda McPhail, director of the Privacy, Technology & Surveillance Program at the Canadian Civil Liberties Association, notes:

> It's not just about whether or not your data is going to be used against you or for you, it's about whether or not your data is going to be used to categorize you and then affect a whole category of people.[5]

That individuals' data can be used in ways that affect others reveals a key limitation in data-privacy legislation, such as the European Union's GDPR, that are based on protecting individual, rather than group, rights. We explore this point further in chapter 9.

Reassessing Data-Driven Prediction

Profiling offers the tantalizing promise of future, predictive knowledge. For the insurance industry, for example, it offers the potential to adjust pricing in ways that better reflect the actual risks posed by an individual or group of individuals. Companies working within a dataist mindset can then act on this knowledge to increase prices for perceived risky customers or even deny them coverage altogether. In doing so, algorithm designers claim that data-driven prediction can unlock benefits ranging from more efficient planning, personalized services and pricing (see Cevolini and Esposito 2020; Horan 2021). Insurance companies offer discounts on premiums to people who install a telematic device in their vehicles that records all driving data like speed, braking patterns and even time of day and places they drive. This enables companies to collect detailed datasets that they can use to further refine their models to determine what groups of people should be charged higher premiums for having what the models determine is 'risky' driving behaviour, which can include something as commonplace and unavoidable as driving at night (Cevolini and Esposito 2020).

Automated profiling builds upon the financial and insurance industries' practices of modeling potential future risky behaviour and ambitiously expands these practices to all aspects of human behaviour. Underlying automated profiling is the dataist idea that human bodies and behaviour can be accurately quantified and that this data can form the basis of reliable, actionable predictions. Like traditional insurance models, these automated models sort people according to their 'propensity to behave in a certain way, rather than as individuals' who have specific behaviour (Taylor 2017a, 31). Automated profiling programs, for instance, may categorize people as risky for defaulting on loans or reoffending because of the characteristics that an individual shares with others

in the model's grouping. Patterns may emerge, in other words, but because of the size of the datasets and the complexity of the automated data tools we may not fully understand why patterns emerged or whether those patterns are connected to other variables or are random occurrences.

Further, in keeping with the dataist faith in correlations and the marginalization of theory and context (chapter 5), automated profiling tends to accord considerable importance to understanding past events and behaviour to make future predictions. The past, simply put, is understood as inherently useful to predict the future. Algorithms identify correlations within datasets, often based on past behaviour, but they may not establish the reason for those correlations or related causal factors (Hildebrandt 2008b, 18). Human behaviour is complex. Past behaviour is not always a reliable indicator of future actions. There may be multiple reasons, for instance, that someone convicted of a crime in the past may not necessarily commit another crime, including stronger family ties, finding employment or treating substance abuse problems. These and other characteristics, moreover, may not be captured (or capturable) in companies' actually existing datasets, themselves guaranteed to be of varying quality. Additionally, as discussed earlier in this chapter, applying automated tools to biased or discriminatory historical datasets merely replicates those biases in the profiling results.

Critics of profiling in the financial and insurance industries point to problems like their often-discriminatory treatment of racialized customers (Park and Quercia 2020; Rothstein 2017). As problematic as these industries are, the tech industry has intensified concerns with its development of the automated profiling of bodily data, a phenomenon some researchers term 'physiogenomic artificial intelligence' (Stark and Hutson 2021). In this field, researchers are using automated tools to examine physical or physiological characteristics, including face, eye, hand, voice, gait and heart rate, and from that bodily data infer or categorize a person's character, traits like race, gender or sexuality, or future behavioural or social outcomes (Stark and Hutson 2021, 10). From an analysis of facial features, some researchers claim they can accurately determine sexual orientation, political affiliation, trustworthiness and potential criminality, including propensity for terrorism or extremism (see Stark and Hutson 2021). Others are developing voice profiling, a practice employed by marketers in which they collect data from voice applications like Alexa to try to determine physiological characteristics (e.g., fear or anger) or linguistic patterns (e.g., signalling lying or truthfulness) (Turow 2021). Parsing bodily data, in other words, is thought to reveal fundamental truths about personal traits, interests and future actions.

Commenting on the application of automated data tools to predict human behaviour, computer scientist and AI expert Arvind Narayanan argues that while there has been 'genuinely remarkable scientific progress' in AI,

> much of what is sold commercially today as 'AI' is what I call 'snake oil'. We have no evidence that it works, and based on our scientific understanding of the relevant domains, we have strong reasons to believe that it couldn't possibly work. (Kaltheuner 2021, 23)[6]

In particular, Narayanan calls out as 'pseudoscience' automated products that claim to predict social outcomes, like who may commit a crime, because these futures 'are all contingent on an incredible array of factors that we still have trouble quantifying – and it's not clear if we ever will' (Kaltheuner 2021, 24). This is because using automated tools to profile bodily data in order to substantiate claims of insight into human behaviour, characteristics and interests pushes the boundaries of what is technically possible – or ethically acceptable. For instance, claims that facial features and expressions can reveal insight into people's social attributes like sexuality or character, including trustworthiness, rely upon debunked research that the 'meaning' of facial expressions is universal across societies (for a critique of these claims, see Durán et al. 2017). Absent a universal standard of facial expressions, for example, dataist claims to predict social traits based on such characteristics fall apart.

Some applications of these bodily data-driven technologies might appear relatively mundane, although discriminatory, such as the use of facial data to predict matches on dating sites. However, technologies that claim to identify gender identity or sexual orientation, for example, in states with anti-LGBTQIA+ laws could result in discrimination, denial of services or monitoring by government agencies.

Using automated tools to infer a person's traits or future behaviour from their gait, facial features or other bodily data is a high-technology version of phrenology, the discredited, racist pseudoscience used to justify social hierarchies and colonialist practices, including the slave trade (see, e.g., Browne 2015; Benjamin 2019). Researchers in the AI field use the term 'cheap AI' to explain the power dynamics at play here: elite corporate actors develop and test the technology and 'suffer little cost' in doing so, while those serving as the 'testing grounds, frequently those at the margins of society, pay the heaviest price' (Birhane 2021, 43).

Dataism is a core element of private data power, particularly evident in companies' claims of predictive accuracy. Businesses market their forecasts as having utility and certainty, while others accord those forecasts with social and economic legitimacy. In short, data-driven forecasting is powerful because businesses and governments act *as if* the predictions are valid, reliable representations of reality, which are core elements of dataism. Structural power is evident in companies' claims of predictive knowledge to which others accord social and economic value, including governments. Commercial actors that can credibly claim to interpret data, in this case of future events or

behaviour, wield power in producing the knowledge that they claim the data provides. This power is consequential, as profiling, produced by opaquely operating automated tools, may negatively affect people's lives, such as denying employment or access to government services or increasing costs of services like insurance or healthcare.

POWER THROUGH STANDARD SETTING

As Strange notes, structural power is the ability to set the rules and conditions under which others operate. Structural power can be exerted most obviously through laws, but also in other ways, and not only by state actors. Standards, for example, are the norms, goals, objectives or rules around which a regulatory regime is organized, a broad definition that encompasses the efforts of public, private or hybrid collaborations of actors (Scott 2010, 104). Just as private actors can exert structural power through their dominance in a particular sector (think of Amazon's monopoly position as a dominant marketplace and major seller of goods in that marketplace), private actors' capacity to set standards, typically in ways that serve their commercial interests, can be a form of structural power.

Chapter 5's examination of Covid-notification apps, for example, illustrated the power that Google and Apple wield as duopolists supplying the mobile operating systems on which these apps would run, as well as operating the app stores through which people would access the apps. Google and Apple, in short, wield structural power as they set the standards for any app to be distributed through their stores. Every app creator must comply with the rules that these companies determine for their app stores. Apple's rules for its app store, for example, prohibiting 'overtly sexual or pornographic material' on apps (Apple n.d.) constitute a standard.

Standards can also be understood as sets of agreed-upon rules that span more than a single community of practice and can be deployed over distance (Bowker and Star 2000, 14). For example, companies, often in cooperation with states and civil-society groups, have designed technical standards relating to the internet's physical infrastructure to realize a design goal of global interoperability (ten Oever 2021). Standards, as legal scholar Harm Schepel argues, can 'hover between the state and the market' and are 'very rarely either wholly public or wholly private; and can be both intensely local and irreducibly global' (Schepel 2005, 3; cited in Peters et al. 2009, 12).

Private actors have a long history of exerting power through standard setting (see especially Scott 2010; Peters et al. 2009; Cutler et al. 1999; Braithwaite and Drahos 2000). Standard setting, as regulatory scholars John Braithwaite and Peter Drahos argue in their groundbreaking book *Global*

Business Regulation (2000), is a means by which multinational corporate actors can exert power to further their commercial interests by enrolling national and international organizations to meet their regulatory goals.

Private actors are involved in standard-setting bodies like the International Organization for Standardization (ISO), Underwriters Laboratories, which certifies electrical products, and the Forest Stewardship Council, which promotes responsible forestry management (Grabosky 2013). Here, actors determine what constitutes the standards of 'safe' electrical products or 'sustainable' forest practices. Outside formal organizations, individual companies like McDonald's and Wal-Mart also have considerable market power to institute de facto standards. They do so in areas such as labour and food safety for their domestic and foreign suppliers via their global supply chain contracts. Some scholars term this form of private regulatory power the 'Wal-Mart effect' (Vandenbergh 2007, cited in Grabosky 2013, 117), referring to that company's ability to set prices, or to establish rules, such as what types of food suppliers can label as 'organic'.

The sheer power that standard setting can grant private actors is reason enough to study how companies endeavour to establish standards. But there are also other reasons to consider private actors' role in exerting power through standards. The act of establishing any standard 'valorizes some point of view and silences another' (Bowker and Star 2000, 5). When standards become embedded in infrastructure, that is, when standards become accepted as the way things are done, 'they risk getting black boxed and thence made more potent and invisible' (Bowker and Star 2000, 325), especially to ordinary users of that infrastructure.

Setting Health Standards

The allure of setting standards is evident in the business practices of technology companies, particularly those operating in the healthcare field. Technology companies are expanding their services into health-data-related services in what the philosophy of technology scholar Tamar Sharon (2016) calls the 'Googlization' of health research (Sharon 2016; see also 2018). This entails the industry promising to 'advance' or innovate research in health by extracting insights from vast datasets to develop automated tools for 'data-intensive personalized and precision medicine' (Sharon 2018, 2) that reflect the companies' commercial interests. For example, cloud service providers like Google, Microsoft, Amazon and IBM market their products as repositories for health data, while Apple and Facebook offer health-related services to users and collect data for health research, a feature that companies are expanding through apps and health wearables like Fitbit and the Apple Watch (van Dijck and Poell 2016; Lupton 2014).

Tech companies have valuable skills and technical infrastructure that have the potential to provide useful tools in the healthcare field. Benefits include tech companies' construction of hardware, such as fitness wearables and automated data tools to extract insights from health datasets and build the next generation of tools to diagnose and treat medical conditions. Alongside building tools, these companies are also endeavouring to set standards in the diagnosis and treatment of diseases and illnesses, including how they are managed in the healthcare system, such as through specific medications or surgical interventions (Powles and Hodson 2017). In other words, by building data-driven tools, technology companies are setting out particular ways (i.e., standards) of doing medicine, determining how conditions are diagnosed and treated. In doing so, companies may end up setting standards for how healthcare is delivered and, more broadly, understood as a service delivered by public and/or private actors. Google, for example, reports that since 2016, its Alphabet subsidiaries have developed AI-fuelled tools to detect eye disease, identify cardiovascular risk factors and signs of anaemia and improve breast cancer screening (Beede 2020). In these cases, Alphabet companies are working to establish standards as to how medical professionals detect and diagnose certain types of disease, such as using AI to identify eye diseases through automated analyses of medical images (see Ting et al. 2019). Google's AI company DeepMind also created an AI-operated tool to diagnose kidney injuries by extracting patterns from public health records from UK patients.

Developing health technologies requires access to mass amounts of detailed, sensitive health data. Google courted controversy in two of its attempts to acquire large health datasets, in 2016 in the United Kingdom and in 2019 in the United States. In the United Kingdom, DeepMind, a UK AI company, which Google acquired in 2014, struck an agreement in 2016 with the UK's National Health Service (NHS) to collect health data on nearly two million patients. In this agreement, DeepMind used the health data to build a clinical app to identify acute kidney injuries that DeepMind would operate in concert with the NHS (Powles and Hodson 2017). DeepMind reported publicly that it would not apply any AI techniques to the health data (Powles and Hodson 2017, 367). However, the information-sharing agreement between Google and the NHS set out that DeepMind would not only develop the app but also build 'real time clinical analytics, detection, diagnosis and decision support to support treatment and avert clinical deterioration across a range of diagnoses and organ systems' (Powles and Hodson 2017, 367). Despite DeepMind's public statements, the agreement did not restrict the company's use of AI on the health data, granting the company latitude for developing and training automated data tools (Powles and Hodson 2017, 367).

In the second case, in 2019, *The Wall Street Journal* revealed details of Google's secret Project Nightingale. In this project, Google secretly harvested medical data on 50 million Americans, including lab results, diagnoses, hospitalization records and prescriptions, from more than 2,000 hospitals belonging to Ascension, a large US healthcare provider (Copeland 2019). Ascension partnered with Google in this project because Ascension wanted to apply data mining to its patient information to create new diagnostic tools (Copeland 2019). For its part, Google's aim was to build machine-learning algorithms able to make recommendations about diagnoses and treatment, reflecting the company's broader strategy of creating data tools to aid in the detection, treatment and management of all kinds of diseases and illnesses. Google's interest in developing automated healthcare tools is evident in patent filings. For example, it owns a 2018 patent to apply automated tools to patients' medical records to make clinical predictions that could alert medical staff to problems, such as forecasting a patient's outcome after 24 hours in the hospital (Rajkomar and Oren 2018). In both the US and UK cases, Google created data tools that if they had been put into common usage, could have become standards to diagnose and treat specific medical conditions.

Technology companies' expansion into healthcare with the creation of automated data tools underlines the importance of understanding how companies amass and commodify data. Given the vast store of sensitive health data that DeepMind and Google acquired from unsuspecting patients in the United States and United Kingdom, the cases raise questions about data protection, especially privacy, and individual consent. Patients in the United Kingdom and United States neither gave consent for the use of their healthcare data nor were they consulted, a situation that elicited criticism from regulators and lawmakers in both countries. UK regulators found Google violated data-protection rules as patients involved did not consent to DeepMind's data collection (see Powles and Hodson 2017). Similarly, US lawmakers raised privacy and data-protection concerns about Project Nightingale, specifically whether patients had notice of Google's collection of their health data, whether patients could opt out of the project, and how Google would use, store and secure the health data against breaches (Lovett 2020).

While patient privacy and informed consent for the use of health data garnered significant media attention in the NHS/DeepMind case and Project Nightingale, there are broader concerns about the increasing use of automated data practices in healthcare. Specifically, when algorithms are 'black boxes', that is, non-transparent to those outside the software designers, it can be difficult to determine how they operate or their efficacy. Health researchers, for example, explain that physicians are not only concerned about whether automated tools perform accurately and effectively (i.e., 'algorithmic performance') but also whether healthcare professionals can have an

understanding of 'the underlying features through which the algorithm classifies disease' (Ting et al. 2019, 173).

A degree of transparency regarding the rules that comprise the algorithm and its operation may be necessary to ensure physician (and patient) acceptance of automated health tools, as well as regulatory approval. However, given the economic imperative to protect information and processes as proprietary property, 'companies are rarely motivated to disclose the underpinning criteria of their algorithms' (Möhlmann and Zalmanson 2017, 5; cited in Berg et al. 2018, 9; see also Pasquale 2015). In the DeepMind case, this likely means that the knowledge that the company extracted from patients at publicly funded NHS institutions 'will belong exclusively to DeepMind' and even if the company publishes scientific results from its studies, 'it is unlikely it will freely publish the algorithms it has trained' on the data (Powles and Hodson 2017, 362). Companies' propensity to lock down knowledge using IP law, such as the trade secrets and patents protecting its algorithms, could have the consequence of making valuable scientific knowledge inaccessible – or unaffordable – to those who need it most. Technology companies' use of IP law to render automated data tools as proprietary knowledge – tools that technology companies intend to be standards in how healthcare is managed and delivered – raises concerns of anti-competitive behaviour. It is this risk of monopolistic data practices that the chapter explores next.

Monopolistic Data Practices

Monopolistic business practices are unfortunately common in the digital economy, with regulators targeting potentially anti-competitive behaviour in the sectors of digital advertising, search and mobile operating systems. European regulators, for example, have levied fines against Google for abusing its market dominance in internet search by giving an unfair advantage to its comparison-shopping service or rivals' products (European Commission 2017). Platforms, as Srnicek (2017) reminds us, have a special capacity to benefit from network effects, which also enables them to enter different sectors (see Kenney et al. 2021). Google's capacity to capitalize upon network effects by drawing upon its datasets from its various enterprises and its expertise in data analytics explains Google's apparent facility to shift into different industry sectors. Smaller or new technology companies face an uphill battle to enter markets already crowded with dominant actors, thereby decreasing competition and possible innovation in the field.

Google's acquisition of Fitbit for US$2.1 billion in 2021 provides a useful example of the potential consequences of monopolistic data practices in the health sphere. Announced in 2019, it attracted the attention of regulators around the world, including in Australia, Europe, Japan, the United States and

South Africa, before it was finalized in January 2021 after approval from the European Commission.[7]

Fitbit was an attractive acquisition for Google as the wearable added a trove of health and fitness data to the company's already large datasets. For regulators in Europe and Australia, concerns over monopolistic data practices were front and centre (see Australian Competition and Consumer Commission 2020b; European Commission 2020). Australian regulators warned that the deal could enable Google to become dominant in data-dependent health services through Fitbit's fitness and health datasets, including providing health analytics to pharmaceutical companies, developing diagnostic tools and building health-related AI tools (Australian Competition and Consumer Commission 2020b). As Srnicek (2017, 42) remarks, 'data analysis is itself generative of data', meaning that those actors in the position to amass and hold as proprietary stores of data can then create further value and data through data analytics.

Regulators also feared that the Fitbit acquisition could exacerbate Google's dominance in the digital advertising sector by adding Fitbit's health datasets to its vast holdings of users' demographic profiles. Google's control over the Android mobile operating system similarly sparked concerns that Google could disadvantage operators of competing wearables systems using Android software by making interoperability more difficult. Wearable devices must connect to smartphones to get software updates or use applications like maps, messaging or social media. Google and Apple's control over mobile operating systems are standards for how most mobile devices function (see Nieborg et al. 2020).

In its approval of the Google-Fitbit deal, the European Commission took a digital economic nationalist approach in its efforts to ensure that European healthcare start-ups would be able to compete with the US tech giants in the 'European digital healthcare space' (European Commission 2020). European Commissioner for Competition Margrethe Vestager said the deal would ensure that 'the market for wearables and the nascent digital health space will remain open and competitive' (European Commission 2020). To encourage competition within the European market for healthcare, before the European Commission approved the Google-Fitbit deal in January 2021, it set several requirements for a ten-year deal, which Google accepted. Google promised continued interoperability of non-Fitbit wearables with its Android operating system. This rule is intended to enable other actors to create health/fitness-related apps using Android without fear of interrupted functionality. In this case, the European Commission intervened in the market to set rules that are intended to nurture the growth of companies domestically within Europe. Google's purchase of Fitbit shows that states have digital economic nationalist fears that knowledge feudalists like Google will shut them out of

innovation, capturing the majority of financial benefits and locking up the underlying knowledge, like algorithms as proprietary information.

Reflecting a digital economic nationalist approach, the European Commission set requirements intended to address Google's advertising dominance. Google agreed to create 'data silos' that would separate Fitbit data from other Google data used in advertising, not just for customers in the European Economic Area but globally (Osterloch 2021). Unless users choose to share their Fitbit data for advertising purposes, Google promises to keep it separate. How and the extent to which Google complies with the European Union's requirements should be scrutinized closely, including how its acquisition of Fitbit might enable Google to contribute data inferences to its other health-related technology businesses. Privacy experts caution that separating data into silos may not effectively address data protection – or monopoly – concerns, as 'Google doesn't necessarily need to extract information about you personally; it's enough for it to get that data from someone statistically similar to you' (Bria et al. 2020). Google can mine its existing datasets for insights, and these analytics could add value to its understanding of its Fitbit datasets.

The DeepMind and Fitbit cases, along with Project Nightingale, covering a wide swath of healthcare, illustrate Google's ambitions in healthcare technologies and the risks of data monopolies. The DeepMind case was not simply about building a healthcare app, but about more broadly mining NHS datasets for new health products and services. A freedom of information request, related to non-legally binding talks in 2016 between DeepMind and the NHS, revealed DeepMind wanted to develop projects including the 'real time prediction of risks of deterioration, death or readmission, bed, demand and task management, [and] junior doctor deployment/private messaging' (Powles and Hodson 2017, 354). While these discussions may have been only aspirational, they demonstrate DeepMind's and Google's interest in constructing NHS-wide systems for centralizing, processing and managing health data and establishing technologies for healthcare and health management. In the words of DeepMind's co-founder, Mustafa Suleyman, in 2016, these projects would apply at the 'hospital-wide level and the population-wide level' (Powles and Hodson 2017, 355).

DeepMind, in other words, aspired to set standards for the provision of healthcare throughout the United Kingdom in which the company could 'build, own and control networks of knowledge about disease' (Powles and Hodson 2017, 364). Google may not (yet) be a data monopolist in this sphere, and it, like other technology companies, may create valuable diagnostic, treatment or healthcare management tools. However, the knowledge feudalist strategy of treating as proprietary all datasets to extract maximum value, even data from public health agencies and locking down innovations through IP

law risks making new healthcare technologies, as well as the knowledge they are built upon, inaccessible to those who cannot afford them.

CONCLUSION

From Google's expansion into the healthcare industry to the companies that dominate the data value chain to companies that market precise predictions of human behaviour and attributes, private actors exert structural power through their control over data. This chapter has reflected upon the consequences inherent in private actors' commodification of personal data, particularly when companies organize their business practices to profit from the dataist assumption that human behaviour can be accurately quantified and even predicted. These examples – data-driven profiling of individual or groups and standard setting – highlight the corporate side of the information-imperium state.

Dataism, a core element of private data power, is particularly evident in companies' claims of predictive accuracy through data analytics. Businesses market their forecasts as having utility and certainty, while others accord those forecasts social and economic legitimacy. In short, data-driven forecasting is powerful because *we act as if* the predictions are valid, reliable representations of reality. Profiling people using data analytics and automated tools may deliver some benefits, such as personalized services and better pricing (Crain 2021; Turow 2021), but the negative consequences can be significant, as profiling can exacerbate existing discriminatory practices and, in worst cases, rebrand pseudoscience as sound social policy (Stark and Hutson 2021). Attempts to make predictions at the level of individuals or groups carry with them significant risks, especially when forecasts can cost people employment, healthcare, housing or even their liberty (Taylor et al. 2017a). Individual privacy frameworks, the chapter points out, are unsuitable to protect people against harm from group profiling, a challenge we explore further in chapter 9. Despite these problems, automated profiling practices will likely remain commercially viable because they offer the seductive (albeit erroneous) dataist promise that complex human behaviour can be precisely quantified and forecast.

Companies like Google, along with Tencent, Alibaba and other big data players that have the commercial and technical resources to amass high-quality datasets and build AI tools reap the financial benefits of their dominant position in global value chains while also entrenching themselves in their position as holders of the 'right', legitimate knowledge needed to address any social problem (see chapter 5). The DeepMind case, Project Nightingale, and Google-Fitbit deal highlight how powerful actors are positioning themselves

as standard setters in important areas of social and economic significance with the capacity, for example in healthcare, to determine diagnostic standards, treatment or disease management tools. This is the essence of private data power, achievable for those actors with the capacity to maintain proprietary holds over datasets and capture the dominant share of data value. Data companies in this position have the structural power to set the 'very limits of knowledge' (Crawford et al. 2014, 1668), whether in selling predictions of future behaviour or operating datasets that allow them to set industry standards.

Control over data and the means to interpret and process large datasets to extract valuable, actionable insights are significant sources of structural power within the knowledge-driven economy. Currently, this power is wielded mainly by data giants, primarily located in the Global North, who are able to shape the terms on which others are able to engage in the data economy. Operating as knowledge feudalists, these companies have the commercial and technical capacity to process and monetize data and market their data interpretations as having social, economic or political value to other businesses and, as chapter 8 will explore in part, to governments.

NOTES

1. In contrast to the content layer, where US companies exert commercial dominance, the infrastructure layer, including content networks and internet exchange points, rests with a more geographically distributed consortia of private and state actors (Winseck 2019).
2. Chapter 7 discusses agriculture's datafication in greater detail.
3. Or more precisely, 'knowledge resellers', to use this book's preferred terminology.
4. The digital advertising industry's claim to predict and, more importantly, influence consumer behaviour is 'sacrosanct' among digital advertisers (Hwang 2020, 4), despite critics pointing out that companies' claims of accurate predictions are overblown (see, e.g., Aiolfi et al. 2021; Crain 2021). Because of these problems, Hwang (2020, 15) argues that the web's financial foundation on digital advertising is 'perhaps shakier' than is commonly understood. In other words, our dependence on surveillance-driven advertising to support free services and power the web rests precariously on over-hyped claims of forecasting accuracy (see Crain 2021).
5. Interview 10 December 2020, via Zoom.
6. As an engineering professor friend of ours once remarked to us, 'I've published on artificial intelligence in academic journals. When I read about AI in newspapers, I don't recognize any of it.'
7. The European Commission's approval of the deal in January 2021 interrupted the investigation by the Australian Competition and Consumer Commission (ACCC) and meant the ACCC's work became an enforcement investigation of a completed merger.

Chapter 7

Property and Control

Who Owns the Internet of Things?

Consider the 'smart home'. In the smart home, data-collecting sensors are embedded in all manner of household objects, from televisions, thermostats and security systems to kitchen appliances, to enable people to customize these goods to suit their lifestyle and even to operate them remotely (Maalsen and Sadowski 2019). These physical goods, embedded with software that enables data to be collected, transmitted and acted upon, form the Internet of Things (IoT) or, more colloquially, 'smart' products. The purpose of IoT products is to add internet connectivity to hardware, thereby creating networks that connect 'people-people, people-things, and things-things' (Morgan 2014).

Such products are sold to us by companies touting their seemingly magical qualities: the ability to control your home thermostat via your smartphone or to ask an always-on microphone-and-speaker-embedded device to run through the steps of a recipe. These consumer-oriented products are mirrored in the smart city in what is often referred to as the industrial IoT. It functions along the same principles as these consumer products, only instead of connecting smartphones and speakers, it connects networked and data-collecting infrastructures in sectors like oil and gas, and healthcare.

The industrial-oriented IoT is made up of physical infrastructure embedded with software-driven networks of sensors in things like sidewalks, wastewater pipes and transit systems, enabling real-time data collection, streaming and analysis to provide services like transit or waste removal. Such systems are what allow a smart city to function. These sensors enable 'ubiquitous trackability', a core smart-city feature since the provision of services relies upon the real-time continuous tracking of people and objects within the urban environment (Koops 2014, 255; cited in Edwards 2016, 39). In Toronto, for example, Sidewalk Labs proposed an 'active stormwater management' system that would 'combine cloud software, sensors and

controls', thus reducing 'the size and cost of future stormwater infrastructure needed' (Sidewalk Labs 2017b, 170). The company also planned 'a public realm management system, enabled by sensor arrays, that monitors air quality, asset conditions, and usage, helping managers respond quickly to emerging needs, from broken benches to overflowing waste bins' (Sidewalk Labs 2017a, 17).

The rising importance of the knowledge structure – of the control over data and intellectual property (IP) in particular – is reshaping the global political economy. We can see this process perhaps most clearly when thinking about smart devices and the IoT, especially around the question of who actually controls IoT infrastructure and devices. In an information-imperium state, as we have explained in this book, power rests primarily with those who control the creation, dissemination and use of knowledge.

This chapter explores how control over software, via IP law and software licensing agreements, enables manufacturers of software-enabled goods to rewrite long-held assumptions about ownership. This control, enabled by a mix of technology and law, is allowing companies making software-enabled products to exert control over device data and to determine the use – and even the lifespan – of these products (Tusikov 2019a).

In contrast to traditional non-connected goods, the control over the devices' embedded software, which enables the goods to function as intended, rests not with the purchaser but with the manufacturer, who also determines what data will be collected and how that data may be used, stored, processed and shared (Tusikov 2019a). In this process, data is not only a valuable asset in and of itself, to which companies lay claim as a reusable commodity, but it is also fundamental to the operation of connected devices. Data – its capture, exchange and processing – is integral to both smart cities and the IoT. In fact, data can be understood as 'both the modus operandi and raison d'être' (Shelton et al. 2015, 16) of the IoT. Those who control software and resulting data flows can exert control over knowledge itself by determining, for example, which actors are 'authorized' to access the specialized tools and manuals to repair devices and who can profit from the commercially valuable data analytics.

By controlling these products' software and IP, companies are redefining the very concept of ownership in a way that rebalances it away from purchasers and towards sellers and their economic interests. This situation has led some scholars to warn of the 'end of ownership' (Perzanowki and Schultz 2016; see also Farkas 2017) and the emergence of a 'new digital serfdom' (Fairfield 2017). While these claims may be somewhat overstated, what's clear is that this control is an expression of structural power. Buyers of such goods are generally only entitled to 'precarious' ownership over smart products, specifically a licence to use – not to control or modify the goods they purchase – and

companies can change the conditions of 'ownership' after purchase, even to the extent of rendering these goods functionally useless (Tusikov 2019a).

This chapter proceeds as follows. The first section provides an overview of smart devices and the IoT, highlighting the prominent role of licensing agreements in regulating ownership of IoT goods. The second section explores how these agreements are used to enable the capture of data. The third section considers the forms and effects of post-purchase control, the ways in which manufacturers assert de facto ownership rights through the creation of proprietary ecosystems based largely on the control of software.

To illustrate how these proprietary ecosystems affect ownership rights, the fourth section examines the 'right to repair'. More than anything, the right-to-repair movement serves as a reminder that the knowledge-driven society is contested and contestable. This section turns to the effects of this proprietary ecosystem on the question of who controls the access and use of not just personal data – the primary focus of most digital activists – but economically valuable non-personal data. We end the chapter with a brief reflection on the implications of this IoT regime for governance generally.

As we have argued throughout this book, such changes are not restricted to smart cities or stereotypically tech sectors. Rather, the transformation of conceptions of ownership can be seen throughout the economy, wherever smart devices are deployed. To illustrate this point, this chapter highlights the experience of farmers with smart tractors in the data-intensive agricultural sector.

DIGITAL RULES GOVERNING PHYSICAL GOODS

Ideas regarding what constitutes property and the nature of ownership, notes legal historian Stuart Banner, are inherently political, reflecting pressure from interest groups in the context of the society within which they operated (Banner 2011, 21). In the United States and the United Kingdom, for example, the notion of property has changed from being conceptualized as a thing to rights in a thing or 'property as a bundle of rights' (Banner 2011, 62). Property, Banner reminds us, 'is a human institution that exists to serve a broad set of purposes' that 'have changed over time' and that reflect dominant political opinions about what property should do and who it should protect (Banner 2011, 289–90). The concept of ownership is additionally complicated with the involvement of IP, the form of protection provided to intangible goods such as computer programs. As we discussed in chapter 3, the limits of IP are inherently political, raising questions of which ideas are considered property, the extent of protection and who can lay claim to that property (Sell 2004).

For instance, it may come as a surprise to learn that we do not own the digital files that make up our music or movie collections, even though we paid for

them and downloaded them legally: actual ownership resides with the copyright owner(s). In fact, the same ownership rules that govern our iTunes music library apply to a new car or rather the software that makes a car run. We are used to controlling the physical things we own, choosing to sell, rent or repair things with few legal limitations, even though more physical goods – those with embedded software – are instead governed by rules set forth for digital goods (see Perzanowki and Schultz 2016). If you are confused by this state of affairs, you are not alone. Regulatory organizations have questioned whether consumers understand the critical differences between connected and non-smart goods (Rich 2016), and studies of consumer behaviour indicate support for the repairability of software-embedded products (Perzanowski 2021).

The Extension of Intellectual Property Rights to Physical Goods

Understanding the difference between traditional and connected devices has become a necessity as the number of smart devices rises, with the IoT market project to grow from US$381.30 billion in 2021 to US$1.85 trillion in 2028 (Fortune Business Insights 2022). Because the functionality of these physical devices depends on their embedded software and connectivity, such objects end up adopting 'all characteristics of digital technology, i.e., they become programmable, addressable, sensible, communicable, memorable, traceable, and associable' (Turber et al. 2014, 21). In turn, this means that control over the software and connectivity equates to control over the physical product itself with consequences to how we conceive of property and how it is regulated.

The embeddedness of software in physical products has made possible a transformation in our common-sense notions of ownership and control. Specifically, the IP and contract laws that protect the software embedded in the physical product, combined with the always-connected nature of the IoT, allow effective control over the physical product to remain with the company.

Companies that make connected products use copyright law to protect the embedded software or, in the cases of complex products like vehicles, series of software systems. Copyright owners are typically the companies that manufacture the connected goods or the third parties that provide the software to those manufacturers. Copyright law enables manufacturers to prohibit their customers from modifying, tinkering with or repairing IoT goods if such acts involve copying or altering the products' software, arguing that doing so violates the software's copyright. The application of copyright law to effectively govern physical goods with embedded software challenges the long-standing distinction between software and physical objects, representing a significant shift in how we conceive of and regulate physical goods (Mulligan 2016).

The actual ownership/control relationship can get somewhat complicated. The American company John Deere, one of the world's largest agricultural equipment manufacturers, reports that about 184 companies operate software applications that are integrated into its (trademarked) John Deere Operations Centre, its 'online farm management system'[1] offering data-related services to farmers and other clients interested in farming data (Patel 2021).

Copyright law often extends protection to what are called 'technological protection measures', digital locks that enable the copyright owner to control access to or the use of the underlying content (Kerr 2007, 6). In many countries, these digital locks are protected by copyright legislation, which often make it illegal to break the locks or to purchase tools to break the locks, sometimes regardless of whether the underlying content is actually eligible for copyright protection (Haggart 2014).[2] The United States has 'aggressively exported' its preferred approach of strong protection for digital locks over the previous two decades (Perzanowski 2022, 124). 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 in the most extreme case, whether the product will continue to function (Tusikov 2019a).

In conjunction with copyright law, companies use end-user licensing agreements, often called software licences, to set rules governing the use of connected devices. These agreements are the omnipresent, seldom-read legal contracts that accompany software-enabled goods setting the conditions under which users can use the software and outlining penalties for violation (see Langenderfer 2009; Perzanowki and Schultz 2016).[3] Through their licensing agreements companies grant themselves the right to restrict and sanction unwanted behaviour, including cancelling warranties and terminating users' access to or disable the product itself, even if the activity in question is itself legal.

LICENCES AND DATA CAPTURE

Data, as we noted in chapters 1 and 4, is a fictitious commodity. It is produced to fulfill an instrumental purpose, but it is also something that can be transformed into an economically valuable commodity. Examining the IoT allows us to understand this dual nature and the motivations behind the IoT business model. Smart devices depend on the creation and transmission of data for their functionality. As Nick Srnicek (2017) and others have noted, the knowledge-driven economy ('platform capitalism', in his terminology) is designed to maximize the creation and extraction of data as a commodity.

As a result, who controls this data in a knowledge-driven economy is an issue of high importance.

The ownership of the data collected by IoT devices is set out in software licensing agreements. Such agreements are becoming as ubiquitous as IoT devices themselves, as they are not just found in high-tech sectors like smartphones and computers. For example, companies such as John Deere and Monsanto (which was purchased by the German chemical/pharmaceutical conglomerate Bayer in 2018) may have been traditionally regarded as agricultural companies, manufacturers of equipment, fertilizers or seed. However, they now position themselves as data and technology companies.

According to John Deere's chief technology officer, 'we have more software development engineers today within John Deere than we have mechanical design engineers' (Patel 2021). The company regards tractors as 'mobile sensor suites that have computational capability' that are 'continuously streaming data' (Patel 2021). This emphasis on sensors reflects the prioritization of data collection over the physical tractor: it's not a tractor with an onboard computer, but a series of sensors housed in a tractor.

The agricultural industry's shift towards data-driven practices and computerized farming equipment is only the latest in a long history of innovation-geared agricultural work, such as the Green Revolution in the 1950s to late 1960s that aimed to 'advance' developing countries' agricultural practices through Western scientific and management practices (Glaeser 1987). Farmers' contemporary battles over repair and control over farming data, both of which are underpinned by agricultural firms' control over IP rights, also evoke decades-long clashes over patented seeds in which agricultural companies determine how farmers can use patented crop seeds (Saab 2019).

This emphasis on data is reshaping farming. Like other industries, farming increasingly operates with a dataist mindset that believes all possible information should be captured to increase productivity and generate value. With the advent of so-called precision or smart farming, agriculture is increasingly reliant upon the application of data-driven techniques and the use of software-enabled, internet-connected devices with the aim of making farming more accurate, predictable and generating greater value (see, e.g., Bronson et al. 2021). Through wireless sensors embedded in the ground or in agricultural machinery or through data collected by ground-based or aerial drones, precision farming enables farmers to collect data including moisture, seeding variety and rates, fertilizer levels, crop health, weeds and machine locations. In regard to livestock, farmers can remotely monitor and track the location, nutritional needs and well-being, and health of farm animals, 'the internet of cows', as it is sometimes called.

Like all knowledge-governance regimes, software licences attached to software-enabled farming equipment like tractors create winners and losers.

For example, sensor-studded tractors collect valuable data on crops and environmental conditions that traditionally was the knowledge that farmers individually documented and carefully stored year over year. The issue with respect to farming data is over who controls not only the data produced by these sensors but, more importantly, over the commercially valuable insights produced from parsing the datasets aggregated from this data. Big agri-businesses such as John Deere and Bayer say that control over farming data rests with individual farmers. John Deere, for example, asserts 'you control who sees your data' (John Deere 2021). Similarly, Bayer's Climate FieldView digital agriculture platform's licensing agreement states that individual users 'own all Customer Farm Data' (Climate FieldView 2021, s. 4.2).

While farmers may own their agricultural data, depending upon the conditions of the sensors' software licence, the big agri-businesses typically assert ownership over the interpretations of the data and any recommendations or forecasts emanating from that data (see, e.g., Bronson and Knezevic 2016). The Climate FieldView platform's licensing agreement, for instance, states that the company, owns all generated work, including 'data, tools, analyses, results, estimates, prescriptions, recommendations and other information generated' (Climate FieldView 2021, s. 4.2). While farmers technically own their data, FieldView's licensing agreement requires farmers to license the data they collect using Climate FieldView to the company. The licence grants the company the right to create its proprietary analyses and recommendations from farming data (Climate FieldView 2021, s. 4.1). In the same way, John Deere advises users that it may employ operational data from the tractors' sensors for 'diagnostic or prognostic activities' (John Deere 2021).

Essentially, although farmers technically own their data, they don't control it. The mere fact of signing onto Climate FieldView's services means farmers essentially cede this control to the company. An individual farmer's data may have some value to that farmer, but it is most useful when it is combined and processed with others' data. Large agriculture firms, operating as de facto tech companies due to their position as data collectors and processors, aggregate data from multiple datasets and process it using proprietary algorithms, and market this back to farmers as providing customized knowledge of and recommendations for their farms. Such processes highlight what we can think of as a 'data value chain', in which value emerges in transforming 'data – from data collection, through processing, and analysis, into digital intelligence – that can be monetized for commercial purposes or used for social objectives' (United Nations Conference on Trade and Development [UNCTAD] 2021, 17).

In doing so, agriculture firms have wrested structural power over knowledge – the ability to control who is able to create, access and use socially valuable knowledge – from farmers. This power places what are probably best thought

of as 'agricultural data companies' in a 'privileged position with unique insights on a field-by-field basis' (Carbonell 2016, 1; see also Bronson and Knezevic 2016). In short, these big agri-firms operate as knowledge feudalists. Consequently, individual farmers, for whom such knowledge is necessary in order to stay competitive with other farms, become locked into a relationship of data dependency, even as Climate FieldView's licensing agreement states it does 'not guarantee any results' and says its services should not 'be used as a substitute for sound farming practices' (Climate FieldView 2021, s. 1.1).

The agricultural sector offers a useful reminder that the issues surrounding the creation, control and use of non-personal data can be just as consequential as with personal data and that data governance challenges extend far beyond concerns over privacy rights. Farmers are often reluctant to relinquish control over the data they regard as proprietary to their business when they may not benefit equally or at all in the monetization of their farming data (van der Burg, Wiseman, and Krkeljas 2021, 1). Farmers may conceptualize agricultural data like soil fertility and crop yield as equivalent to trade secrets central to their agricultural practices and business methods and accord that data considerable financial value (Carbonell 2016).

Surveys of farmers in the United States, Canada, Australia and Europe have found varying degrees of concern around the corporate access to farming data and how that data might be used (see, e.g., Wiseman et al. 2019; Steele 2017; van der Burg et al. 2021). A general concern is that farming data is regularly traded or disclosed to third parties, leaving farmers unaware of who knows the details of their commercial enterprises (Wiseman et al. 2019, 8). This concern is exacerbated for farmers outside the United States and Europe, where many agricultural companies are headquartered, as there is uncertainty as to the level of data protection afforded to farmers and their farm data (Wiseman et al. 2019, 9). Farmers may find themselves in a difficult position: either work with large agricultural technology firms that typically require farmers to surrender control of their farming data or risk the commercial viability of their farms by eschewing the technology (Carbonell 2016, 5). In the view of some analysts, farmers have become essentially 'glorified sharecroppers' with decreased autonomy over their agricultural practices (Carbonell 2016, 5).

Software-enabled devices do not just link devices and products to their manufacturers. The IoT also collects data on individuals' activities, movements and behaviour. Such data flows disproportionately benefit the companies that collect this data, particularly major foreign (especially American) technology companies. Researchers from the National Research Council in Canada, a federal government organization, have warned that the country is at risk of becoming a nation of 'data cows', with the flow of data generated in Canada to foreign companies like Facebook, Amazon, Netflix and Google

(Press 2018). These unequal relations are mirrored between dominant companies in the Global North and populations in the Global South, reflecting what communication scholars Nick Couldry and Ulises Mejias call 'data colonialism' (Couldry and Mejias 2018). Whether it's personal or non-personal data, such acts of data collection place those who produce data at the bottom of the data value chain (United Nations Conference on Trade and Development [UNCTAD] 2021, xvi).

POST-PURCHASE CONTROL

Beyond the advantages that come with the control provided to manufacturers by copyright and software licences, the always-connected nature of these products allows those who control the physical object's software to claim extended post-purchase control over the object itself, improving or restricting its functionality, at the extreme even rendering it completely inoperable. This control is possible because software-enabled products are dependent upon regular communication with their manufacturers' servers in order to receive instructions and communicate the data necessary for their proper functioning, creating a 'tethered' manufacturer-user relationship (Zittrain 2009).

This always-on relationship has both benefits and drawbacks. On the plus side, monitoring can allow manufacturers to ensure that their products' software has not been infected with malware or to maintain the integrity of their product by verifying that only authorized service providers are allowed to repair their products (Brass et al. 2017; we discuss the consumer's perspective on repair further in this chapter). Connected products can also function as 'trusted systems' in which 'authenticated devices and platforms' sell the promise of interoperability and safety to consumers, while enabling companies to retain tight control over the software and hardware (Graber 2015, 391). Consumers can also benefit from improved product functionality. For example, facing the landfall of Hurricane Irma in Florida in 2017, Tesla remotely upgraded battery capacity to allow its vehicles to travel greater distances without recharging in order to aid in evacuation efforts (Westbrook 2017). This free extended battery capacity expired several weeks later unless customers purchased the upgrade.

On the downside, at least from the user perspective, this always-on software linkage between product and manufacturer enables 'perfect enforcement' of a company's terms of service (Zittrain 2009, 123). This linkage enables not only software updates in the consumer's interest (such as security updates or increased functionality) but also ones that interfere with product functionality. Companies can unilaterally impose restrictions on consumers' use of the product, modify the products' software after sale and require customers to

purchase cloud-processing services to operate the goods without providing consumers sufficient information about these conditions beforehand (see Manwaring 2017). Tethered devices, for example, offer companies the ability to shut down products remotely if buyers miss a payment, as John Deere has done with construction equipment in China (Waldman and Mulvany 2020). For better and worse, this link allows companies to determine how the software – and by extension, the product – works and how it can be used. As a result of this 'tethered' relationship, software-enabled goods are 'rented instead of owned, even if one pays up front for them' (Zittrain 2009, 107).

Proprietary Ecosystems, Lock-in and Control through Bricking

Proprietary closed IoT devices can trap users in an ecosystem in which control over the technology rests with the manufacturer. The use of IoT exposes the user not only to the risk that the technology may fail (software being held to a much lower standard than we demand of physical infrastructure) but also that the company may decide not to continue servicing it.

This is an example of 'bricking', the most extreme form of post-purchase control. Bricking refers to manufacturer-pushed software interruption or impairment that has the intention of negatively affecting product functionality, even limiting the product's lifespan (Tusikov 2019a). By discontinuing software updates, which may contain essential security patches, or by pushing software updates that negatively affect product functionality, manufacturers can cause IoT products to cease functioning properly, either immediately or over time, depending upon the nature of the product. Some connected devices will not operate without functioning software, while others will work without software but will lack the smart functionality, such as of a talking doll whose voice-recognition software is disabled.

Like post-purchase control generally, bricking is not without its positive aspects. Bricking devices can be an effective, rapid response to products discovered to be dangerously defective or pose a public health or safety risk, especially given the challenges of implementing wide-scale product recalls. For example, after Samsung launched its Galaxy Note 7 smartphone in the summer of 2016, customers reported that their phones were overheating, catching fire and even exploding because of a faulty battery design. That September, Samsung issued a product recall and in December 2016 released a software update designed to render the remaining phones non-functional, and thus non-explosive (Kieler 2016).

However, while bricking harmful products can be beneficial for consumers in such circumstances, when companies disable still-functional devices, it can be an undue curtailment of consumers' rights in a way that is not possible with non-software-enabled goods.

In some cases, companies have bricked still-functional products when they've canceled a product line or merged business divisions. In 2016, for example, Google's Nest company bricked the Revolv smart-home hub (which it had purchased in 2014), which enabled communication among light switches, garage door openers, motion sensors and thermostats and allowed users to program these devices and operate them remotely. After offering customers refunds, Nest remotely destroyed the Revolv system without their customers' consent (Kingsley-Hughes 2016).

Companies may also brick products as a consequence of changes in corporate ownership or the sale of IP. Following the sale of the social robot Jibo's IP assets to a New York venture capital firm in June 2018, the robot lost functionality, specifically its ability to dance, play games and respond to questions, and, in the words of its devoted owners, the social robot 'died' (Gault 2019).

Bricking can also result from a change in business strategy. In 2020, for instance, the speaker company Sonos announced its intention to support only the newer versions of its products, essentially triaging its software support and abandoning older internet-connected product lines. Sonos informed its customers that they had to choose between functionality and their speaker systems as certain legacy systems would stop receiving security and software updates, or they could trade in their old speakers for a discount on a new system (Bode and Gault 2020).

At least Sonos kept in touch with its customers. In April 2022, Insteon, 'a smart home company that produced a variety of internet-connected lights, thermostats, plugs [and] sensors', all based on a proprietary networking protocol, simply disappeared, 'breaking users' cloud-dependent smart-home setups without warning' (Amadeo 2022). Without access to Insteon's servers, the Insteon app 'appears worthless, and users' automations and schedules have stopped working'. But because the company's protocol had been reverse engineered, something that purveyors of proprietary platforms tend to work to prevent, customers could potentially move to another platform (Amadeo 2022).

Orphaned technology is another potential drawback of post-purchase control. Software has a much shorter lifecycle than physical infrastructure, typically lasting only several years. When software is embedded within physical products, this leads to what legal scholar Woodrow Hartzog and philosopher Evan Selinger call the 'internet of heirlooms and disposable things': products that outlive their software and linger as dumb or zombie products (Hartzog and Selinger 2016, 588–89). Designed-in obsolescence is not only frustrating to those who reasonably assumed that their connected goods would have a similar lifespan to non-smart goods but also contributes to the significant environmental problem of electronic waste, which is largely dumped in developing countries (Andeobu et al. 2021).

Bricking and loss of control are not just consumer-level problems. When cities and governments adopt IoT technologies, they also open themselves up to a loss of control. Smart cities, dependent upon vendor-operated systems of software for digital infrastructure to function, could be similarly stranded or 'orphaned' if companies interrupt or discontinue the provision of software that operates certain technologies or if vendors are unable or unwilling to repair proprietary technologies. Depending upon the nature of the digital infrastructure, smart cities abandoned by their vendors could face downgraded or interrupted services like transit systems that do not communicate with each other or wastewater systems that no longer detect leaks. Sidewalk Labs left the Quayside project in Toronto before construction began, leaving no orphaned technologies. But imagine a smart city in which vendors were unable or unwilling to maintain smart-city services, in which a company like Sidewalk Labs, facing declining profit rates or a citizenry wanting more control over their city, decided to walk away. Recalling the fate of Insteon's customers, the city could be left with no lights at all.

The examples of bricking in this chapter illustrate the vulnerability of consumer-oriented objects operating through servers and the importance of consumers understanding the difference between connected and non-connected goods. Policymakers and regulators also need to understand that when building a smart city, they are not just purchasing a cool piece of tech; they are buying a relationship in which they may not be the ones calling the shots. This state of affairs highlights the need for city managers and planners to understand that building – and maintaining – a smart city 'requires a political understanding of technology' with 'a focus on both economic gains and other public values', concluded a meta-study of fifty-one academic publications on smart-city governance (Meijer and Bolívar 2016, 392).

While city officials may have considerable experience with public-private partnerships in the construction of physical infrastructure like bridges or airports, they may have less experience with corporate vendors who operate digital infrastructure as ongoing services. Depending upon the procurement process and IP rights applied to the digital infrastructure, it may be difficult to determine who is responsible for maintaining the infrastructure and what happens in the case of the vendor's bankruptcy, sale or shift in business model away from smart cities. Municipal staff often do not have the resources or expertise to deal with smart-city problems.

Studies of smart cities have found that cities were poorly prepared to evaluate the technologies that vendors were selling as municipal IT staff lacked the capacity to assess the technologies under consideration or, problematically, were contracted from the vendor company attempting to provide the services (Viitanen and Kingston 2014; cited in Hartt et al. 2021, 218). In the Toronto smart-city case, for instance, the auditor general of Ontario noted

that the province of Ontario lacked the capacity to evaluate a smart-city project like Sidewalk Labs' Quayside plans (Auditor General of Ontario 2018, 653, 649). Similarly, the regulator found that Waterfront Toronto, the public body responsible for issuing the smart city bid, 'had limited experience in digital data infrastructure development' (Auditor General of Ontario 2018, 653, 649).

OWNERSHIP, CONTROL AND THE RIGHT TO REPAIR

The ability to repair broken technology – more specifically, the ability to access the knowledge needed to repair broken machines – is a longstanding challenge that predates and extends beyond the digital realm. For example, the Covid-19 pandemic has drawn global attention to the difficulty many hospitals face when it comes to repairing medical devices. Addressing the issue of inadequate supplies of crucial medical equipment, especially ventilators, has been made more difficult thanks to manufacturer-imposed restrictions on hospital technicians' capacity to repair ventilators on-site (He et al. 2021; Koebler 2020). For example, in order for hospitals to perform a repair on ventilators, technicians must sometimes obtain authorization from or send machines off-site to manufacturers to be fixed, which may result in critical machines being unavailable for days or weeks (Scher 2020). This problem is particularly acute in developing countries, where it can be difficult and costly to access manufacturers' repair manuals and acquire manufacturer-authorized replacement parts for everything from ventilators to electric 'power' wheelchairs (part of the medical IoT), as well having the resources and technical knowledge for onsite maintenance (Marks et al. 2019).

The ability to decide who is able to access what knowledge is a fundamental expression of structural power in the knowledge structure. It creates relations of dependency, haves and have-nots. The question of how software-enabled goods can be repaired and by whom has become heated with political and public battles around the world, from Europe, the United States (Perzanowski 2022), Australia (Productivity Commission 2021) and Canada (La Grassa 2022) to developing countries such as South Africa (Ho 2021). While questions of who can repair products and under what circumstances may seem esoteric, they are fundamental to issues of ownership and control. Control over intangibles, data, IP and the focus of this chapter, software-enabled goods, are central to exerting power in the knowledge structure and the knowledge-driven society.

Power in the knowledge structure is contested and contestable. In this case, the battle is over whether companies can lawfully restrict their customers or third-party repair personnel from repairing software-enabled

products. Repairing or identifying problems with faulty software-enabled goods often necessitates the use of diagnostic software, while undertaking repairs often requires copying all or part of a product's software (Perzanowki and Schultz 2016). However, manufacturers' licensing agreements typically prohibit any actions, including repair, that copy or alter the product's software.

Companies typically cite this provision to prohibit any repairs by unauthorized personnel, which they define as anyone not authorized by manufacturers using their branded parts. In order to incentivize customers to patronize repair shops that have been authorized by the manufacturer, companies may decline to reimburse warranty repairs or void warranties entirely for repairs done by independent repair personnel or involving non-original equipment manufacturer parts (Tusikov 2019a).

In many jurisdictions, the ability of individuals to repair the software-enabled goods that they have purchased is further limited by technological protection measures: digital locks that enable the copyright owner to control access to the underlying content. As noted earlier in the chapter, these digital locks are often protected by copyright legislation that prohibits the breaking of these locks or the manufacture of computer programs that could be used to circumvent them (see Kerr 2007). Legal exemptions for the circumvention of digital locks tend to be narrow in scope, often meaning that even if the activity in question is 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. In the case of digital locks, rights holder–imposed restrictions via their terms of service can effectively trump legal exemptions allowing for the lock to be broken. In keeping with its maximalist, knowledge-feudalist approach to knowledge governance, the United States has been the main proponent of this form of copyright protection, using trade agreements to promote this policy (Haggart 2022; see also chapter 3). As legal scholar Aaron Perzanowski notes in his 2022 book *Right to Repair: Reclaiming the Things We Own*, trade agreements that institute technological protection measures effectively 'imperil legitimate repair activities around the globe' (Perzanowski 2022, 124).

Taken together, repair work that violates a manufacturer's prohibitions set within its digital rights management policies on modifying the product's software could thus constitute copyright infringement. Companies may not want the reputational damage that could accompany pursuing their customers for copyright infringement. However, the threat of legal action, along with the potential loss of the product warranty for violating the company's licensing agreement, does enable companies to impose significant post-purchase restrictions on user activities.

Proprietary Ecosystems and the Right to Repair

Prior to the advent of software-networked goods, companies encouraged customers to purchase their branded parts or patronize authorized suppliers and repairers in part by building customer loyalty. Goods tethered to manufacturers through software, however, allow companies to exert greater influence over consumers' ability to work around the company's designs, locking them even more deeply into proprietary ecosystems and enabling companies to 'hardwir[e] restrictions on consumer behaviour into our devices' (Perzanowki and Schultz 2016, 123). Companies can strongarm customers into purchasing their branded supplies by having the product software authorize or authenticate their parts as genuine, such as by detecting a manufacturer's code or identification chip before the product is permitted to operate (Hruska 2017). A broad range of products, from coffee makers, juicers and cat litter trays to printer cartridges and tractors, now include software verification to force buyers to purchase authorized parts instead of cheaper third-party alternatives. Companies may also strategically employ copyright law to thwart competitors looking to reverse engineer or repair their products from accessing necessary knowledge since product schematics, repair manuals and diagnostic software are typically protected by copyright. This protection makes it more difficult for independent repair shops to access these items.

Social and Security Dimensions

Repair not only entails a consumer right to fix products we buy. Repair also involves a broader set of social and economic benefits (Perzanowski 2022, 17–18). Repair helps consumers save money as product lifespans are extended and secondary markets, including second-hand stores and resellers, provide sources of used goods, an important money-saver for economically marginalized communities. As well, repair helps to decrease the enormous environmental burden of modern consumerism, a problem particularly acute in the manufacture of many technologies that require the extraction of rare earth minerals and, once these products no longer function, are later dumped as often-toxic e-waste, often in developing countries (Forti et al. 2020). The United Nations has found that restrictions on repair contribute to the growing problem of e-waste (Forti et al. 2020).

The right to repair also has a security dimension. Some farmers in Canada and the United States with John Deere tractors facing company-imposed repair restrictions have resorted to acquiring pirated John Deere software from illicit websites in Poland and Ukraine to run diagnostic tests on their tractors and fix or customize the vehicles (Koebler 2017b). Meanwhile, the US Defense Department's increased use of commercial technologies, which is mandated by federal rules, has shifted power to industry actors

and forced the military to accept restrictive warranty provisions that it could previously avoid (Ekman 2019). Elle Ekman, a logistics officer in the US Marine Corps, argues that the Marines are prevented from repairing equipment like generators and engines or from manufacturing parts using their 3D printers. According to Ekman, these restrictions mean that the Marines lose 'the opportunity to practice the skills they might need one day on the battlefield, where contractor support is inordinately expensive, unreliable or nonexistent' (Ekman 2019).

Market Power

When people want someone to repair their connected products, it can be difficult to find an independent repair shop that has the necessary tools, replacement parts and diagnostic equipment. This is because original equipment manufacturers may only supply their authorized repair shops with their branded replacement parts and specialized tools, leaving independent repairers to acquire these items where possible from third-party suppliers (Koebler 2017b). In doing so, companies strategically create a proprietary ecosystem of authorized dealers, resellers and repairers underpinned by the legal authority of IP law and licensing agreements. Through these proprietary ecosystems, companies accrue economic power that enables them to exert control over the market in replacement parts and repair services. Restrictions on repair pose a threat to market competition or what the US Federal Trade Commission has called 'potentially exclusionary conduct' (Federal Trade Commission 2021a, 10).

Market power is evident in how big technology firms impose restrictions on independent repair. In 2018, for example, Apple struck a deal with Amazon that not only expanded the selection of Apple products for sale on Amazon sites worldwide, including phones, tablets and watches, but also sharply restricted the sale of its refurbished products on Amazon. Only Apple or its authorized resellers can sell Apple products on Amazon, meaning independent repairers have to become Apple-approved official resellers to sell goods on the site (Rubin 2018). The Amazon-Apple deal is about marketplace control: Apple receives greater control over the pricing and offerings of its goods on Amazon, while Amazon gains important market insights on Apple sales data, customer purchase patterns and other metrics. Apple and Amazon 'conspired to make it harder for consumers to buy repaired goods' with the effect that these powerful companies benefit 'but consumers, repair providers, and the rest of the planet are worse off as a result' (Perzanowski 2022, 101). The agreement has raised anti-competition concerns, including scrutiny by regulators in the United States, Italy and Germany (Lovejoy 2020).

Apple's strict requirements for selling its refurbished products on Amazon are difficult for small operators to meet (Statt 2019; Stone 2020), which in effect reduces the available selection of used Apple goods. Customers will likely pay higher prices, and defunct Apple products may be unavailable on Amazon. 'My product was sunsetted', says a small repairer of iPods. 'I'm selling something they've completely stopped manufacturing and don't support anymore. Why would that matter to Apple and Amazon?' (Statt 2019).

Restrictions on repair have sparked multiple government inquiries into possible anti-competitive behaviour. The US Federal Trade Commission in 2019 undertook a review into repair restrictions (FTC 2021a). In 2020, Australia's Competition and Consumer Commission (ACCC) studied the after-sales market in agricultural machinery in that country. The ACCC stated its concerns that manufacturers and their authorized dealers 'are controlling access to diagnostic, service and repair materials, limiting the ability of independent repairers to compete in the provision of after-sales services' (Australian Competition and Consumer Commission 2020a, 12). Manufacturers' practice of voiding warranties for machinery repaired by third parties that develop faults unrelated to repair, the ACCC contends, is 'a particularly strong disincentive to the use of independent repairers' (Australian Competition and Consumer Commission 2020a, 12).

The Right-to-Repair Movement

The attempt to engage in 'perfect enforcement' (Zittrain 2009, 123) of a company's terms of service regarding manufacturer-imposed restrictions on repair has galvanized opposition, taking the form of a transnational right-to-repair movement. According to the Australian Government's Productivity Commission, which in 2021 held hearings and issued a report on the topic, the 'term "right to repair" describes a consumer's ability to repair faulty goods, or access repair services, at a competitive price' (Productivity Commission 2020).[4]

By pairing IP law and licensing agreements with connected goods, manufacturers of software-enabled goods have deliberately reduced the spectrum of allowable consumer behaviour and created uncertainty about consumer rights. Advocates portray the right to repair as a fundamental element of ownership. Ownership, in short, entails the right to choose how to use or treat a product. Repair restrictions can be understood as a form of knowledge governance as the intention is for original equipment manufacturers to lock down knowledge relating to the operation and repair of their products. Limiting repair can negatively affect people's creativity and innovation by stifling the freedom to tinker, which includes learning how things work, discerning

flaws, and tailoring, reverse engineering or repairing devices (Samuelson 2016, 564). Tinkering with a product 'means that if there is a problem with it, you can figure it out and you can publicize it', explains Charles Duan, then-director of the Patent Reform Project at Public Knowledge, a Washington, DC-based non-governmental advocacy organization (Duan 2016). As not everyone has the ability or resources to tinker, it's important that tinkerers can share their knowledge and, where appropriate, assist others without fear of reprisal from companies or sanction under IP laws. How software owners permit repairs and modifications is 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 2018, 9).

While the right-to-repair movement has tended to be associated with legal battles to give consumers the right to have smartphones repaired at independent shops, it also brings under its umbrella a broad range of goods with embedded software – from common household appliances to vehicles. Farmers, particularly in the United States, have also been vocal proponents of repairing their agricultural equipment themselves or patronizing independent repair shops because of the high cost of hauling pricey farm equipment from rural properties to manufacturer-authorized repair shops, especially during harvest season (see Carolan 2018). The issue of repair disproportionately affects people living outside major population centres who may have to travel long distances to access manufacturer-authorized repair shops or acquire original equipment manufactured parts. As the US Federal Trade Commission noted in 2021, repair restrictions also unduly affect racialized and low-income communities given the heavy involvement of Black-owned small businesses in the repair and maintenance industries (Federal Trade Commission 2021a, 3–4).

The power asymmetries between consumers and companies, when it comes to the ownership of software-enabled products and related right-to-repair issues, are mirrored globally, with dominant companies largely headquartered in the United States and Europe effectively setting rules restricting users in other markets via licensing agreements. Outside the United States and Europe, countries considering right-to-repair legislation often frame the issue in digital economic nationalist language, emphasizing the need to protect local jobs in the repair and after-sales market industries and underlining the importance of rules that are responsive to domestic democratic oversight and accord with domestic regulatory frameworks. The Australian agricultural equipment market, for example, is dominated by large multinationals, especially those from the United States and Europe, as is the Canadian market: Says Western Australian farmer Paul Green, the need for a right-to-repair movement is greater in Australia than in the United States because 'Australia doesn't get a choice in the types of engines we get. We just get what the Americans and the

Europeans build because the Australian market is just too small' (Burt 2018). Licensing agreements regarding the collection and use of data, as well as any restrictions on repair, are governed by the law of the country where the company is registered, creating uncertainty as to the restrictions on or protection accorded to Australian farmers (Wiseman and Sanderson 2017, 15). Farmers outside the major US and European markets 'may not have the benefit of consumer or other legislative protections of their own country', as disputes tend to be addressed in overseas jurisdictions (Wiseman et al. 2019, 9).

These global power asymmetries extend to the issue of who is able to innovate and on what issues are considered important enough to warrant attention. In the Global South, repairing costly goods like medical equipment or agricultural equipment by independent repair personnel is an essential way to restore and reuse donated or resold critical equipment (He et al. 2021). This practice, however, can be hindered by manufacturers in Europe or the United States that may be reluctant or decline to provide the necessary tools or diagnostic software, making it difficult for non-authorized repairers in the Global South to fix or even modify equipment to suit local needs and conditions (He et al. 2021).

Legislative Action and Industry Opposition

The right-to-repair movement can be understood as a pushback against the commodification of knowledge and a battle over who should be allowed to control and use knowledge – in this case, the ability to repair – and in whose interests. In the case of the right to repair, the battle is between manufacturers (and their industry and government supporters, including in IP offices) that claim expansive IP rights over the embedded software systems in connected devices and, on the other side, repair proponents, including consumer rights organizations. Repair advocates encompass a broad array of people, including aftermarket parts manufacturers, independent repair shops, disability advocates and activists concerned about e-waste and planned product obsolescence.

The right-to-repair debates have been most prominent in the United States and Europe. The US president Joe Biden bolstered the cause in July 2021 with an Executive Order intended to strengthen competition in the US economy, which included support for right-to-repair measures (The White House 2021). The US Federal Trade Commission, in response, determined it would increase enforcement against illegal repair restrictions (Federal Trade Commission 2021c). In the United States, as of August 2022, thirty-four states were considering, introducing or reintroducing right-to-repair legislation (The Repair Association n.d.). Repair legislation, however, faces heavy industry opposition in the United States, as elsewhere. As of August 2022, the

United States has right-to-repair legislation for motor vehicles in Massachusetts and for consumer electronic devices in New York. A Massachusetts law, the *Motor Vehicle Owners' Right to Repair Act* (2012, updated in 2020 for sharing of vehicle data), became a national voluntary standard agreed upon amongst the vehicle industry and trade associations (AutoCare Association n.d.). New York's *Digital Fair Repair Act* (2022) applies to phones, computers and tablets, not farm or medical equipment or motor vehicles. It requires manufacturers in New York State to provide free repair documentation, free diagnostic software and reasonably priced replacement parts and repair tools for consumers and repair shops.

In Europe, the European Parliament has supported strengthening consumer repair options for a more than a decade with the view of developing a more resource-efficient circular economy focused on sustainable growth (Šajn 2022). Since 2020, right-to-repair legislation has been working through the European Union's political processes. In particular, the European Parliament adopted two resolutions on the right to repair, one on a sustainable single market in 2020 and the other on a sustainable economy in 2021 (Bertuzzi 2022). These measures built upon several years of regulations intended to make manufacturing and product design more eco-friendly, including a 'right to repair' for devices like mobile phones, laptops and tablets as part of the European Commission's Circular Economy Action Plan (Gartenberg 2020; Šajn 2022). Measures also include mandatory labelling on the estimated lifetime and reparability of products, such as a repair score for certain product categories, and ensuring that consumers are provided with the information on availability of spare parts, repair services and software updates (Šajn 2022, 7). The European Commission is planning to put forth a legislative proposal on the right to repair by mid-2023 (Repair Cafe 2022).

Other countries, including Australia and South Africa, are considering or are in the early stages of implementing right-to-repair laws.[5]

Despite widespread consumer and political interest in the right to repair in many jurisdictions, concerted industry lobbying has been largely successful in defeating legislation or limiting action to piecemeal changes (see Perzanowski 2022). The right-to-repair lobby has faced well-funded opposition by prominent multinational companies in the technology, vehicle, agricultural and medical device industries, along with their related trade associations, that generally represent knowledge-feudalist positions. Apple, Microsoft, Amazon, Google and Facebook have all lobbied against legislation in the United States, and big industry players including General Motors and John Deere are also vocal opponents.

Countering the right-to-repair arguments, industry actors tend to argue that repairing or tinkering with software-enabled products raises potentially serious security and safety complications. These concerns may be valid in

some cases, particularly when dealing with safety-critical goods like medical devices, where modifying complex software systems requires specialized technical knowledge and the consequences of making a mistake are particularly potent. That said, some industry arguments are less serious on their face, such as an Apple lobbyist's claim in 2017 that if Nebraska passed a right-to-repair bill, it would turn the state into a 'mecca' for hackers (Koebler 2017a; Matsakis 2019).

On another front that demonstrates the contested nature of this issue, John Deere has somewhat softened its stance on self-repair, announcing in March 2022 that customers and independent repair shops can purchase software to diagnose and repair farm equipment (John Deere 2022). In January 2023, in a move that appears designed to deter legislative action, John Deere signed a US-wide memorandum of understanding with a trade association, the American Farm Bureau Federation (AFBF), to expand American farmers' right to repair (see American Farm Bureau and John Deere 2023). In the agreement, John Deere agreed to supply farmers and independent repair personnel with timely access to its diagnostic tools, manuals and software necessary for repair at 'fair and reasonable terms'. What those terms and costs may entail, and how this agreement may meet farmers' needs, are yet to be seen. The agreement is voluntary and commits the AFBF to refraining from supporting or introducing right-to-repair legislation at the state or federal level in the United States. This stipulation demonstrates not only Deere's continued resistance to right to repair but also its continued market power in determining how repairs of its products shall be undertaken.

Apple, after years of pressure from right-to-repair advocates to soften its restrictions on repair, introduced in 2019 its Independent Repair Provider programme in more than 200 countries, which allows independent repair stores to obtain genuine parts, tools and training to fix Apple products (Apple 2021). In November 2021, Apple announced a self-service repair programme for tech-savvy customers to repair certain models of iPhones (Apple 2021). Despite these steps and making its repair manuals freely available, Apple still imposes restrictive conditions that the do-it-yourself repair site iFixit remarks continue to hamstring 'third-party repair with feature loss and scare tactics [that] could dramatically limit options for recyclers and refurbishers, short-circuiting the circular economy' (Chamberlain 2022). Continuing with the theme of control, technology site *Motherboard* revealed details in 2020 of Apple's restrictive contracts for shops in its Independent Repair Provider programme in which Apple required participants to agree to unannounced audits and inspections by Apple, including interviews of shop employees, for up to five years after a shop leaves the programme (Stone 2020).

John Deere and Apple's initiatives, while welcome and an achievement for right-to-repair activists, are relatively modest. Such initiatives are limited

exceptions to the companies' opposition to self-repair rather than a re-balancing of rights back to consumers from companies and, because of this, demonstrate the companies' continued market power. With right-to-repair legislation under consideration in multiple countries, the issue will remain a hot topic for years to come, especially as industry opponents have commercial interests in fighting any change, perceived or actual, in their control over IP rights. Control over repair is a proxy for larger battles for control over technology and knowledge.

CONTROL OVER DATA, CONTROL THROUGH DATA

With networked products, one is not so much buying the physical good as access to the service enabled by the product. The sheer volume of data that networked devices collect, not only to operate normally but also to serve their makers' opportunistic data plans (as outlined in chapter 6), raise serious concerns about privacy, data ownership and consumer choice. Key questions here include who has access to and control over data collected by software-enabled devices, as well as who benefits from the use of the data collected by IoT goods.

For those who are concerned about issues like privacy and control over one's data, one common exhortation is for consumers to choose not to buy networked products. Doing so, however, is easier said than done. In some cases, the choice between networked and non-networked products has effectively disappeared (as expected, given the imperatives of the knowledge-driven economy). Some markets, such as for televisions, are characterized by an 'increasing "erosion of choice"' as fewer and fewer non-smart objects are even being produced (Office of the Privacy Commissioner of Canada 2016; see also Manwaring 2017).

Some people, moreover, may be unable to disconnect from certain smart devices, which may be controlled by landlords or other people in their homes. This problem is particularly acute for victims, and potential victims, of intimate partner violence who can be tracked and abused through software-enabled devices. Perpetrators can use smart locks to lock victims out of their residences or harass an ex-partner by remotely changing the temperature on a smart thermostat (Dragiewicz et al. 2018; Tanczer et al. 2021).

Ironically, and perhaps demonstrating that the data-driven economy isn't the positive revolution it's usually taken to be, some non-smart goods have held their value. As some US farmers have discovered, older, non-computerized tractors remain popular – and hold their value – because they are easy and cheap to repair (Belz 2020). As an added bonus for surveillance-conscious farmers, non-computerized tractors neither automatically collect data on tractor usage nor have manufacturer-imposed repair restrictions.

Data-intensive farming, when the data is proprietary to the company whose sensors are collecting it, can also create lock-in conditions. The longer a farmer uses a particular brand of agricultural equipment, the greater the cost of switching to a different manufacturer because farm data acquires more value over time as more information is collected on seasonal variance, operation error and other data fluctuations (Australian Competition and Consumer Commission 2020a, 15). The value of this historical data may lock farmers into a particular brand of agricultural machinery, as well as render farmers reliant upon data companies that interpret the data and provide actionable recommendations, as the Australian Competition and Consumer Commission noted in its review of agricultural machinery (Australian Competition and Consumer Commission 2020a).

The problem here is not smart devices in and of themselves. Rather, the problem is industry-crafted software licensing agreements that transfer control over the devices from their users and cede it to corporate interests, thereby enabling companies to capture and disproportionately benefit from the products' data flows. Collecting and processing data is not necessarily problematic, as such practices can achieve socially and economically valuable goals. The problem is when data is commodified with a handful of (primarily corporate) actors capturing the disproportionate share of its value, a dynamic also evident in farmers' struggles with big agri-data businesses. In the language of Karl Polanyi, the corporate monetization of farming data has problematically shifted actors away from the central purpose of growing food to nurture people to the (fictitious) commodification of farming data. In this dynamic, ordinary farmers tend to have less autonomy over their sensor-collected farming data, while agri-data companies not only capture the greater share of value but also have the capacity to set rules regarding the access to and use of data.

CONCLUSION

Corporate post-purchase control over connected goods is rewriting long-held assumptions about ownership. In an indication of the structural power that corporate actors can accrue by controlling data flows and IP rights, owners of IP rights are accorded a greater proportion of rights over software-enabled goods than if these goods were mere physical objects. Customers purchase the hardware but rent access to the software, with companies enjoying a continued revenue stream that comes from supplying the software as a service. As a result, ordinary users have only a 'precarious ownership' of software-enabled goods while companies maintain structural power to set the terms under which people can and use the goods, and even the goods' lifespan (Tusikov 2019a).

Certain actors are best positioned to accrue the most benefit in the data economy, namely large commercial actors with the infrastructure to amass, interpret and monetize data, as well as controlling ownership of IP rights pertaining to the data-collecting and data-interpreting technologies. Winners here – knowledge feudalists – are companies that have expanded from manufacturing into data companies, in the fashion of John Deere and General Motors, along with technology firms like Google, Apple and Samsung. In some cases, big tech firms are usurping the positions of companies that traditionally dominated agriculture. A worker for a leading Canadian-based precision agricultural corporation stated that 'our biggest competitor is no longer Monsanto, it's Google' (Bronson et al. 2021, 128).

Those losing out include ordinary people who want to fix or tinker with connected goods themselves, right-to-repair organizations, small-scale farmers, independent repairers, small retailers of refurbished goods, people who patronize second-hand or reseller stores, and those in the aftermarket industry selling third-party parts. Also facing structural barriers are those outside of major population centres, more broadly, people outside the United States and the European Union, whose major manufacturers set rules that privilege their business models. These include farmers in Australia, Canada and elsewhere unable to repair their tractors (see Perzanowski 2022), farmers concerned about how their farming data might be shared or monetized without their consent (Wiseman et al. 2019), and farmers whose business practices are not served by the big data-focused models on monocultural, chemical-intensive productions on the biggest commercial crops (Bronson et al. 2021). In different ways, these actors have clashed with manufacturers' restrictions and the proprietary ecosystems that companies have built to privilege their networks of authorized repair personnel and suppliers.

Depending on the type of data collected and the technology used, people may have differing interests in accessing or exerting control over the data. Farmers, for example, have commercial and personal interests in retaining control over their farming data. Cities may find themselves in the unenviable position of being data exporters where citizens' data flows across their national borders and away from their data protection laws, as is explored in chapter 9. The 'closed architecture' enabled by IoT devices and the legal protection that surrounds them, notes tech CEO and Quayside critic Kurtis McBride, can 'restrict the ability of cities to access the valuable asset (data) that is trapped inside the infrastructure they have purchased' (McBride 2018). Overall, those who control the software facilitating the data flows can capitalize upon the knowledge and power asymmetries between data producers (technology users) and data owners (typically large data companies), a dynamic characteristic of the information-imperium state and of knowledge feudalism in particular.

NOTES

1. John Deere Operations Center webpage, https://www.deere.com/en/technology-products/precision-ag-technology/data-management/operations-center/. Accessed 31 March 2022.

2. For example, the US 1998 *Digital Millennium Copyright Act* (Section 1201) and Canada's *Copyright Act* (Section 41.1) prohibits the bypassing or breaking digital locks, except in very specific circumstances.

3. For a detailed analysis of licensing agreements, their origins in the software industry and implications for ownership of digital and physical goods, see Perzanowski and Schultz (2016).

4. For a comprehensive analysis of the right to repair, see Perzanowski (2022).

5. In Australia, for instance, the ACCC recommended in the May 2021 findings of its study of the agricultural equipment market that agricultural machinery should be included in any right-to-repair programme that Australia may introduce (Australian Competition and Consumer Commission 2021). South Africa's right-to-repair regulations, which came into force on 1 July 2021, enable consumers to choose where to service vehicles without risk of voiding the warranty (Right to Repair South Africa 2022).

Chapter 8

The Data-Driven State

The previous two chapters concentrated primarily on the role of the private sector as a consequential regulator and the resulting effects of private actions in the knowledge-governance sphere. This chapter explores the state side of the information-imperium state, namely the varying interests that states have in facilitating the shift underway to a data-driven society and economy. In particular, it explores how states work to exercise structural power in their cooperative and conflictual relationships with private actors, especially companies whose data-intensive business models place them at the heart of the data economy. This cooperation-conflict dynamic exists because states not only govern through data, such as in the management of public services, but also require detailed industry data to perform important public planning and regulatory functions, data that companies are often reluctant to disclose, as it underwrites their commercial advantage in a data-driven economy.

States are increasingly using data and automated data tools to gain knowledge about their citizens, on actors and practices in the data economy and on potential threats to state security and order. The growth of rich, diverse datasets held by government and private-sector actors, paired with automated tools, provides states with new options for governing through data. States are also increasingly dependent upon big data-driven tools in the areas of national security and political campaigns (see Simon 2019). Related to the question of who has the authority and legitimacy to govern the data economy is the question of which actors possess the requisite data and expertise to do so. Public regulatory efforts, however, may be hampered or even deliberately undermined by private actors who are reluctant to allow governments to access their data, thereby imperilling public planning and regulation (see Scassa 2017).

Driven by the same dataist mindset we've seen at play in other chapters, governments are also embracing the ideological belief that data- and algorithm-fuelled technologies can provide precise quantifiable understandings of human behaviour and events and, more broadly, accurately forecast future events and behaviour (van Dijck 2014). Such technologies, should they work,[1] hold the promise of any number of tangible benefits, including being able to predict who might pose threats to the state, what people might acquire certain diseases and who are best suited as employees or immigrants. Governments that accord value to forecasting all manner of events can be understood as embodying the 'oracle state' (Hayward and Maas 2021, 221).

Relatedly, governments, including those in Australia, Canada, the Netherlands, the United States and the United Kingdom, are trialling the provision of public services through big-data-fuelled algorithms in areas including social assistance, child protection, immigration and criminal justice services (see Eubanks 2018; Redden et al. 2020). According to tech vendors selling dataist solutions to governments, with the correct application of big data-fuelled analytics and automated tools, the public sector can become another 'datafied marketplace' (Redden et al. 2020, 516).

This chapter proceeds in four parts. First, it explores the global battles over knowledge and technology regulation. In this contest, both authoritarian and democratic countries are adopting data-driven tools and engaging in state-corporate partnerships to exert order over and manage populations. Domestically, both democratic and authoritarian states are responding as information-imperium states to the same underlying dynamics that characterize our shared knowledge-driven society, in which questions of knowledge – especially data – regulation and control are pushed to the forefront. Internationally, we can understand tensions in the ongoing trade and technology skirmishes between China and the United States as an example of rising digital economic nationalism confronting the dominant knowledge-feudalist power that is centred around these states' attempts to control and capture global data flows.

From the geopolitical to the domestic, the second section of this chapter explores the challenges states face in governing through data, including state battles with industry to obtain the data necessary for public planning and regulation. In its third part, the chapter shifts to consider some of the consequences of the move towards data-driven public services, specifically how governments use algorithms to deliver a range of public services, including housing assistance and welfare, by profiling recipients, often with discriminatory results. The chapter then offers a brief conclusion.

GLOBAL BATTLES OVER KNOWLEDGE

There is a tendency to draw stark contrasts between surveillance programmes undertaken by democratic versus authoritarian countries, especially those relating to the internet (see, e.g., Glasius and Michaelsen 2018). For example, China's governance of the internet is often portrayed as involving absolute state control, while the United States is lauded for its free-market policies that privilege free global data flows (Shen 2016). This debate unhelpfully counterpoises Chinese 'internet sovereignty' against US 'internet freedom' (Liu 2012; cited in Shen 2016, 305). While there are important social, political and legal differences in state internet surveillance practices between liberal democracies and authoritarian regimes, there are also broad similarities. The information-imperium state is agnostic as to political orientation, with the effect that both authoritarian and democratic states pursue power over (and through) technology, while also enrolling their domestic industries in the pursuit of state policy goals (see Glasius and Michaelsen 2018; Haggart et al. 2021). States, in other words, seek political and economic superiority through the pursuit of technological 'supremacy' (Schulze and Voelseon 2020; cited in Pohle and Voelsen 2022, 8).

Democratic and authoritarian countries have aspirations, if not always the capacity, to expand their control in relation to internet governance, which we interpret broadly as governance of its physical infrastructure layer, along with flows of data in the content and application layers (see Haggart et al. 2021; DeNardis 2014). In an information-imperium state, governments focus on exerting power by controlling and legitimizing forms of knowledge, including through working to set technical and regulatory standards and to establish norms that preference specific political, economic, legal and security policies. States, whether democratic or authoritarian, work with and through regional and international organizations to develop technical standards and governance processes (ten Oever 2021; Cavalli and Scholte 2021; Pohle and Voelsen 2022). Determining encryption standards or data-protection rules shapes not only how the internet operates but also how knowledge is created, accessed and shared. Russia and China, for example, are actively developing norms to legitimize authoritarian power over the internet by persuading like-minded states to do the same and shaping digital governance discussions at the regional and global levels (Flonk 2021). There are also clear security implications to the encryption debate as states have intentions in shaping encryption standards that they can exploit for their security interests, a practice civil rights advocates reject and many security experts argue weakens systems overall (Stevens and Allen-Robertson 2021).

The global trade in information-communications technologies, both hardware and software, employed in state's surveillance programmes 'does

not neatly correspond to the patterns of the liberal-authoritarian dichotomy' (Pohle and Voelsen 2022, 4). Surveillance technologies are not simply manufactured in one authoritarian country for the use in another. Instead, companies in liberal democracies like Canada, France and Japan sell such technologies to repressive regimes and democracies alike (Deibert 2013), as do those in authoritarian countries, particularly China (Feldstein 2019). US technologies, for instance, remain critical to enabling China's surveillance and social programmes operating alongside equipment from Huawei and other Chinese companies, even as there is political pressure 'across the political spectrum in Washington' on US companies doing business in China (Weber and Ververis 2021).

Corporate-state relations – both cooperative and conflictual – are a general feature of political economy, and industry involvement is necessary for effective state internet governance, whether that involvement is achieved through incentives or coercive state pressure (Fuchs 2016; Glasius and Michaelsen 2018). Simply put, state surveillance is strongly interconnected with big tech surveillance (see Tréguer 2019). There is a mutual dependence between states and the private-sector providers of digital infrastructure, including software and hardware providers that supply services like data analytics or cloud storage, as well as companies that provide spyware technologies (see, e.g., Deibert 2013).

Communication scholars Shawn Powers and Michael Jablonski (2015) describe this relationship in the US context as the 'information-industrial complex', while journalist Shane Harris refers to it as the 'military-internet complex' (Harris 2015). Both are describing a dynamic characterized by mutual interests in extending policies and standards that preference US economic and national security interests. This state-corporate dynamic is familiar in liberal democracies from revelations of 2013 leaks by former US National Security Agency (NSA) contractor Edward Snowden, which revealed the extensive cooperation between US technology companies and the NSA and its allies (see Harding 2014). The NSA, for example, relies heavily on siphoning information from US-based companies and, in return, protects these companies from threats, including foreign hackers (Harris 2015). This dynamic extends to influencing the future direction of technological innovation. The US Central Intelligence Agency, acting through its not-for-profit venture capital firm, In-Q-Tel, invests in technologies that will have both commercial potential and respond to the 'technology needs of the intelligence community' (Powers and Jablonski 2015, 65). Because an In-Q-Tel investment indicates government interest and the potential for future government contracts, it has become a 'trendsetter in the ICT venture capital sector', leading to such technological innovations as the Keyhole software underlying Google Earth. This technology has proven important to the military with the US Pentagon relying upon 'Keyhole, using proprietary

satellite imaging to support missions around the world' (Powers and Jablonski 2015, 66).

The information-imperium state describes a similar state-corporate mutual dependency to serve economic and security interests that is evident in authoritarian countries. The Russian government, for example, has ambitious plans to monitor online content and data and create its own internet ('Runet') that the authorities could, if they wanted, disconnect from the global internet, a strategy that reflects, in part, a logic of digital economic nationalism. However, there are vast differences in state capacity to institute their plans as the influence that the state can exert in internet governance depends in good part on the degree to which it controls key corporate actors operating on its territory. In contrast to China, argues political scientist Daniëlle Flonk (2021, 1933), Russia's internet infrastructure is more decentralized and thus is more dependent on legislation than on technical capabilities for its control over the internet. Russia's plans are hampered by technical, economic and political circumstances, notes International Relations scholar Ilona Stadnik (2021), and its legislative efforts are constrained by the government's limited ability to compel compliance from foreign, largely US-based internet giants with its content filtering or data-localization laws, which require data to be stored in Russian territory.

China, with its Great Firewall and bans on popular US-based platforms, is the paradigmatic case of a state exerting control over the internet. Communication scholar Lianrui Jia (2021) argues that despite the Chinese government's heavy-handed social control, governance of the internet in China is more dynamic and less monolithic than is typically portrayed in Western accounts. Rather than operating as mere tools of the Chinese government, there is a 'mutually beneficial symbiotic relationship' (Jiang and Fu 2018, 384) between the government and domestic technology companies, where the latter receive lucrative business opportunities as well as 'access to the government agenda-setting process' (Dai 2021, 51). Because the Chinese state depends on its technology companies not just for security but also for economic prosperity, the companies have some room to manoeuvre with respect to government rules (Luo and Lv 2021). For example, the Chinese government permits internet companies to exploit regulatory grey areas to access international sources of financial capital, especially from the United States, which are essential to the companies' continued growth (Jia 2021; Jia and Winseck 2018; see also Segal 2021). Chinese industry and state interests are both served by a globally expansive technology sector, which is also evident in China's Belt and Road Initiative (sometimes called the Digital Silk Road), a massive project of technological development and investments, including pipelines and railways, throughout Africa, Asia and into Europe to expand China's economic and geopolitical reach (Triolo et al. 2020; United

Nations Conference on Trade and Development [UNCTAD] 2021). China's efforts, particularly through its Belt and Road Initiative, demonstrate its interest in expanding from a digital economic nationalist state into knowledge feudalism.

The Geopolitics of Data

In a data-driven economy, the state becomes a central player because it alone has the power to divert resources at the national scale and craft appropriate regulatory responses (Ciuriak and Ptashkina 2021). States vary widely in capacity and willingness for action, but the view of the state as having the requisite legitimacy, authority and capability to direct and govern the digital economy effectively departs from four decades of economic policymaking that prioritized free-market solutions and minimal government.

As economists Dan Ciuriak and Maria Ptashkina argue, the move to an economy that places intangibles such as data at its centre has profound implications for the role of states at the domestic and international levels (Ciuriak and Ptashkina 2021). This shift towards greater state intervention in the data-driven economy is bringing states into new rivalries, with geo-economic and geopolitical overtones (Ciuriak and Ptashkina 2021, 77). Powers and Jablonski, for example, speculated in 2015 that the knowledge-driven society is leading to the 're-nationalization of transnational companies' (2015, 65). This trend has become increasingly obvious in recent years. Control over digital technologies is part of the ongoing US-China trade war. In addition to having national security implications – an example of how events in the knowledge structure influence events and actors in the security structure[2] – the US-China trade dispute is also a technological dispute, with both parties wanting to dominate global markets in advanced technologies like robotics, autonomous vehicles and artificial intelligence (Kim 2019). In what some characterize as a 'technological cold war' (e.g., Muñiz 2019), the US government has targeted Chinese technology companies. In particular, they have focused on Huawei, the massive manufacturer of telecommunications equipment, including consumer electronics and hardware for wireless networks, over concerns that Huawei may facilitate spying by the Chinese government on the United States (Segal 2021).

The US government has thwarted Chinese investment in US technology and data assets and tried to exclude Chinese technology experts from participating in international standards-setting bodies (Ciuriak and Ptashkina 2021, 88). What both countries have in common is a heavy investment, both public and private funds, in developing technologies critical to the data-driven economy (Ciuriak and Ptashkina 2021). Long-term effects from the US-China trade war are uncertain, as is whether US hegemony is declining and whether

the balance of power is shifting towards China. Many scholars contend that the United States' structural economic power remains strong, with its large consumer market, a disproportionate share of global production and related revenue streams, and the structural power of the US financial market in the global economy (see Drezner 2021; Schwartz 2017). These features, achieved in no small part through US advocacy for ever-stronger intellectual property (IP) rules globally and free transnational data flows, make the United States the leading knowledge-feudalist state.

In contrast to the United States and China, both of which are technology superpowers along with their economic and military might, the European Union is establishing itself as a regulatory superpower, using the size of its market to export its preferred regulatory frameworks like the 2018 General Data Protection Regulation (GDPR) and policies to enable the free flow of data throughout the European Union (see particularly Bradford 2020).

As we will discuss in greater detail in chapter 9, the GDPR operates as an international standard-setting framework, as it sets rules and practices to ensure a regulated trade for all entities that deal in personal data, applying to all entities that deal in the digital personal data of European Union residents. Companies in countries outside Europe may implement EU-style data-protection standards to do business with European Union residents or make their entire production lines compliant with European Union standards (Bradford 2020). Multinational tech companies, like Apple for example, extend their GDPR-compliant policies to users outside the European Union (Bradford 2020, 142–47). Similarly, to facilitate trade with Europe, companies 'across Africa, Asia, and Latin America have followed EU data protection standards' (Bradford 2020, 172). In this way, EU standards reach beyond Europe, a type of extraterritoriality that international legal scholar Anu Bradford (2020) calls the 'Brussels Effect'. As developed by Bradford, the 'Brussels Effect' refers to the European Commission's practice of strategically exporting its preferred standards globally in areas such as environmental protection or consumer protection through the de facto extraterritorial application of its regulations. The European Union's status as a global regulator is not only the result of its large internal market but also because it has strategically crafted 'an institutional architecture that has converted its market size into a tangible regulatory influence' (Bradford 2020, 25). As a result, the European Union's power can be understood as stemming from its legal innovations, in contrast to the technological innovation of the United States and China (Daly 2021, 69). Despite its focus on human rights in data governance, its ambitions to set global data-protection and other standards suggest that the European Union can best be understood as endeavouring to become a knowledge-feudalist state, with it setting the global rules regulating the free flow of data.

The European Union is not alone in its global data standard-setting efforts. In April 2022, members of Asia-Pacific Economic Cooperation (APEC) created the Global Cross Border Privacy Rules (CBPR) System to regulate cross-border data flows (United States Department of Commerce 2022). The CBPR is an effort to globally expand APEC's regional system by bringing together the United States, Canada, South Korea, the Philippines, Singapore and Taiwan to 'facilitate data protection and free flow of data; disseminate best practices for data protection and privacy and interoperability; and pursue interoperability with other data protection and privacy frameworks' (United States Department of Commerce 2022).

While they lack the resources of the great powers, smaller states are also pursuing digital economic nationalist approaches. These include policies to create and protect domestic technology industries. For many countries, developing domestic technologies is not only perceived as a smart economic move to capture greater portions of the value chain but also a hedge against globally dominant US-based technology giants. State responses to digital capitalism vary depending upon specific countries' historical, political, and social contexts, for example, reproducing colonialist patterns of resource extraction throughout the Global South (see Couldry and Mejias 2019). In the context of Latin America, for example, International Relations scholar Jean-Marie Chenou (2021) highlights how states are pursuing what he calls 'varieties of digital capitalism'. Surveying several Latin American countries, he argues that the state has been active in translating global economic and technological pressures into 'different regional and national contexts', reflecting both their history and position within the global economy (Chenou 2021, 212).

States Tapping into Global Platform Power

As Susan Strange noted, the ability to control how knowledge is disseminated is a central element of structural power, with effects on everything from economic well-being to ensuring the security of states and their populations (Strange 1994). It should therefore come as no surprise that states have a long history of seeking control over various communications technologies, from the telegram, mail system and telephone to radio and television, a centuries-long tradition that includes internet communications technologies (see, e.g., Goldsmith and Wu 2006; Spar 2001).

Globally-operating internet firms offer states extraterritorial reach if they can tap into companies' networks, including over internet firms that provide the critical services of search, payment and domain name functions (Kohl 2013; Pohle and Voelsen 2022). Platforms, as set out in chapter 6, are two- or multi-sided markets focused on extracting and controlling data (Srnicek 2017; Dunne 2021), and their position within the marketplace makes them an

attractive target for states.[3] Private actors can exploit their position as providers of key commercial and technical services by monitoring or blocking information flows, or structuring markets in their favour as is evident in Google and Apple's duopoly in mobile operating systems and app ecosystems (Nieborg et al. 2020). Companies that operate key services offer an attractive leverage point for states that can co-opt or coercively pressure private actors (Birnhack and Elkin-Koren 2003).

Depending upon the type of services provided, key internet companies that command dominant market shares can exert structural power in several ways, including through what Tusikov (2016) calls access or revenue chokepoints. By withdrawing payment services, platforms can disable websites' capacity to process payments or receive advertising funds, thereby 'choking' the websites' revenue streams (Tusikov 2016). Platforms can also interfere with the proper functioning of domain services, rendering the targeted entities commercially nonviable by preventing users from accessing the desired site. Companies with global operations, dominant market shares and providing vital services can have a regulatory capacity similar to or even exceeding that of typical state regulators.

Platforms' legal authority to enact chokepoints on behalf of states stems from the platforms' terms-of-use agreements where they can remove content or terminate services even when the act in question is lawful. As Tusikov details in her book, *Chokepoints: Global Private Regulation on the Internet* (2016), states best positioned to leverage cooperation from internet companies are those that can encourage – or coerce – companies into action in the absence of legislation or formal legal orders with credible threats of legislation or legal action. Government officials in the United States and European Union, for example, have pressured companies to act against child sexual abuse content, counterfeit goods and copyright-infringing content on the internet (Tusikov 2016). States can also pressure companies to exceed their legal responsibilities 'voluntarily', that is, in the absence of legislation or formal legal orders, a practice understood as 'compliance-plus regulation' (Tusikov 2019b). This tactic can enable states to reach beyond their jurisdictional boundaries and export their desired policies extraterritorially. For example, the US government pressured the Chinese platform Taobao to strengthen its enforcement policies 'voluntarily' to protect US companies complaining that Taobao was selling counterfeit versions of their products (Tusikov 2019b). The US government used threats of withdrawing access to its market to push a Chinese marketplace to change its practices because the protection of IP is a key US economic (and national security) priority (Tusikov 2019b; see also 2021).

There are several key lessons we can draw from states' efforts to weaponize chokepoints. Not all states have equal capacity to compel compliance:

leveraging large platforms is primarily the domain of powerful actors like the United States, European Union and China, but even large states have only been partially successful, at times, in their efforts to regulate such firms (Rone 2021).

Relatedly, companies vary in their ability to resist states. Jurisdiction remains important, as governments may have greater influence over companies that operate within or are headquartered in their territory. Firms, simply put, are national, not global. Conflicts between states and private actors – and amongst private actors – are inevitable (Avant et al. 2010; Rone 2021), as they may have shared interests but differing goals in expanding their control over the internet. US-headquartered tech firms have sometimes adopted aggressive legal strategies to defend their business models built upon data extraction and global flows of data in countries that have different political norms. In Brazil, for example, independent researcher Pedro Mizukami, who worked for the Centre for Technology and Society at FGV Rio from 2007 to 2018, recalled to us that in Google's entrance into the country, 'Google had a very aggressive strategy' and 'wouldn't comply with orders' from judges to remove content from its services. Brazilian judges 'absolutely hated Google because they were challenging our jurisdiction, they were defying our authority: "they're not respecting Brazilian law, who do they think they are?"'[4]

Regulating Financial Technologies

State interest in knowledge governance extends to the financial structure, which – like the rest of society – is being reshaped by the rising knowledge structure in a contest not only between public and private power but also amongst actors whose power comes from different structures in the global political economy.

To take the most high-profile example of a financial technology that has the capacity to upend the financial structure, consider cryptocurrencies.[5] While cryptocurrencies had been around since 2008 and the invention of Bitcoin, it was Facebook's June 2019 launch of Libra, its much-publicized proposed cryptocurrency, that really got regulators' attention. It signalled the entry of the global data giants into 'finance in such a fundamental way as to have the potential to usurp many of the functions of central banks, including monetary and payment systems' (Zetzsche et al. 2021, 82). Regulators and traditional financial institutions reacted immediately. Facebook appeared not to have adequately consulted regulators and its plans were 'vague, incomplete and contradictory', a particularly troubling situation as Facebook's 'Two billion users meant the reserve would be large enough to affect whole countries' financial systems, and knock out small currencies entirely' (Gerard 2020, 8; see also Murphy and Stacey 2022).[6]

Facebook's ambitions and the perceived threat to financial markets and state authority over financial matters triggered strong reactions throughout

the international financial system. Less than two weeks after Libra's launch, influential financial regulators, including the Financial Stability Board (FSB), US Federal Reserve, Bank of England, Bundesbank and Bank of France, stated they would each examine Libra and apply strict regulatory standards, while the Group of Seven countries set up a high-level forum to examine the risks of digital currencies to the financial system (Zetzsche et al. 2021, 81). Clearly, when states – alongside the powerful financial institutions – perceive potential threats to their financial structural power, action is swift.

Similarly, governments around the world are scrutinizing cryptocurrencies, with many regulators raising concerns about their effects on both financial stability and security generally. On the latter point, cryptocurrencies play a key role in 'ransomware' attacks, in which malicious actors encrypt an individual's or organization's hard drive and demand payment in (supposedly) untraceable cryptocurrencies (Myre 2021). In February 2022, the FSB, an intergovernmental organization that monitors the global financial system, issued a report on cryptocurrencies that outlined its concerns with cryptocurrencies. The FSB concluded that while crypto-assets represent a small part of the global financial system, crypto-asset markets are 'fast evolving' and could reach a point where they 'represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system'. These vulnerabilities include the lack of regulatory oversight of the sector, as well as poor investor and consumer understanding of crypto-assets, money laundering, cybercrime and ransomware (Financial Stability Board 2022, 19).[7]

Even while states are working to regulate financial technologies, they are not doing so uniformly, and business interests are working to influence results. As economic historian Adam Tooze highlights in a survey of the current global regulatory framework, the United States, European Union and China have all highlighted the need to regulate cryptocurrencies, with China having done the most to curtail their activities, not least because of worries about the potential threat these speculative assets pose to global financial stability (Tooze 2022). This case has become much easier to make following the spectacular failure of several key crypto exchanges, most notably the potentially fraud-related implosion of FTX in Fall 2022 (Levine 2023). In the wake of the sector's collapse, the United States administration of Democrat Joe Biden has become much more suspicious of cryptocurrencies, most notably in his March 2023 Economic Report of the President, several pages of which were devoted to a scathing critique of crypto (United States Council of Economic Advisers 2023, 237–75).

Beyond this day-to-day drama lies the pursuit of structural power and the reinforcement of US global advantages, which includes leadership in the digital-finance space. In March 2022, President Biden signed an Executive Order on developing and regulating the market in digital assets, including

cryptocurrencies. Alongside ensuring protections for US consumers and businesses and ensuring the stability of the financial system globally, the Executive Order explicitly lays out the US interests in reinforcing United States' 'leadership in the global financial system' and ensuring the country remains at the 'forefront of responsible development and design of digital assets and the technology that underpins new forms of payments and capital flows in the international financial system' (The White House 2022).

The push to regulate cryptocurrencies, in its early stages as we write this section, is a clear example of the contest for structural power within and between the knowledge and financial structures, engaging state and non-state actors in cooperation and conflict in the pursuit of their interests. As with all such conflicts, its outcome will reveal a great deal about who holds power in the twenty-first century.

STATES GOVERNING THROUGH DATA

Contemporary states' interest in and practice of expanding their control over online spaces represents a continuation of their historical practices of exerting power over information flows within their jurisdictions. States have long sought to exert control over their citizens through comprehensive knowledge of those populations. As James Scott (1998) sets out in his book *Seeing Like a State*, making a population legible – that is, defining – by quantifying and categorizing aspects of people's lives is amongst the first actions of colonizing forces after invasion. State practices of counting and managing populations typically reinforce social hierarchies demarcated by class, gender, race, citizenship, sexuality, disability and other social characteristics. Scholarship by Ruha Benjamin (2019) and Simone Browne (2015) demonstrates that contemporary US surveillance efforts are rooted in centuries-long racist practices going back to the transatlantic slave trade and colonial conquest.[8]

Controlling Populations through Data

In the information-imperium state, amassing and analysing data is a path to political, economic and social power (see chapters 2 and 3). Regulation – that is, the setting or enforcing of rules, or the delegation of that power to other actors (see Black 2008) – is a key way in which the state attempts to exert control through data. Both authoritarian and democratic countries are increasingly adopting data-fuelled tools to deliver programmes and for policymaking. States are susceptible to dataist claims that data-driven tools will augment public-sector practices, making government more efficient and able to distribute resources more effectively. In China, for example, government

officials see value in adapting technology companies' perceived data-driven efficiencies to the public sector (Dai 2021). Alibaba founder Jack Ma has been reported to claim (paraphrasing his words) 'that "dataism" could ultimately replace the market system with technology-empowered central planning' (Dai 2020, 50). Whether in authoritarian or democratic countries, there is little difference in state or market logic when it comes to operating through data, driven as it is by the seductive idea, that government, like technology companies, can achieve efficiency, accuracy and power through command over data.

India and China provide notable examples of states that have adopted data-driven tools to implement society-wide social and economic programmes aimed at 'modernizing' parts of their respective states (Henne 2019; Dai 2020). While there are significant differences between the Indian government's Aadhaar programme and China's social credit programme in terms of design, goals and, not least, the political orientation of the governments involved, it is worth considering their similarities.

In 2010, India launched its Aadhaar programme, a national identification initiative that operates by assigning a unique twelve-digit identification number to every Indian resident tied to their biometric information, specifically fingerprints, iris scan and a facial photograph (Masiero and Shakthi 2020). Aadhaar is a way for the Indian government to verify individuals' identities with the aim of making the distribution of subsidies and benefits, including food subsidies, more efficient and comprehensive, as many people in the country lack formal identification documents (Henne 2019). The Indian government explicitly sets out Aadhaar's purpose as 'improving efficiency and efficacy' and 'curbing leakage', where beneficiaries do not receive the services or benefits to which they are entitled, such as when someone else takes their food rations.[9]

Western media accounts of China's social credit programme, meanwhile, often commonly mischaracterize it as an extension of the country's repressive surveillance and censorship systems like the Great Firewall that blocks non-approved foreign sites and services (e.g., Greenfield 2018). China's social credit programme is not simply about social control (Daum 2019), nor does it assign each person a single 'credit' score (contra Greenfield 2018). Created as part of China's efforts to modernize and transition to an information era, the social credit programme is a wide-ranging series of policies and regulations aimed at monitoring and managing the trustworthiness of people, companies and governments in China (Zhang 2020; for historical context, see Jia 2020). Although too complex to examine in detail here, the system has three pillars: (1) a financial credit reporting component for individuals and enterprises to determine creditworthiness, similar to those found in many countries; (2) a moral education component focused on core values of trustworthiness,

honesty and integrity; and (3) an administrative enforcement component involving a series of industry blacklists and joint punishment agreements for those who violate laws and regulations (Daum 2019; Dai 2020; Zhang 2020). The programme is largely, though not exclusively, aimed at businesses, particularly forcing non-compliant businesses to abide by court rulings (Dai 2020; Zhang 2020). People with outstanding court fines could be blacklisted from flights or train travel, while businesses could face bans from government contracts or subsidies (Daum 2019).

For our purposes, several similarities between the two systems are important. Each programme relies upon partnerships between governments and private-sector technology companies and incorporates technologies to identify and track citizens as part of the programmes (for India, see Henne 2019; for China, see Jia 2020). Further, each programme has ambitious bureaucratic goals. For India, it was to make efficient the distribution of its social assistance benefits, specifically food aid (Masiero and Shakthi 2020), and for China, it was to strengthen the efficacy and legitimacy of its judicial system (Dai 2020).

Aadhaar is rooted in the dataist assumption that human bodily data can unproblematically be rendered into code, which in turn gives rise to problems of biometric accuracy – that is, situations in which people's bodies don't fit the norms coded into the programme (on this critique, see Magnet 2011). There are significant consequences when people's biometric details (e.g., irises or fingerprints) cannot be accurately read because of illness, heavy labour or poor data practices, for example, people may be denied services like food aid (Henne 2019). India, in other words, is datafying its population, instituting a sort of 'coded citizenship' that is categorizing its entire population through technological means (Masiero and Shakthi 2020, 3). Aadhaar is not a standalone project; it is part of a larger set of programmes and infrastructure called 'Digital India' that includes strengthening cybersecurity, digital literacy, nationwide internet access and delivering social services like health and education digitally to rural areas (Shallu and Ravi 2019).

Legal scholar Xin Dai (2020, 43) argues the Chinese government's motivation for the social credit system is also part of a broader effort to improve the authority and effectiveness of its judicial system, as too many court judgments were ignored, damaging the legal system's credibility. The social credit programme, Dai (2020, 45) contends, involves rearranging the country's institutional resources by, for example, making its court systems more effective and instituting a consumer credit rating system. However, the Chinese government's authoritarian interests in political control, Dai (2020, 47) argues, should not be seen as separate from its economic development interests, as both elements are evident in the social credit system, but when those interests conflict, political interests typically prevail. It is these governmental interests in political control that scholars focus upon in their warnings

that the social credit system enables the government to enroll information and telecommunications companies in the monitoring and governance of vast swaths of political, social and commercial activity in China (Liang et al. 2018). Overall, India's Aadhaar and China's social credit programmes illustrate efforts by democratic and authoritarian states to exert power through command of their citizens' data.

Just as data-driven technologies have become integral to the operation of many governments' bureaucracies, political parties have become increasingly reliant upon data-driven political campaigns, lured by the promise of being able to track and understand voting intentions at ever-more granular levels. Parties' reliance on big data explains, in part, why governments are often reluctant to set rules limiting its use by political parties (for Canada, see Bennett 2022, 2016). Political data analytics companies, such as the infamous Cambridge Analytica, promise to identify and target individual voters and, crucially, 'persuade them to act, donate or vote in line with the clients' interests' (Simon 2019, 165).[10]

The microtargeting of individuals raises concerns not only around data privacy and the potential for data breaches. It also raises the potential for voter manipulation. For example, microtargeting could allow candidates and parties to present different information to different voters to appear as 'a different one-issue party' to different voters. This approach reduces the transparency of the electoral process because it makes it difficult to determine for what positions the party or candidate actually stands. Or microtargeting could lead parties to neglect certain groups of voters entirely, which is also not healthy in a democracy (Borgesius et al. 2018, 87–88). That said, mirroring claims made about algorithmic processes in other sectors, political data analytics companies promise accurate predictive power. Even though there is little substantive proof that they can deliver on their predictive promises (Simon 2019, 165) – for reasons that we discussed in chapters 4 and 5 – microtargeting remains a favoured electoral tactic. Dataism is an ideology that is not easily set aside.

Battling 'Data Deficits'

All public regulators require timely access to data, but government officials' battle to access and use relevant data from industry to regulate the digital economy is particularly acute within cities. Municipal officials are at the forefront of dealing with the gig economy, as ride-hailing and accommodation companies like Uber, Lyft and Airbnb operate locally and city officials often play key roles in licensing such companies and setting operating standards, such as fare rules in the taxi industry. With the rise of ride-hailing and accommodation companies cities also face another key challenge: accessing data for public planning. Central to the platform business model is data extraction and

monetization (Srnicek 2017), meaning such companies have little material interest in disclosing voluntarily their datasets, even to governments. There are real consequences to private-sector data hoarding. City officials lacking a detailed understanding of the effects of ride-hailing vehicles on transit use or rental unit turnovers struggle to plan housing and transit policies, a consequential 'data deficit' (Scassa 2017) in policymaking.

Uber and Airbnb have attracted headlines around the world for their aggressive entry into cities, often in defiance of local laws related to private transportation services and commercial accommodation, respectively. Airbnb, for example, has been described as engaging in 'a city-by-city, block-by-block guerrilla war' against local governments (Martineau 2019). These data-driven companies that strategically describe themselves as technology firms, not taxi companies or hotels, have also raised the ire of hotels and taxi companies. Residents, governments and industries have a long list of complaints against the gig economy, ranging from unfair labour practices and undercutting incumbent industry to operating without the licensing and regulatory frameworks imposed upon traditional industry actors (Dolber et al. 2021). Ride-hailing platforms, in particular, are challenging municipal governments, as they have positioned themselves outside of local taxi industries' usually tight regulation, thus representing a challenge to municipal governmental authority (Zwick 2018; cited in Spicer et al. 2019, 159).

Data-based companies' operations may impede or outright thwart government regulation and public planning. Municipalities collect important data in the normal course of granting business licences and enforcing services like transportation and housing. Lacking data on rentals available through accommodation apps like Airbnb limits policymakers' understanding of the size, nature and effects of platform-based rental activities in communities (Scassa 2017). Without access to popular mapping apps, data from ride-hailing services like Uber, or e-scooter company data, city officials have an incomplete understanding of traffic patterns or transit needs. City planners and officials need this data to: manage traffic; maintain safe, effective travel networks; evaluate public transit routes and service times; consider changes like congestion pricing; and react to incidents like accidents, sporting events and, in emergency situations, evacuations. Moreover, leaving the collection and use of this data to the private sector can lead to perverse outcomes. Traffic apps, for example, are designed to help individual drivers quickly reach their destination but neglect to consider consequences, such as their role in causing systemic traffic congestion or routing speeding commuters through quiet residential streets (MacFarlane 2019).

Access to data can also be a problem when municipal authorities contract gig economy companies to provide services, as became evident in the 2017 ride-share partnership between Uber and the small Ontario town of Innisfil,

located north of Toronto, to complement the town's struggling public transit system (Ruggles 2021). While the public strongly approved of the programme, in which the town subsidized a monthly quota of rides, its costs ballooned as riders took more trips than planned (Pentikainen 2021). There were also municipal data deficits as city officials had to request data from Uber on rides and customers, an important shortcoming as municipalities usually have their own data on transit systems (Ruggles 2021, 151). The Innisfil programme also provides Uber with valuable transit data on a rural municipality, an unusual dataset for its largely city-based services that may help the company expand to other rural areas (Ruggles 2021, 154).

Data Companies as 'Policy Disruptors'

Partnerships with ride-hailing firms are a 'modern take' on public-private partnerships, as urban studies scholar Zachary Spicer (2021, 179) notes. In contrast to traditional partnerships, these 'relationships do not transfer risk to the private sector' as the municipality retains 'operational and policy risk' leaving governments, not firms, responsible for any actual or perceived deficiencies (Spicer 2021, 179, 165). As a result, gig economy companies like Uber should be understood as 'more than just market disruptors; they are also *policy* disruptors' that act 'by exposing gaps in existing regulatory regimes and straining the relationship between regulators and market incumbents' (Spicer et al. 2019, 147; emphasis in original). Policy disruption occurs when business innovation upends the structure of an existing regulatory system (Biber et al. 2017) such as by exploiting legal loopholes, thus necessitating novel regulatory responses (Spicer et al. 2019, 148).

Companies can disrupt public policymaking when they withhold data critical to regulating core public services and public planning, thereby causing 'data deficits' that impair municipal government officials' capacity to govern (Scassa 2017). Alongside using IP law and licensing agreements to set out their proprietary control over data, companies may argue that their collected data may be confidential information, thereby typically requiring governments to obtain a court order to access the data (Scassa 2017). Given companies' reluctance to share data for public planning, some cities, including Vancouver and San Francisco, have resorted to legal action to compel access to privately held data, but this is costly and time-consuming (Scassa 2017).

Where companies share their data with governments, it is often insufficiently detailed and lacks important information about how the data was collected and processed, as well as categories of data (Scassa 2017). Uber, for example, has shared limited, aggregated datasets on traffic speeds and travel times for certain US cities, but researchers contend the company was 'cherry-picking data' (Dobush 2020) to counter criticism that it is responsible

for increased traffic congestion and declines in transit ridership (see Ward et al. 2021).

Not content with merely co-developing rules with governments, some gig companies are inserting themselves into areas traditionally seen as the purview of governments, such as tax collection and remittance. Airbnb, for example, uses voluntary tax collection agreements to collect taxes from hosts, a policy it instituted in response to government calls for Airbnb to comply with taxes on accommodation (Scassa 2017). Problematically but predictably, Airbnb's solution cuts government out of the data loop, as government receives taxes owed but without 'collecting any data from the hosts' (Scassa 2017, 1067). In other words, governments may receive taxes due but without valuable data about people working in the gig economy. Uber and Airbnb are each positioning themselves 'an expert policy intermediator, offering insider knowledge' of the urban economy with the goal to 'dominate and limit the discourse on regulation by assembling and promoting transferrable sets of policing and regulatory approaches' that benefit their interests (Grisdale 2021, 36).

DATA-DRIVEN PUBLIC SERVICES

Governments require data to govern, be it with respect to the collection of taxes, defence of borders, approval of new pharmaceuticals or any other policy area. For governments facing budget constraints and public or political opposition to the expansion of public services, dataist promises are nearly irresistible: that agile precise automated tools can perform tasks formerly undertaken by skilled frontline civil servants, even including programme delivery. Governments' growing reliance upon technology- and data-driven solutions to automate processes in service delivery can be understood as the rise of a regime of data analytics in public services (Eubanks 2018).

It is therefore no surprise that governments are using automated decision-making in immigration applicant screening (Molnar and Gill 2018), predicting recidivism (Rudin et al. 2020), addressing child welfare (Redden et al. 2020), identifying welfare fraud (Mann 2020; Vervloesem 2020) and determining eligibility for housing and social assistance (Eubanks 2018). Similar to companies, governments around the world are adopting dataist ideas that attempt to quantify human behaviour, with the aim of precisely and efficiently predicting human behaviour and events. Automated decision-making often involves 'practices of categorizing and segmenting, and sometimes rating and ranking, populations according to a variety of datasets, with the goal of allocating services accordingly and identifying specific "risks" and behaviours' (Dencik et al. 2018). Decisions encoded in software, not decisions made by

frontline bureaucrats, determine who is eligible for services or flagged as potentially having committed fraud.

Automated decision-making in this context refers to the application of computerized data to the administration of 'simple legal rules amenable to coding as deductive reasoning steps', explains legal scholar Terry Carney (2020, 2). Such systems could determine whether applicants are eligible for a government service by examining applicants' age and income. Algorithms used in decision-making processes, sometimes termed 'policy algorithms', can be categorized into three types (Carney 2020, 5). Supportive automation assists human decisions, meaning that there is an 'electronic application of a rule-based decision' (Carney 2020, 5). Replacement automation replaces human decision-making with algorithms, while disruptive automation results 'in different *forms* of administration and justice' (Carney 2020, 5; emphasis in original). The latter two types of automated decision-making – replacement and disruptive – offer the seductive promise of policymaking that exceeds the human capacity for understanding and processing complex information. Legal scholar Michael Veale and regulatory scholar Irina Brass (2019, 126) refer to these types of advanced automated processes as 'augmentive' decision-making as that, when data sources are combined, can '"mine" data for insights public professionals alone would miss'.

While machine learning and automated tools for processing information are evolving quickly, predictions of sophisticated decision-making remain 'speculative' as these tools currently 'fall short of *replicating* complex human reasoning' (Carney 2020, 4; emphasis in original). As we discussed in chapters 4 and 5, claims of automated data tools' accuracy and precision are too-often empty marketing promises as automated decision-making typically cannot yet replace the complexity of human reasoning. Governments are often keen to tap into the extraordinary power that algorithms promise, which in this case is the better use of public resources through data, a set of practices that often involves subjecting people to continual surveillance and auditing. In this sense, governments like other actors may be susceptible to 'automation bias' in which people tend to attribute greater accuracy and legitimacy to technological outputs than human judgement (Cummings 2004; cited in Redden et al. 2020, 520).

Automated Welfare Eligibility

Automated tools are invariably marketed as quick-fix technological solutions to social problems that almost always have very complex, often historically rooted, pathologies. Because they are seen as unbiased, new technologies often elicit a 'dangerous form of magical thinking' (Eubanks 2018, 183) that is ahistorical and ignorant of the socio-political contexts from which the problems

in question emerge. Automated tools focus on technical problems, such as identifying welfare payment discrepancies, but this focus not only deliberately ignores the broad causes of social problems like poverty but also works to delegitimize efforts for structural and institutional reform. For example, if the 'problem' is defined as one of individual 'welfare cheats' who can be countered by automated tracking of payment anomalies, then structural programme reforms to address underlying causes of poverty are perceived as unnecessary.

Failures in automated social assistance or welfare programmes have arguably attracted the most media attention amongst governmental experiments with automated decision-making. This is particularly the case with automated debt-recovery programmes designed to detect possible cases of welfare fraud or overpayment and claw back funds from recipients. Welfare recipients are a perfect test population for governments to apply experimental treatments as they have few socio-political advocates and tracking applicants appeals to '"tough on welfare" constituencies' (Carney 2019, 5). People on social assistance are amongst the 'most highly surveilled and regulated in Western societies' (Mann 2020, 6). Sociologist Krystle Maki (2011, 60) notes that welfare recipients are often perceived as 'neoliberal deviants', a portrayal that reinforces stereotypes of poor women, especially racialized women, as 'inherently suspicious', necessitating 'invasive welfare programmes that track their financial and social behavior' (Eubanks 2014).

Automated debt-recovery programmes have wrongly identified innocent recipients as fraudsters and accurate payments as errors. In the Netherlands, for instance, the tax authority implemented an automated welfare fraud-detection system in 2014 called SyRI (Systeem Risico Indicatie) that compiled claimants' personal data from different government databases containing details of retirement or housing benefits to detect possible cases of fraud (for a detailed history, see van Bekkum and Borgesius 2021). The programme wrongly accused thousands of people of fraud, particularly people from low-income neighbourhoods where the programme's efforts were apparently focused (see Vervloesem 2020). In 2020, a Dutch court decided the SyRI legislation was unlawful as it did not strike a fair balance between fraud detection and privacy; moreover, the court found the system was opaque and collected more data than it needed to operate (van Bekkum and Borgesius 2021). As the Dutch government did not appeal the court's decision, SyRI will no longer be used, but it is unclear if this decision also applies to other fraud-detection systems in the country (van Bekkum and Borgesius 2021).

To explore the operations and real-life consequences of automated decision-making programmes, consider Australia's Robodebt programme, which attracted international media attention when it was revealed that its algorithms wrongly determined that hundreds of thousands of poor and vulnerable Australians had received welfare overpayments, with accusations by

family members that some people identified as wrongfully owing payments took their own lives (Medhora 2019). In July 2015, the Australian government began an automated debt-recovery process to detect and recover overpayments to welfare recipients in a programme officially termed the 'Online Compliance Intervention' programme but commonly known as 'Robodebt'. The automated programme replaced a manual verification process in which bureaucrats hand-checked records and contacted individuals (Mao 2020). Prior to Robodebt, the Australian government already had a 'lean' administrative capacity in Centrelink, its social service agency, with few internal policy experts, meaning that government staff were distanced 'from a detailed appreciation of the needs of clients when designing [this] AI' (Carney 2020, 22).

Robodebt's algorithm operated by matching welfare recipients' biweekly income with tax data to identify discrepancies, which the programme determined as overpayments, then informed recipients to repay the amounts or have their welfare payments garnished. When weekly income varied, as with those working irregular shifts or part-time hours, the algorithm flagged these as possibly suspicious discrepancies. Recipients' ability to appeal the decision was hampered by the fact that the programme denied clients access to their own data, held by Centrelink – data that could possibly have helped them resolve their case (Henman 2019, 77). Making things worse, Robodebt's algorithm identified only apparent overpayments, not underpayments. As a result, argues criminologist Monique Mann (2020, 5–6), rather than 'administering welfare' by ensuring that recipients received the accurate payments to which they were entitled, compliance officers largely focused on 'raising revenue', with perceived overpayments returned to the government.

Robodebt attracted widespread media attention with mounting complaints from recipients who received massive erroneous bills and accounts of people committing suicide because of debt notices they could not repay. The programme was a disaster, 'based on a tabloid myth of rampant welfare fraud [that] was heartlessly implemented, and which turned out to be illegal' (Manning 2020). In 2019, the Federal Court of Australia concluded that the debt calculations were based on erroneous assumptions of averaged income and the government conceded that its automated approach to debt recovery was illegal (Mann 2020). In 2020, the government announced it would refund more than AU$721 million unlawfully charged on debts to about 400,000 vulnerable Australians and, in 2021, agreed to a settlement of AU$1.2 billion in relation to a class action lawsuit (Doran 2020).

Problems with Algorithmic Decision-Making

Automated decision-making feeds into the dataist logic explained in chapters 4 and 5 in that algorithms' creators make broad, sometimes untested, claims

about their predictive accuracy and effectiveness. In her essential *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, political scientist Virginia Eubanks (2018) concludes that algorithms are too often considered more reliable and accurate than human decisions, albeit wrongly so. Algorithms are often marketed as having mathematical objectivity and infallibility, a practice that legal scholar Elizabeth Joh (2017, 292) describes as 'math-washing' as it wrongly assumes 'that algorithmic models don't have subjectivity baked into them because they involve math'. As the Robodebt scandal demonstrates, algorithms have politics: they are always for someone and for some purpose. Its unstated purpose in targeting pay discrepancies was to make it more difficult for people to access welfare (see Mann 2020).

Automated decision-making programmes can present multiple risks, depending on the types of services and populations involved. Risks from automated decision-making, points out legal scholar Susan Morse (2019, 1510), range from the mundane but devastating at the individual level, such as denial of government benefits, to the macro-economic, including failure to recognize 'risks to bank capital on the eve of the global financial crisis'. When governments adopt automated tools, there may be little evaluation of their appropriateness or effectiveness. For example, a study of UK municipal authorities' use of automated tools in the areas of fraud prevention, health, child welfare, social services, and policing found there were no standard practices as to how data systems are implemented or audited (Dencik et al. 2018). Algorithms' statistical models are difficult for ordinary people to understand, a challenge further complicated as algorithms are typically protected as trade secrets. Evaluating how algorithms make decisions is challenging, as 'algorithms may generate and follow rules that are indiscernible to human observers', meaning that people 'may be unable to determine what factors are considered by an algorithm or how they are weighted' (Robertson et al. 2020, 35).

Governments use data-driven tools to measure and understand their populations with greater precision, and these tools can have benefits, such as enabling health agencies to track the spread of pandemics. A key problem, however, is that surveillance tools implemented for one reason, like a global pandemic, often become permanent features of surveillance and control. Once installed, digital infrastructure that facilitates surveillance and enables automated decision-making can be difficult to dismantle. In the case of criminal justice or social welfare systems, obsolescence was effectively embedded within paper files: material subject to decay and requiring offline (difficult to access) retention. In contrast, digital records can be cheaply stored and easily reviewed, meaning a criminal record or determination of risky behaviour 'can follow people perpetually' (Eubanks 2018, 187).

At the heart of discussions over the deployment of automated tools to determine people's eligibility for social assistance, child welfare protection or

immigration services are questions about the role of the private sector in shaping how public services should be offered and even the values that should be prioritized in government bureaucracy. Algorithms tend to function by ranking or scoring specific targeted behaviours, instead of understanding the complexity of people's motivations, actions or circumstances. Automated tools may prioritize efficiency, cost effectiveness and speed of service delivery over other important values, such as accountability and equity in treatment.

Chapter 5 examined how legitimacy and authority have been accorded to algorithms and automated processes. This chapter expands on those observations, highlighting how the knowledge and experience of frontline service workers risks being sidelined. For governments, the shift from human to increasingly automated decision-making often involves a sharp transition from face-to-face decision-making between government workers and the public – that is, 'street-level bureaucracy' – to a type of 'screen-level bureaucracy' (Bovens and Zouridis 2002, 177). The application of private-sector data tools and analytics to the public sector constrains, and even prevents, the decision-making capacity of some frontline staff (Eubanks 2018; Dencik et al. 2018). In some cases, this has had the effect of essentially substituting the experience and knowledge of public employees with privatized technological outputs designed and delivered by data scientists. In other words, data scientists' understanding of social issues like poverty or child endangerment is accorded greater legitimacy and authority than that of the public officials who deliver programmes.

CONCLUSION

This chapter has explored various ways that states govern by assuming dominant positions in the knowledge structure. Historically, states commonly gathered information on their populations, including through census data to achieve security and political goals, a practice that has contemporary relevance as states enlist telecommunications and technology companies to amass data on populations foreign and domestic. States govern through data, as demonstrated in examples like India's Aadhaar programme, China's social credit system and Australia's Robodebt programme. Despite common claims of 'authoritarian' technologies or surveillance, divisions between democratic and authoritarian states have blurred as there are broad similarities in how states undertake surveillance, as well as co-opt or coerce industry involvement (see, e.g., Glasius and Michaelsen 2018). Instead of viewing state data practices in an unhelpful authoritarian/democratic binary, this chapter argues that it is more productive to understand these practices as states' efforts to exert control via the knowledge structure.

As states govern through data, this puts private-sector actors who control valuable datasets in powerful positions as to the nature and extent of information that government officials and regulators can access. Access to industry data is vital to public regulators and planners at all levels of government whose work can be hampered, even obstructed, by data deficits. Data deficits are particularly evident in the gig economy, where companies view their valuable data as bargaining chips with which to strike favourable deals with public regulators or further companies' goals to enter the public sphere as regulators to serve their commercial interests (see Scassa 2017). Court battles and regulatory debates are laying bare what's at stake in the data economy, including the nature of work, who counts as an employee, the roles of public-sector versus private-sector actors, and what actors have the authority, legitimacy and capacity to govern.

More broadly, there are geopolitical and geo-economic implications to the battle over the knowledge structure, as is evident in the US-China trade and technology war (see, e.g., Segal 2021) and the European Union's regulatory standard-setting efforts. This contest amongst the great powers is not just a battle over technology but also a global battle over the control of knowledge. The European Union and China, the leading digital economic nationalists, are each aspiring to become knowledge feudalists to counter the United States. China's efforts are largely focused on becoming a technology superpower, such as through its Belt and Road Initiative, while the EU plans to become a regulatory superpower by setting rules and standards with extraterritorial applications like the GDPR (Bradford 2020). In contrast, it remains to be seen how smaller states will either align themselves with one of these big state actors or attempt to forge a different path, perhaps with a coalition of like-minded states. As chapter 9 will examine, smaller states may explore various digital economic nationalist strategies such as data sovereignty policies that mandate the storage and use of data according to domestic state laws. These strategies, however, generally aim to counter knowledge-feudalist states, such as through data-localization laws requiring data collected within a country be stored and governed within that state but do not seek to challenge fundamentally the information-imperium state.

NOTES

1. Though see chapters 1, 4, 5 and 6 on why such faith is often misplaced.
2. Recall, from chapter 2, that power in the security structure involves the power to provide or deny someone, or some group, security.
3. See Gillespie (2010) for a thorough discussion of the multifaceted meaning of 'platforms'.
4. Interview, Pedro Mizukami, Rio de Janeiro, 3 May 2018.

5. For a thorough critique of the political economy of fintech, see Allen (2022). See also the *Review of International Political Economy* special issue 'The Changing Technological Infrastructures of Global Finance' (Bernards and Campbell-Verduyn 2019).

6. Following swift criticism from regulators and lawmakers globally, Facebook in 2020 scaled back the project to assuage regulator concerns, renamed it Diem from Libra in December 2020 and delayed its launch until 2021. In January 2022, Facebook sold Diem to Silvergate Capital, a bank specializing in financial technologies. For an accessible, critical history of Libra, see journalist David Gerard's *Libra Shrugged: How Facebook Tried to Take Over the Money* (2020).

7. As the late 2002 implosion of the crypto bubble has ably demonstrated.

8. For the Canadian context with respect to slavery and policing, see Maynard (2017).

9. Available at https://uidai.gov.in/my-aadhaar/about-your-aadhaar/usage-of-aadhaar.html, accessed 25 April 2022.

10. Cambridge Analytica, a data analytics firm owned by hedge fund billionaire Robert Mercer and that worked with Donald Trump's election team, amassed data from millions of Facebook profiles of US voters and created software programmes to try to predict and influence voters' intentions. While the degree to which the company may have influenced the 2016 US presidential election is a matter of debate (see Gehl and Lawson 2022), the scandal sparked multiple investigations by governments and regulators worldwide, a public relations crisis for Facebook, and a public backlash against data firms' surveillance-based business models.

Chapter 9

Governing Data

The information-imperium state has emerged through a series of fundamental social, economic, political and technological shifts. Chapters 5 through 8 examined how these shifts are transforming the ways in which state and private actors understand, value and have incorporated data into their activities, and how this incorporation has reshaped the exercise of power. Reflecting upon those chapters, this chapter asks: Which actors have the legitimacy and authority to determine what types of data should be collected, the manner in which that data can be legitimately used and the appropriate modes of data governance? In short, who can and, more importantly, who *should* set the rules of data governance that are at the heart of structural power in the knowledge-driven society? Whose interests should be served by this regime, and how might they affect data governance?

The starting point for this chapter is the recognition that the information-imperium state is highly contested. As we've set out in the book, knowledge feudalism and digital economic nationalism are the two opposing economic strategies within the information-imperium state. The United States, the dominant knowledge-feudalist actor, prioritizes global flows of data and the maximalist protection for intellectual property rights, which largely benefit US industry. The United States also has economic, political and national security interests in ensuring the free flow of data globally, and its large data companies disproportionately benefit from capturing, interpreting and monetizing these data flows. As a counterpoint to knowledge feudalism, multiple states are undertaking various digital economic nationalist strategies, including policies that restrict or regulate global flows of data. These include policies that require data to be stored within a state's legal jurisdiction, a practice termed 'data sovereignty' that this chapter explores.

The European Union, the most prominent digital economic nationalist actor alongside China, capitalizes upon its large internal market and regulatory capacity to institute its own preferred rules on the data market. This chapter explores how the EU's General Data Protection Regulation (GDPR), widely perceived as a global data-protection standard, regulates but does not dismantle the problematic trade in personal data. We contend that the GDPR must be understood as part of the European Union's long-term strategy to become a global regulatory superpower, exporting its preferred data standards and practices to other countries and applying them to big data actors, including US companies like Apple and Facebook. In the terminology of this book, the European Union is aspiring to become a knowledge feudalist by setting rules for the market in personal data that are applied globally through the extraterritorial application of the GDPR.

In staunch opposition to an information-imperium state that accords economic, political and social power to the control over knowledge, there exists a collective rights approach that centres human rights within the knowledge structure. This approach encompasses an array of strategies and practices, and brings together a diverse coalition of workers, activists, civil-society groups, privacy experts and technologists, and Indigenous groups. While opposition takes many forms, common amongst them is resistance to the surveillance-intensive practices of governments and businesses, as well as pushback against dataist ideologies that privilege quantifying all aspects of human life and employ automated data techniques to augment or even replace human decision-making. A human rights approach tends to favour restrictions on the collection and use of personal data, particularly its commodification, and to support data-governance models that accord greater collective control rather than corporate models that focus on narrow commercial interests. In a rejection of the dataist imperative that all data must have value extracted to realize social and economic benefits, some actors within the human rights approach advocate for people to have the right to exit data markets, essentially opting out of corporate practices datafying all aspects of social life. In contrast to knowledge feudalism and digital economic nationalism, we term this approach 'data decommodification'.

Workers and citizens, for example, are engaging in protests against surveillance-focused business models that exist to monetize data. Such efforts are particularly evident in the exploitative gig economy, where workers have sued gig companies to be recognized as employees and engaged in strikes and other collective labour action (Woodcock and Graham 2020). Resistance is also evident against the intensification of state security–related surveillance programmes (e.g., Stevens and Allen-Robertson 2021), as well as protests and lawsuits against state use of automated tools to manage and deliver public services like welfare (Vervloesem 2020).

While contestation can be seen at the state level, it is also present within the knowledge-driven society itself. This contestation is focused not just on the ability to reap the spoils of the knowledge-driven society, but on the meaning of fundamental terms, like privacy. While this book has explored the tendencies, or imperatives, of the information-imperium state toward pervasive surveillance and knowledge commodification in pursuit of improved security and boosting economic growth, data and knowledge governance remain contested topics, including both their meaning and their limits.

This chapter reflects upon the contested state of data governance. Alongside efforts to scale back corporate and state surveillance measures, scholars and activists are developing concepts that emphasize collective approaches in the treatment of data and human rights more broadly to counter the hegemony of the information-imperium state. Collective data-governance approaches – data justice, group privacy and Indigenous data sovereignty – emphasize governance by and benefits accruing to a collective in contrast to legal frameworks focused on individual control and individual rights, while also generally pushing back against the commodification of data.

This chapter proceeds in four sections. First, it argues for the need for a critical rethinking of individualized notions of privacy and consent. As part of this consideration, we explore how the EU's GDPR functions not only as a regulation to standardize the treatment of personal data across Europe but also as part of the EU's efforts to shape regulations globally that prioritize its own particular economic and social interests, which may not align with the interests and needs of others. The chapter argues that we need alternative human rights approaches to privacy and to data governance more broadly to counter the problems inherent in the data economy, principally pervasive surveillance, discriminatory data practices and vast gulfs between those accumulating power through knowledge and those without such power.

Second, the chapter examines forms of resistance to the information-imperium state by considering various collective models of data governance, including data trusts and data sovereignty approaches, particularly Indigenous data sovereignty. Third, the chapter considers the concepts of group privacy and data justice as human rights-centred alternatives to the problems of an increasingly datafied society and economy. The chapter ends with a brief conclusion.

RETHINKING PRIVACY AND CONSENT

Understandings of privacy are neither unchanging nor universal. Underlying the global data economy is the Western individual-focused understanding

of privacy that draws from the Anglo-Saxon legal tradition. Privacy is understood to be an individual right similar to other individualized notions of human rights (Taylor et al. 2017b). This individualized conception of privacy is evident in companies' legal terms-of-service agreements, which require all users to signal their consent (say, by clicking 'I agree' on a website) before being able to access digital products and services. As explained in chapter 4, understanding privacy as attached to individuals has been the dominant view since the late 1990s, exported globally from the United States through its tech companies via the so-called notice-and-consent model of privacy policies (Cranor 2012, 304), a practice that has enabled the United States to become a knowledge-feudalist state. This model of privacy assumes that people are capable of acting as rational consumers who read and understand the policies (notice) and then give informed consent (choice) (Cranor 2012). The model, which provides the legal underpinning of the digital economy, problematically assumes that privacy can be straightforwardly understood as applying to the collection and use of personally identifiable information.

Understanding Privacy and Consent

Privacy is a more complex and intangible concept than is generally acknowledged. 'There is no overarching conception of privacy', explains privacy scholar Daniel Solove (2008, x): 'it must be mapped like terrain, by painstakingly studying the landscape'. A perennial challenge with privacy is that it is 'an unusually slippery concept' (Whitman 2004, 1153), as what is considered to be 'private', such as public nudity, varies widely among societies and over time, as do state regulatory frameworks and private-sector data practices. There are gender, race and class dimensions to how people experience privacy, dependent upon their status and circumstances. Historically, institutionalized populations, including prisoners, and noncitizens, immigrants, children, people with disabilities, and racial and sexual minorities have been disproportionately subjected to intensive bureaucratic surveillance, a trend that continues today (see Igo 2018). Similarly, women and sexual minorities traditionally were presumed to have a lesser claim on privacy than heterosexual men (Igo 2018, 9). Concerns about state and corporate limitations on and violation of individual and groups' privacy are nothing new, as historian Sarah Igo (2018) explores in her historical study of shifts in public understandings of privacy in the United States following the US government's introduction of its social insurance programme that provides retirement benefits. While many studies traditionally focused on privacy rights in relation to governmental practices, privacy in relation to private-sector activities has become an increasingly important topic (for an early influential text, see Gandy 1993).

Consent, like privacy, is a more complicated concept than it may first appear. Key to understanding consent is the idea of informed consent. Generally, consent is seen as valid only when people can understand to what they are consenting and are given clear options to accept or decline the data collection, use or disclosure (see e.g., Hoofnagle 2018). The EU's GDPR, for example, defines 'informed' consent as a 'freely given, specific, informed and unambiguous indication' or 'a clear affirmative action' (European Parliament 2016 GDPR Art. 4(11)). In some cases, however, there may be no way to opt out, if the data collection is attached to critical services like transit or when data collection is tied to locations in a smart city.

Recognizing that most people do not read terms-of-service agreements, legal scholar Teresa Scassa (2018a) argues that 'clicking "I agree" without reading privacy policies is an act of surrender, not of consent'. Communication scholar Jonathan Obar (2015, 2) concludes that this situation reflects 'the fallacy of data privacy self-management', in reference to the misconception that people can understand and provide informed consent in this area. Companies' practice of unilaterally changing the terms of the agreements without notice to the user can result in 'shadow terms', which consumers may not know about (Horton 2010). People cannot consent to future uses of their data of which they are unaware, and it is nearly impossible for ordinary people to calculate a fair or reasonable exchange of services for personal data. Implicit within the model of informed consent is the idea that consumers can decline contracts with onerous conditions, if they are aware of them, or they can switch to providers with more favourable conditions. Switching providers, however, can impose costs, assuming that there are even viable alternatives. This, unfortunately, is not the case in many parts of the winner-take-most data-driven economy. Social media companies, for example, almost all operate with similar surveillance-based business models, while it is difficult to find non-smart versions of many consumer goods like televisions.

The lack of informed consent in terms-of-service contracts can lead to negative outcomes for users. Contracts may, for instance, 'restructure the rights of users' or, even more worrisome, 'delete rights that are granted through democratic processes, substituting for them the system that the firm wishes to impose' (Radin 2012, 16). This problem can be evident in contracts deployed internationally by globally dominant companies with little regard for the distinctive nature of domestic legal systems. Legal wording that may have been drafted to respond to the needs, ideologies and requirements of one jurisdiction (usually the United States) ends up being exported to other jurisdictions, like Australia, to the extent of reproducing 'verbatim the contractual wording of the original US source' even though the language may not be suitable (Noto La Diega and Walden 2016, 3). As a result, legal contracts attached to digital services or software-enabled products are 'commonly'

used within Australian contracts even when not particularly suitable (Manwaring 2017, 286). This cookie-cutter approach, discussed in chapter 7 in relation to agricultural data, has the effect that consumers, typically those in smaller countries, are subject to rules set in another country. These practices of rule exportation raise classic questions of regulatory scope and legitimacy: Whose rules and where?

The GDPR: Not a Privacy 'Gold Standard'

Given the challenges outlined earlier with how we understand privacy and consent-based data collection, solutions can be difficult to articulate. A common – and understandable – reaction to the ills of the data-driven economy is a call for new or strengthened data-protection laws, including tougher privacy measures. For many privacy scholars and privacy-focused policymakers, the EU's General Data Protection Regulation (GDPR), which came into force in May 2018, offered a groundbreaking development in terms of privacy protection. The GDPR does more than just enact data-protection and privacy rules on the personal data across the European Union. Crucially, it is designed to regulate, not impede, the trade in personal data (Daly 2021), while also enabling the European Union to exert global structural power by setting global standards for the online treatment of personal data (Bradford 2020). In its attempt to set global standards for the data market, the European Union is endeavouring to become a knowledge-feudalist state.

Advocates of the GDPR claim it constitutes 'a sort of digital gold standard' and 'the most ambitious endeavour so far to secure the rights of the individual in the digital realm for a generation' (Buttarelli 2016, 78, 77). The GDPR harmonizes privacy laws throughout the European Union in relation to the collection and processing of EU residents' personal data, which includes mining, aggregating and sharing data. It applies to entities, whether in the European Union or outside, that collect data from EU residents in relation to offering goods or services to Europeans or monitoring their behaviour. Amongst its key provisions, the GDPR sets out a stricter definition of consent and new rights for individuals to access their data. With some exceptions, EU residents can erase their data, restrict the processing of personal data and have the right to data portability, which means that people can transfer their personal data from one entity to another.[1]

Following the introduction of the GDPR, multiple countries have adopted or are in the process of introducing data-protection laws. Brazil, long considered a leader in digital rights following the passage of its *Marco Civil da Internet* (Bill of Rights for the Internet) in 2014, introduced its *General Personal Data Protection Law* (LGPD) in 2018 and created a National Data

Protection Authority (ANPD) in 2020. Although the United States lacks GDPR-like provisions at the federal level, California passed its 2018 *Consumer Privacy Act*. Countries in Africa, Asia and Latin America have adopted GDPR-like data provisions, in part to ensure continued access to the European Union's market (Bradford 2020). While each of these state efforts can be understood as digital economic nationalist responses, that these laws are intended to complement the GDPR to enable access to the European market demonstrates the regulatory power of the European Union.

Although the GDPR is rightly praised for establishing a baseline of data protection, it should not be understood as a bulwark against the pervasive surveillance characteristic of the digital economy. The GDPR was designed to facilitate data collection and streamline digital capitalism across the European market, particularly in terms of the trade in personal data. After all, the European Union, like other states and regions, needs a functioning data economy, and there is an additional need in Europe for consistency in the treatment of personal data across EU Member States. The GDPR is a digital economic nationalist response that endeavours to balance principles of freedom, security and economic development according to European preferences in contrast to the free-market orientation of the United States.

Legal scholar Angela Daly (2021, 88) contends that the GDPR is 'ultimately permissive of various surveillance capitalist data gathering and processing practices' as it sets out rules for the datafication of personal data. This is because the GDPR facilitates 'the free flow of personal data between Member States' (Article 3). The effect, Daly argues, is that instead of countering surveillance capitalism, the GDPR is effectively establishing a 'surveillance capitalist Internet with European characteristics' with those characteristics being stronger data-protection compliance and oversight than elsewhere (Daly 2021, 92–93). In essence, the GDPR has a dual aim as a digital economic nationalist strategy: it establishes important data-protection standards for all EU residents and ensures the free flow of personal data throughout the European Economic Area.

Consequently, the GDPR regulates the digital economy but does little to curb the trade in personal data. More broadly, the GDPR enables the European Union to reach its long-standing ambition of becoming a regulatory superpower on the global stage in two ways. First, the GDPR applies extraterritorially to govern non-European actors that collect data on EU residents (like a Canadian company selling products to Europeans). Second, other countries are adopting provisions similar to the GDPR to be able to continue trading with the European Union. This is why the GDPR functions as more than a data-protection law: it is a key part of the European Union's long-standing effort to establish itself as a regulatory superpower.

EU as Regulatory Superpower

The EU's GDPR is more than just an EU law. It is an example of the 'Brussels Effect' that we discussed in chapter 8, the European Commission's practice of strategically exporting its preferred standards globally (Bradford 2020). The GDPR has a similar extraterritorial application, requiring all companies serving EU residents, even those located outside Europe, to institute GDPR rules in the treatment of personal data. Companies and states outside the European Union thus have a strong interest in implementing the GDPR into their business operations or instituting EU-style provisions into state law to continue doing business with EU residents. Bradford (2020) further notes that countries across Africa, Asia and Latin America have emulated EU data-protection standards, while US-based multinational technology companies like Apple have expanded GDPR policies to users outside the European Union.

Through these developments, the GDPR has become a de facto global privacy standard, a development that positions the European Union to become a knowledge feudalist capable of structuring the global data market to preference its economic, social and political interests. According to the United Nations Conference on Trade and Development (UNCTAD), 'Out of 120 countries outside the European Union, 67 have adopted a GDPR-like law' (UNCTAD 2021, 136). Some may view the GDPR's spread as an unqualified good, particularly for regions without data protection laws. Others, however, have critiqued this development, arguing that it may create a 'privacy universalism' that transplants a Western, specifically European, conception of privacy that results in the 'flattening of privacy values across cultures and contexts' (Arora 2019, 718). In line with traditional Western legal conceptions of privacy, the GDPR frames privacy in terms of individual choice and assumes a degree of digital literacy, which, as digital anthropologist Payal Arora (2019, 718) argues, may not be appropriate for regions that 'may perceive, experience, and value privacy in unpredictable and varied ways'.

The extraterritorial application of standards to countries that may not choose to be governed by EU-style rules and do not participate in either the making of the law or its implementation can be understood as existing within a 'neocolonial' relationship, in which 'laws and regulations . . . are not necessarily designed and executed for the protection of all citizens' (Arora 2019, 718). That the GDPR represents an imperial approach to global standard setting is sometimes not always fully appreciated by Europeans, as we learned first-hand at a pre-pandemic data and internet governance conference in Germany, to which we had been invited as presenters. During a conversation about the merits of the GDPR, a European scholar mentioned that the GDPR was designed to situate the European Union as a global privacy standard

setter, with those European standards intended to benefit other countries, through their adoption of these standards. We were asked what we, as Canadians, thought of the GDPR. One of us replied that we appreciated the GDPR as a thoughtful and pioneering attempt to address fundamental human rights within a commercial context. However, we said we also felt an undercurrent of resentment borne of the fact that it was designed to institute and enforce European values and rules onto other populations without us having a say, since countries and companies effectively had adopted GDPR-compliant provisions in legislation or terms-of-service agreements as the price for accessing the European market. We saw the GDPR, in other words, as a type of neocolonialism: legislation imposed upon the world without most of the world having a say in the process.

Our German hosts were, perhaps understandably, dismayed by our reaction, especially by our use of the term 'neocolonialism'. Our colleagues countered that the European Union has good intentions in designing rules intended to spread European values globally. This is undoubtedly true. However, good intentions are often in the eye of the beholder, and claiming that you have the best intentions does nothing to address fundamental issues of democratic accountability. When we asked how smaller countries might create data-governance models responsive to their specific needs and values, we were told smaller countries could choose amongst several models: a free-market US style, an authoritarian Chinese model or the EU's GDPR. Apparently, self-determination wasn't on the menu.

It would be naïve, moreover, to assume that the extension of regulatory frameworks originating in the United States, European Union or China – the three dominant digital powers – is driven purely by humanitarian concerns. As a 2021 UNCTAD report on the digital economy notes, while 'these expansion strategies towards developing countries may allegedly be grounded in international cooperation, humanitarian or development-oriented motivations, there seems to be motivation for extracting data from those countries to create value from their processing'. The UNCTAD report goes on to state:

> Thus, there is an extractive logic in these expansion strategies, which is similar to the experiences of developing countries that have specialized in natural resources production; it would result in an unequal exchange, as countries that provide raw data become highly dependent on those that extract and control them, making them flow out to foreign countries. The latter have the technological capacity to capture the value of data by converting them into digital intelligence. However, developing countries would need to pay for the imports of those data products, which could support their development, created in part on the basis of raw data originally generated domestically. (UNCTAD 2021, 112)

Concern about this type of imperial overreach is not limited to the world outside Europe. At the German conference, a participant from a smaller European country approached us privately to say that they agreed with our concerns, but did not feel comfortable saying so publicly.

Alongside the democratic issues with this type of transplantation of laws and norms designed for one jurisdiction (typically the Global North), countries looking to implement privacy-protection laws face other hurdles. The GDPR, after all, was developed in a relatively institutionally robust political and legal system, while other countries' situations may involve 'fragile institutions' and 'an overburdened and often weak legal system' (Arora 2019, 720). Simply passing laws and granting states greater power, in other words, will not necessarily address rights violations, especially if the actors responsible are located outside the jurisdiction in question, if the laws themselves are difficult to challenge or if national governments see greater economic or political value in facilitating, not countering, privacy-violating behaviour, such as to surveil their citizens to safeguard political stability.

The European Union is not alone in its knowledge-feudalist ambitions in setting standards to govern global flows of data. The United States, as a technological superpower and leading knowledge-feudalist state, is pursuing a similar strategy (UNCTAD 2021, 111–12). As discussed in chapter 8, the United States, Canada, South Korea, the Philippines, Singapore and Taiwan announced the creation of a Global Cross Border Privacy Rules (CBPR) System in April 2022 to govern cross-border data flows (United States Department of Commerce 2022). Both the GDPR and the CBPR approach to cross-border data flows are designed to structure the trade in data. However, as lawyer Andrei Gribakov notes, the two systems 'represent competing views on the trade-offs between privacy and economic growth', with the GDPR focused more on human rights and the CBPR rooted more in the 'desire to increase information flows and trade' (Gribakov 2019).

China, for its part, also has plans to expand its technological dominance outside the country, in part through its Belt and Road Initiative designed to enlarge the reach of the Chinese tech industry. Alongside the Belt and Road Initiative, building on efforts begun in the early 2000s, China enacted a data-protection law in 2021, the Personal Information Protection Law (PIPL) (Creemers 2022).[2] The PIPL bears a resemblance to other data-protection laws worldwide and, like the GDPR, it has extraterritorial elements, which means its provisions may apply to entities providing services to or conducting analysis of individuals on Chinese territory (Creemers 2022, 6). Like the United States and European Union, China's data policies are designed, in part, to expand its influence globally and to facilitate economic growth domestically. Paired with strategies like the Belt and Road Initiative, China's data policies may enable it to 'gain influence among third countries grappling with similar issues' (Creemers 2022, 9).

How the battle over data-protection standards will play out amongst the European Union, China and APEC's CBPR multilateral effort is yet to be determined (on the data-governance battle amongst China, the United States and the EU, see Carr and Llanos 2022). However, as political scientist Daniel Drezner notes, the lack of a consensus in this area amongst competing global actors reduces the likelihood of a single global regime (Drezner 2005).

ALTERNATIVE APPROACHES TO DATA GOVERNANCE

Rules setting out who can access, own and benefit from data are vitally important because, as argued throughout this book, power accrues to those who control data. How these rules are set and the resulting distribution of benefits involve questions of and negotiations over structural power, creating winners and losers. In this section we highlight collective approaches to data governance, which are attempts to deliver widely shared benefits while addressing key challenges in a knowledge-driven society, particularly pervasive surveillance and global asymmetries in the capture and control of data flows.

Collective approaches to data governance include a broad range of policies such as data cooperatives, data trusts and data sovereignty practices. These approaches vary widely in structure, purpose and degree of legal formality. Common amongst many of these approaches is a shift away from a focus on the individual to benefits accrued to or control undertaken by a collective, whether at the level of a domestic state, Indigenous nation or group of like-minded people. Benefits or control may not be shared equally or fairly amongst the population, nor are these approaches necessarily democratic in governance.

Knowledge-feudalist patterns of data extraction and commodification that disproportionately benefit a handful of Global North actors are generating a countervailing interest amongst national governments and citizens in asserting control over their data locally. The importance of understanding local contexts, conditions and populations of those providing the data aligns with the argument of Science and Technology Studies scholar Yanni Alexander Loukissas (2019, 23), who remarks that this necessitates 'forming close relationships with not only data but the conditions in which those data are manifest'. This can entail, for example, appreciating the distinctiveness of data because of its geographical, linguistic and cultural contexts. Preferences for local control over data, that is, at the national or subnational levels, can also be a political and security response for states concerned about foreign influences over technology, in what is often termed data or digital sovereignty (Musiani 2022). Such practices at the domestic level, whether in data

governance or policies to stimulate innovation like patent pools, are characteristic of digital economic nationalism.

Discussions about data governance tend to privilege state interests, especially when the term 'sovereignty' comes into play. However, there exist several alternative approaches to data governance, explored further next, that are premised upon the idea that data is a public good and those providing the personal data 'should have some say in what data is collected, how it is used and who benefits' (Dencik and Sanchez-Monedero 2022, 6). These include Indigenous data sovereignty, which challenges the structural power of the settler/colonial state – and, increasingly, of companies – in terms of deciding who legitimates and controls knowledge. Elsewhere, data cooperatives and trusts generally recognize that social or economic value accorded to data generally rises when data is aggregated, meaning an individual's personal data is typically not worth much on its own (Srnicek 2017), but collective actions can help people gain greater benefits than any individual could alone. Each perspective presents a different approach to how power in the knowledge structure is used, by whom and to what ends.

State Data Sovereignty and Data Localization

The role of states in regulating data has become increasingly contentious in recent years, an object of interest for democratic and authoritarian governments alike (see Haggart et al. 2021). The concept of state control of data goes by many different names – digital sovereignty, technological sovereignty, internet sovereignty or data sovereignty (see, e.g., Couture and Toupin 2019; Hummel et al. 2021). All of these terms share a general outlook, a belief central to digital economic nationalism, that states should affirm their authority over 'the Internet and the broader digital ecosystem, to protect their citizens, institutions, and businesses from the multiple challenges to their nation's self-determination in the digital sphere' (Musiani 2022, 1). Data sovereignty (we use this term for simplicity's sake) involves at its heart the issue of control: 'It depends on locally owned, controlled and operated innovation ecosystems, able to increase states' technical and economic independence and autonomy' (Musiani 2022, 2).

The concept of data sovereignty is often associated with authoritarian regimes, especially China and Russia, as both states have linked data sovereignty to broader geopolitical goals of strengthening their political standing globally (Budnitsky and Jia 2018). Both states, for example, have instituted a series of digital economic nationalist measures to extend state control over the operation of domestic and foreign technology companies within their jurisdiction, stimulate their domestic technologies industries and regulate data flows domestically (for Russia, see Stadnik 2021; for China,

see Jia 2021, and Luo and Lv 2021). States cannot enact such measures alone (see discussion in chapter 8), but rely upon cooperation, sometimes coercively obtained, from the private sector. Even authoritarian states face limits to their capacity for data sovereignty. Russia lacks the capacity to compel compliance from foreign tech companies in comparison to its ability to extract cooperation from its domestic industry to comply with the Russian government's efforts to regulate online content (Stadnik 2021). China, in contrast, is characterized by relatively less reliance upon foreign companies, as it has nurtured a strong domestic technology sector that the government partners with to operate its systems of online surveillance and censorship, including the Great Firewall that blocks prohibited foreign content and applications (Jia 2021).

The push towards state data sovereignty is not just coming from authoritarian countries. Policymakers around the world are increasingly focusing on 'the ability of a country to make its own decisions on data and data flows – their data sovereignty' (UNCTAD 2021, 60). Among democratic countries, the Snowden revelations about the global surveillance programmes of the US National Security Agency and its allies led many countries, including Germany and Brazil, to consider data localization policies to thwart monitoring by the US government and limit US companies' data practices (Hill 2014). Repercussions from the US knowledge-feudalist position, in this case its security ambitions, stimulated other countries' interest in digital sovereignty.

Data Localization

Data localization – the requirement that data produced or extracted from an area remain in and under the control of that jurisdiction (Sargsyan 2016) – is a key element of data sovereignty. Estonia, for example, uses data localization to protect its data sovereignty. It is often referred to as a 'digital republic' because of the country's embrace of digitization in all realms of life, including voting, taxes and the storage of all citizens' health, tax and personal records online (Heller 2017). Estonia established the first 'data embassy' in Luxembourg in 2019, a digital economic nationalist strategy intended to safeguard its data from cyberattacks, especially by Russia (Samsel 2019). Estonia's agreement with Luxembourg gives Estonia full jurisdiction over the servers holding sensitive data: Monaco is planning a similar data embassy in Luxembourg (Samsel 2019).

Sidewalk Labs' Quayside project, for its part, introduced many people in Canada to the concepts of data sovereignty and data localization. The benefits and drawbacks of the practice of data localization remain hotly debated. Opponents of data localization – and, by extension, supporters of free cross-border data flows, especially the knowledge-feudalist United States – argue

that data localization can reduce economic efficiency and increase the cost of doing business, while not necessarily contributing to data security (UNCTAD 2021, 50, 56). Differing regulatory frameworks across jurisdictions, for instance, can interrupt the 'global supply chain for data' by impeding 'the benefits of sharing data or making it available to researchers, developers, and innovators' (Carr and Llanos 2022, 288). Supporters of data localization, in turn, highlight that cross-border data flows tend to privilege primarily those economic powers based overwhelmingly in the Global North, particularly the United States (UNCTAD 2021, 56).

Locating data outside of the jurisdiction in which it was created can also present accountability challenges. For example, it may place data beyond the reach of domestic law enforcement. That countries have different privacy-protection standards means that data captured from the residents of one country may end up being regulated by the laws of another country, laws that they had no role in defining.[3]

During Sidewalk Labs' public consultation, key points of contention were not only how data would be governed and where it might be stored but also how the economic benefits from smart-city data might be shared amongst the local tech industry (McBride 2018). Reflecting digital economic nationalist concerns, critics questioned how governmental bodies in Canada could reclaim that data, once transferred, 'should future voters decide that this is appropriate for security or other reasons', or what would prevent the commercialization of intellectual property related to that data in ways not in the public interest once it was outside of Canada (Banks 2018).

In response to critics' concerns, Sidewalk Labs agreed to use 'its best efforts at data localization, as long as there are Canadian-based providers who offer appropriate levels of security, redundancy, and reliability' (Sidewalk Labs 2019c, 460). Sidewalk Labs' 'best efforts' may have been as much as could be obtained in the project, as some experts pointed out that mandating foreign private actors to retain their collected data in Canada could constitute a violation of the country's United States-Mexico-Canada trade agreement (USMCA). This agreement, in keeping with the knowledge-feudalist governance approach, which favours free and open cross-border data flows, bans data localization except in certain circumstances (Gribakov 2019).

The importance to the United States, the leading knowledge-feudalist state, of encouraging cross-border data flows and restricting data localization can be gleaned from comments in October 2021 by Christopher Hoff, US deputy assistant secretary for services in the US Department of Commerce. When asked what the United States' 'offensive strategy' was with respect to global privacy policy, Hoff listed three priorities: 'Tracking and combating data localization, in any form; Prioritizing direct bilateral negotiations with jurisdictions around the world; [and] Supporting the globalization and

expansion of the Asia Pacific Economic Cooperation Cross-Border Privacy Rules [CBPR] system' (Zweifel-Keeegan 2021; see also UNCTAD 2021, 152). On this point, it's also worth noting that the USMCA commits the three member countries not only to restricting data localization but to the APEC CBPR. This combination highlights how 'regional, bilateral and transnational trade agreements have become increasingly important instruments' not only to regulate intellectual property (see chapter 3) but also to address 'issues related to cross-border data flows' (UNCTAD 2021, 151). In both cases – data and IP – the objective is the same and reflects a knowledge-feudalist logic of maximizing cross-border exchange of commodified knowledge, with benefits accruing primarily to those actors already possessing economically valuable knowledge.

In contrast to the United States, the European Union's actions on data localization are more ambivalent and in keeping with a digital economic nationalist approach to knowledge regulation. While it formally supports free cross-border data flows, UNCTAD argues that the GDPR does not make it easy for such flows to occur, while recent privacy-related developments 'may suggest that the European Union is shifting its position on data localization' (UNCTAD 2021, 107).

Even facing such geopolitical headwinds, safeguarding data within a specific jurisdiction is not a silver bullet against abuse or domination. Depending on how data localization rules are implemented, they could restrict the ways that globally operating data companies could collect, use and store personal data from people within the jurisdiction in question. But such rules alone do not prevent problematic surveillance practices from occurring; they merely mandate that such data be housed in a specific jurisdiction. In fact, data localization policies could intensify state surveillance programmes by providing ready access to valuable caches of personal data (Sargsyan 2016).

Indigenous Data Sovereignty

In debates of data governance, states and large businesses are often perceived to be the dominant actors. The concept of Indigenous data sovereignty, however, offers a counter to governments, companies and academics, operating within an information-imperium state that seeks to appropriate and profit from data derived from Indigenous peoples, lands and cultures. There is a long, bloody history of government and industry researchers appropriating Indigenous knowledge and cultural property, and placing bodies for sale or on display in museums (Tuhiwai-Smith 1999) and disregarding cultural taboos by publicizing or profiting from cultural information, such as patenting traditional remedies for commercial gain (First Nations Information Governance Centre [FNIGC] 2016). Academics, too, have exploited Indigenous

knowledge for gain, often drawing inaccurate, discriminatory conclusions that have detrimentally shaped government policy towards Indigenous peoples (Walter and Carroll 2020).

Indigenous data sovereignty recognizes the fundamental point that control over the legitimation, creation, dissemination and use of knowledge is a fundamental expression of structural power. It sets out principles respecting Indigenous peoples' control over the collection, usage, storage and governance of data, placing it under the control and ownership of the Indigenous groups who created or generated the data/knowledge (Kukutai and Taylor 2016; Walter et al. 2020). Indigenous data sovereignty not only complements digital economic nationalist ideas of domestic control over data but also extends far beyond economic policies, as Indigenous data sovereignty is also a sociocultural and political response to centuries of colonialism and discriminatory state (and non-state) practices. Data sovereignty emerges from Indigenous peoples' inherent rights of self-determination and jurisdictional authority to enact laws and governance processes to create and deliver programmes, services and capacities within Indigenous communities (First Nations Information Governance Centre [FNIGC] 2016, 142). Indigenous data sovereignty movements exist in Australia, Canada, New Zealand and the United States, with efforts also underway in regions such as Southeast Asia, South America and Africa (see Walter and Carroll 2020).

Indigenous perspectives, in contrast to individualized notions of privacy and data governance, generally take a more collectivist approach to data use and control, as demographer Tahu Kukutai and population geographer John Taylor (2016) set out in their noteworthy edited volume, *Indigenous Data Sovereignty: Toward an Agenda*. Indigenous worldviews, for example, may require community or group consent for research to occur (Sherwood and Anthony 2020).

Indigenous research practices also tend to emphasize the importance of collective benefits from data collection (Sherwood and Anthony 2020). Sociologist Maggie Walter and public health researcher Stephanie Russo Carroll explain that Indigenous data sovereignty 'inverts the standard Indigenous data/policy nexus' in which the central question is not what data the state needs to deal with problems in Indigenous communities, but 'what data are needed to meet the needs, priorities and aspirations of Indigenous Peoples?' (2020, 14–15). This perspective shifts our view from a techno-solutionist framing (how can data/technology address this problem) to a more humanist framing (what problem do we want to address).

Reflecting upon collective data governance necessitates critically examining taken-for-granted ideas embedded within the digital economy, such as individualized approaches to privacy and consent. Taking collective approaches seriously entails understanding how this worldview may complement – or,

importantly, conflict – with other data-governance perspectives. Open data, for example, represents a popular policy solution to numerous challenges posed by a data-driven society. Open data is data that is openly accessible and usable, even for commercial purposes. The concept also includes 'government data that are usually provided for free' with 'few, if any, restrictions on reuse' (Janssen et al. 2012, cited in Scassa and Robinson 2022, 1). The push to make more government data available as open data responds to concerns that governments collect and control significant data that are beyond the reach of non-state actors. Open data proponents argue that making this data available can strengthen government transparency and accountability, while also stimulating innovation (see Robinson and Scassa 2022). Implicit in the open data perspective is a preference for free data flows (Robinson and Scassa 2022), driven by the idea – which also underlies the intellectual property regime – that the primary goal of a knowledge regime is to maximize access to and dissemination of knowledge.

An open data policy that privileges free flows of information, however, may conflict fundamentally with Indigenous data sovereignty principles, when the government data pertains to Indigenous peoples, lands and cultural knowledge. As critical data studies scholar Tracey Lauriault (2022, 25) points out, open data approaches generally overlook historical contexts and power differences amongst the entities sharing data, thereby creating tensions for Indigenous peoples who are asserting greater control over the use of their data and knowledge. In contrast to an open data perspective, decisions reflecting an Indigenous data sovereignty perspective may require restricting non-community members' access to or limiting specific cultural knowledge to insiders. Indigenous peoples in Canada, for example, are repatriating sensitive cultural objects ranging from ceremonial pipes, feathered headdresses, totem poles and pottery, to human remains from museums to their rightful Indigenous owners. Some objects are so sensitive, however, that if outsiders view them, it violates the spirit of the objects (Bernstien 2021). Contrasting questions of Indigenous data sovereignty with an open data perspective highlights a point we made in chapter 1, that the primary knowledge governance issues are related to questions of control. Considering the role and treatment of sacred art offers us a needed reminder that taking an unreflective open data perspective (or perspective on the use of intellectual property to encourage innovation or protect knowledge) involves assuming a consensus on policy objectives that may not exist between Indigenous and non-Indigenous groups or amongst countries.

Data Cooperatives

Control over data has emerged as a flashpoint in the information-imperium state, as workers struggle to assert greater control over their working

conditions, including collection of their data. Without access to data, gig workers know little of their working or payment conditions, how tasks are allocated or why they are disciplined or fired, while the data company controls such data for its commercial benefit. Gig workers, for example, have taken to court the ride-hailing companies Uber, Lyft and DiDi Chuxing, along with food delivery firms like Instacart, Doordash, Deliveroo and UberEats in the United States, Canada, across Europe and South Africa (Allsup et al. 2022). In these suits, workers claim that platform companies' tight control of working conditions and use of algorithmic decision-making practices means that workers are employees, not independent freelancers.

One response to gig workers' battle for access to and control over their data has been the formation of data cooperatives, similar to the long-standing cooperatives in housing and banking. Data cooperatives are groups that form around perceived collective interests in sharing and using data with individuals who want to voluntarily pool data resources (Ada Lovelace Institute 2021, 49). The Barcelona-based Salus Coop, for example, is a non-profit, citizen-driven data cooperative founded in 2017 that manages its members' health data in part by providing anonymized data for health research and for use by non-profit institutions that openly share their research results (Salus Coop n.d.).

Platform cooperatives are democratically governed and collectively owned (Scholz 2017) and, for the gig economy, are intended to provide gig workers better wages and fairer working environments (see also Woodcock and Graham 2020; Scholz and Schneider 2017). A wide variety of platform cooperatives have emerged, including Fairbnb, an accommodation alternative to Airbnb that invests proceeds in communities; Resonate, a music-streaming app owned by musicians, labels and fans; and RWASHOCCO, a Rwandan collective of coffee farmers. Driver collectives have also emerged, such as the Yatri app, which, as a taxi aggregator, represents over a thousand drivers in Kochi, India (Prabhakaran 2022).

Platform cooperatives face a difficult challenge countering gig companies' network effects as, in contrast to local cooperatives, companies like Airbnb and Uber are widely known and omnipresent in the marketplace. In contrast to the small funds of platform cooperatives, gig companies have amassed significant venture capitalist funding that enables the companies to offer artificially low prices to customers that the cooperatives cannot match, which, in turn, drives down worker pay (Scholz 2017).

Data Trusts

Similar to the concept of data cooperatives, data trusts are a type of collective data governance in which benefits from data are shared amongst people

who provide the personal data (Dencik and Sanchez-Monedero 2022). A data trusts, according to the London, UK-based Open Data Institute, is 'a legal structure that provides independent stewardship of data for the benefit of a group of organisations or people' (Hardinges 2018). Central to the concept of a data trust are a defined decision-making process, description of shared benefits, articulated rights and duties over stewarded data, and an independent intermediary between data collectors and those providing data, often termed 'data subjects' (Delacroix and Lawrence 2019).

Sidewalk Labs proposed a data trust to approve and oversee all data collection in the smart-city project area in Toronto (Sidewalk Labs 2019c, 383). At the time, most policymakers and the public had little familiarity with the concept. This trust, which the company envisioned as being guided by a charter, was intended to assuage public concerns over privacy and ensure data collection and use that 'spurs innovation and investment' (Sidewalk Labs 2018, 13). Problematically, argued data trust expert Sean McDonald, Sidewalk Labs was 'openly vague' about how its data trust would be structured or operate, meaning it would be challenging for anyone 'to understand the potential for credible privacy and data governance' (McDonald 2019, 2).

Depending upon how they are designed, data trusts may offer the distribution of monetary benefits, the collective power over data and independent, even public, oversight by data stewards of data access, use, storage and benefits. The London, UK-based Ada Lovelace Institute contends that the 'unique characteristic of data trusts' is that the institutional safeguards provided by trust law, at least in the context of the United Kingdom, may achieve the aim of balancing 'asymmetries between those who have less power and are more vulnerable (individuals or data subjects) and those who are in a more favoured position (organisations or data controllers)' (Ada Lovelace Institute 2021, 24). However, as Sidewalk Labs discovered, 'simply calling a data trust a "trust", or indeed any other data access architecture "trustworthy", is not sufficient', remarked Professor Dame Wendy Hall, chair of the Legal Mechanisms for Data Stewardship working group, in her foreword to the Ada Lovelace Institute report on data trusts (2021, 8).

As Sidewalk Labs learned via the Quayside project, data trusts are more complex than they first appear. Legal scholar Lisa M. Austin and computer scientist David Lie (2021, 256) observe that the concept of the data trust has been used in diverse and sometimes-conflicting ways. One set of meanings focuses on reducing technical and legal complexities regarding data protection, while the other set examines novel measures for data stewardship. As this diversity suggests, inherent within the concept of data trust are sometimes-conflicting notions of privacy and stewardship with the former emphasizing data protection and the latter focusing on managing data access:

two policy issues that involve separate responses that may or may not be complementary (Austin and Lie 2021).

While our focus here has been on data, the *trust* element of 'data trust' is also worth highlighting. Data trusts draw legitimacy not just from legal frameworks that purport to distribute benefits from data to the trust's beneficiaries but also from the rhetorical emphasis on 'trust'. Using the term 'data trust', observes legal scholar Christine Rinik (2020, 353), elicits a greater sense of stewardship than '"a data hoard" or "data warehouse"', even though these terms might more accurately describe a relationship involving 'the storage and exploitation of vast amounts of data by third parties'. As a result, a degree of wariness should be called for in determining whether specific data trust proposals fulfill legitimate policy objectives or are merely being deployed as rhetorical tools to elicit public trust or launder more problematic data regulation policies.

We do not discount that data trusts may have some potential to mitigate concerns over data control and ownership on different issues. However, given the challenges we outline here, policymakers need to be cautious about viewing data trusts as a simple or all-purpose tool to gain public trust. Data trusts are simply legal structures that manage data. As McDonald points out, 'data trusts manage assets, but do not inherently solve capitalism's asymmetries' or 'implicitly solve abuses of power' (McDonald 2019). Policymakers still need to think through the fundamental questions related to data governance, namely, for whom, by whom and for what purposes.

BEYOND INDIVIDUAL PRIVACY: ADOPTING A COLLECTIVE APPROACH TO RIGHTS

Contemporary privacy laws reflect a historical legal context that has generally privileged and assigned rights to individuals (Taylor et al. 2017b). Our contemporary environment, however, is characterized by several trends that challenge this individualist focus. As chapters 4 and 6 set out, there has been a dramatic increase in datasets, driven in part by the data broker industry, actors like Google and Facebook, and the rise of the consumer-oriented Internet of Things (IoT), which chapter 7 explores. Social media data, geolocational information from mobile phones, and data flowing from IoT devices provide rich detailed data. Automated tools have made it easier and more commonplace for actors to amass and parse large datasets, which combine the data of many individuals, in efforts to extract socially and commercially valuable insights, with effects that reach far beyond any one individual. These moves have led private and state actors to embrace group-level profiling, which current individual-focused privacy frameworks do not adequately address.

As chapter 4 cautions, actors can re-identify previously anonymized data, thereby capturing valuable personally identifiable information. But even beyond this fundamental challenge to individual privacy-focused laws, socio-legal scholar Mariana Valverde and legal scholar Alexandra Flynn (2020, 12) observe that Western privacy frameworks, focused on individual privacy, say 'very little about corporate control over the economic value of aggregate, non-personal, de-identified data' that can be used to target groups rather than individuals.

Privacy frameworks focusing on individual consent leave the public few protections in dealing with the dual problems of the data market and datafied public sector where governments employ data-fuelled analytics and automated tools to determine people's eligibility for services like welfare or housing. These decisions are made by identifying individuals as part of a group, not as individuals themselves. Ordinary people are caught in the rapidly evolving data economy and are expected to be capable managers of their personal data, even though research demonstrates that people cannot manage all the ways that companies use, and often abuse, their personal data (Obar 2015). In contrast to some private-sector data collection, people generally cannot opt out of interacting with their governments.

Any policy response aimed at addressing the deep-seated and structural problems we've discussed as inherent to the rise of the information-imperium state must go beyond individualistic notions of privacy and informed consent. Such an approach does not require ignoring or minimizing individual privacy rights: these are fundamental human rights and should be treated as such. Rather, the concepts of data justice and group privacy should be important complements of individual-based privacy. Both concepts adopt human rights-driven, collective approaches to governing data that fundamentally challenge the dataism and pervasive state/corporate surveillance integral to the information-imperium state.

Data Justice

Approaching data within a collective rights framework requires a consideration of the ways in which data-driven practices undertaken by states and private actors create harm. The concept of data justice is an alternative to individualistic approaches to human rights, as the concept takes a social justice-driven approach to resisting the modern datafied society (Dencik et al. 2016; Taylor 2017b). Communication scholars Lina Dencik et al. (2019, 181) have developed data justice as a concept that foregrounds questions about power relations in the collection, use and commodification of data, including how we may consider ideas of security, equity, fairness and sustainability in a data-driven society in which some groups reap enormous benefits and others are excluded.

A data justice approach is intended to transform concerns about privacy, data protection and surveillance from specialized 'digital' issues into 'a core dimension of social, political, cultural, ecological and economic justice' (Dencik et al. 2019, 181). In other words, questions about privacy, consent and governing data are not technical but rather fundamental to our society. Data justice does not focus merely on strengthening existing rights like privacy. Rather, it should be understood as 'a system-level critique' that does not focus on a specific type of data collection or technology 'but rather how datafication features in on-going negotiations of social relations and power dynamics within society' (Dencik and Sanchez-Monedero 2022, 8). In short, data justice aims to challenge and resist the 'central position of data in contemporary capitalism' (Dencik et al. 2019, 181).

As it is a concept intended to achieve social justice goals, data justice has concrete aims. Law and technology scholar Linnet Taylor (2017b) sets out these aims in three pillars: (in)visibility, anti-discrimination and (dis)engagement. The first pillar recognizes that sometimes people are too visible, as states or companies subject them to intense, often discriminatory, surveillance or profiling, especially if they are poor or otherwise marginalized, while other times people are overlooked or undercounted, leaving people without access to services. Addressing these two extremes entails recognizing that it is important people are represented accurately and appropriately (visibility), and are treated fairly and equitably (invisibility). Second, people should have a right to non-discrimination to identify and challenge bias in data use (Taylor 2017b, 9).

Finally, the pillar of (dis)engagement requires that people have the freedom to control the terms of how, or even if, they engage with data markets, including determining how their data is used and by whom (Taylor 2017b, 9). In practical terms, this means that people should be able to decide to opt out of specific private-sector data collection activities. This essentially involves a wholesale withdrawal from the datafied society and economy which operates according to the imperative that if information can be collected, it must be. The freedom to disengage from commercial databases has not yet been adequately theorized, as even privacy scholars generally 'assume that such engagement is inevitable' (Taylor 2017b, 10).

Adopting a data justice approach requires considering seriously how and where state and corporate data practices should be limited to address related harms like that of discrimination, as well as exploring the potential consequences of such limitations. A core element must also involve considering the nature and implications of data decommodification by examining how people may opt out of data markets, thereby removing their data from private actors or somehow remaining off-limits from data collection.

Group Privacy

The concept of group privacy is a response to private-sector and state uses of automated data tools to process massive amounts of data, often with a focus on group-level analysis. As scholars studying privacy point out, 'the individual is often incidental to the analysis. Instead, data analytical technologies are directed at the group level' (Taylor et al. 2017b, 2). This expansion of analytical focus from the individual, where privacy frameworks apply, to groups, where privacy frameworks are absent, 'challenges the very foundations of most currently existing legal, ethical and social practices and theories' (Taylor 2017b, 5). Simply put, as we note in chapter 4, we are in a situation where contemporary legal frameworks do not adequately address group-level data effects.

As we saw in chapter 6, fears of privacy violations or exposure to discrimination from group-level analysis are not abstract concerns. Genetic data, for example, complicates the notion of individual privacy as it reveals information not only about a specific individual but also their immediate and extended family members without their consent (Hallinan and de Hert 2017). The use of genetic data has received media attention as law enforcement has begun using consumer-oriented ancestry DNA databanks like GEDmatch to solve cold cases where genetic material (e.g., via a suspect's blood sample) was recovered (e.g., Chamary 2020). While catching violent offenders is laudable, law enforcement's use of consumer-oriented DNA companies raises critical questions of privacy and consent, as DNA samples uploaded for one consented purpose (ancestry research) can be (and are being) used to detect suspects and, in doing so, reveal genetic connections between individuals without their consent. In other contexts, law enforcement generally must obtain a legal order to access an individual's genetic material, raising concerns that police may use commercial DNA databanks indiscriminately.

The notion of group privacy or collective privacy has promising utility to address this gap in data protection. Group privacy has gained prominence in recent years, most notably in the edited volume *Group Privacy: New Challenges of Data Technologies* (Taylor et al. 2017a; see also Loi and Christen 2020; Puri 2021; Arora 2019). Philosopher and legal scholar Edward J. Bloustein (1978; see also 2017) was one of the first to articulate the concept of group privacy, but the idea is also evident in scholarship on privacy, to varying degrees, as 'relational privacy' or 'family privacy' (e.g., Westin 1967; see also Floridi 2014).

Definitions of group privacy vary broadly, as scholars from different disciplines explore what this new approach to privacy might entail (e.g., Loi and Christen 2020; Puri 2021). Legal scholar Alessandro Mantelero provides a useful starting point in describing collective privacy as 'the

right to limit the potential harms to the group itself that can derive from invasive and discriminatory data processing', particularly 'the unfair and harmful use of data that is processed using modern analytics' (Mantelero 2017, 148).

Group privacy, as understood by Mantelero and others, is not intended to replace individual privacy rights but rather to act as an 'important complement to individual privacy' (Taylor et al. 2017, 236). Individual privacy rights would continue to have legal protections attached, for example, to the collection and use of personal information, but group privacy would form a yet-to-be-determined additional layer of protection. A key part of group or collective privacy is deciding how to identify the cluster of individuals forming the grouping. This point may seem merely philosophical – at what point do individuals constitute a group? – but there are practical implications to this discussion. For the concept of group privacy to have meaning, the group itself needs to be somehow defined, as when 'some threshold of unity or identity has to be reached' (Jones 2016; cited in Loi and Christen 2020, 217).

Defining what constitutes a group is challenging. Do members self-define or can they be unaware that they belong to a particular group? Groups can be dynamic in their formation and membership. If the criteria constituting the group change, such as from people genetically prone to one disease to another health condition, then the group will change. Reasons for the creation of algorithmically generated groups, discussed in chapter 6, may only be known to the algorithm and its designers (Kammourieh et al. 2017; see also Loi and Christen 2020). Even if people were aware that group profiling affected them, when the origin and nature of such data practices are not publicly disclosed, there are few options available to challenge the conclusions.

Group privacy usefully provides the beginnings of a new vocabulary to counter some of the negative consequences of the information-imperium state and its overly commercial approach to data regulation. Of course, identifying and protecting group privacy rights does not automatically address the structural problems of mass data extraction and commercialization inherent to the data economy. Consequently, we argue that combining data justice and group privacy offers a useful perspective. Both data justice and group privacy reject the notion – foundational to the data economy – that people are individual rational consumers who should be responsible for managing companies' collection and use of their personal data (e.g., Taylor et al. 2017). Relatedly, both concepts push back against a mode of capitalism that views the datafication of all manner of social activities and personal attributes as somehow 'natural' or uncontested (e.g., Dencik et al. 2019). Instead of viewing people as consumers voluntarily and knowledgeably negotiating their way through a datafied society and economy, both concepts emphasize people's identity as 'citizens requiring data protection' (Taylor et al. 2017, 234). Government restrictions

on the type of personal data that private actors can collect and monetize are important elements of the broader process of data decommodification.

CONCLUSION

There are important geo-economic and geopolitical ramifications to data-governance debates, as states jockey for primacy in the control of the knowledge structure. Rules governing knowledge (in the form of data and intellectual property) are highly contested, as the regulatory and trade battles amongst the United States, European Union and China illustrate. These great powers are each forging ahead with their own plans for the data economy, with the latter two aspiring to become knowledge-feudalist states to counter the United States. Smaller states, in contrast, must determine how best to meet their domestic needs, which may include aligning with one of the great powers or enacting digital economic nationalist policies as a bulwark to protect domestic interests. Conflicts over how data should be conceptualized and governed exist not only among states but also between (and within) states and Indigenous nations. Recognizing the legitimacy of Indigenous data sovereignty requires taking seriously Indigenous group's rules prohibiting the sharing or commodification of sensitive knowledge (Kukutai and Taylor 2016; Walter et al. 2020). In some cases, Indigenous data sovereignty may conflict with governmental or civil-society preferences for open data, especially in relation to knowledge Indigenous groups deem sensitive or culturally important. This is because the fundamental issue regarding data – and knowledge governance – is around the question of control and who should decide the ends that should be pursued in regulating knowledge.

Shifting from an information-imperium state view premised upon the all-encompassing control of knowledge to a collective rights approach will be challenging and involves countering powerful state and industry interests that have accumulated considerable authority in a datafied society and economy. A central element of effectively countering negative knowledge-feudalist measures is a strong democratically accountable state, one that is bolstered and pushed forward by an engaged civil society. However, the degree to which governments have the necessary skills, resources and desire to regulate the digital economy and institute effective protections for human rights is an open question. Capacity will vary amongst countries but state action should be responsive to local contexts and needs rather than being driven by transnational business interests. Public regulators and governmental officials will require expertise in digital policymaking, intellectual property and data governance, amongst other key issues.

Adopting a human rights-driven collective rights approach also requires a fundamental shift in mindset. Instead of viewing people as consumers voluntarily engaging in the trade of personal data, people must be understood as citizens (broadly interpreted) who deserve to have their rights protected. Such a shift necessitates direct state action to ensure that data activities are 'linked to citizenship and accountability' (Taylor et al. 2017, 234). Data justice and group privacy provide a vocabulary and set of policies, situated within the larger approach of data decommodification, that potentially offer tangible data-protection benefits, such as enabling people to opt out of data markets. As they are relatively new, further work is needed by academics, civil-society groups and policymakers to develop and operationalize these concepts. An important element of this research will be to consider how they might be adapted to different sociocultural and political contexts to meet local needs.

NOTES

1. For a detailed examination of the GDPR, see Edwards (2018).
2. Unlike the GDPR, China's PIPL does not recognize privacy as a fundamental right, nor does it impose restraints on government bodies to collect and process data, although it does set out the data collecting powers and limitations of individual government departments (Creemers 2022, 8).
3. This point is often used to argue that data collected in one country may be subject to privacy-invading laws in the data-extracting country, as with the USA PATRIOT Act's expansive rules for government surveillance. The more fundamental point is that countries may have legitimate differences on what privacy legislation should look like. What this means is that the fundamental critique of cross-border data flows is linked to the lack of democratic accountability, not necessarily the nature of the privacy regime.

Conclusion

Thinking Beyond the Market

In this book, we explored several key questions:

- What is the nature of the knowledge-driven society?
- What are the social (economic, political, creative) effects of the emergence of the control of knowledge as a key power vector?
- Who will benefit and lose out from these changes?
- How can we respond to these changes so as to encourage widely shared prosperity without compromising fundamental human and democratic rights?

The previous chapters explored the first three questions. In this final chapter, we will briefly summarize our argument and findings before turning our attention to our final question.

POWER IN THE KNOWLEDGE-DRIVEN SOCIETY

Drawing on the work of Susan Strange, we argue that we are witnessing the increasing relative importance of the knowledge structure. As a result, the global political economy is being reshaped, with the control of knowledge, particularly as data and intellectual property (IP), at the heart of society.

This transformation is pervasive: manufacturers are retooling their business structures to facilitate data measurement (Srnicek 2017); companies have used IP to shift the global economy from an international trade model to one based on global supply chains (Schwartz 2021). Governments around the world, democratic and authoritarian, are embracing algorithmic regulation

and surveillance as a means to govern (Eubanks 2018; Henne 2019; Harb and Henne 2019).

Drawing on the work of Robert W. Cox, we argue that a knowledge-driven society is propelled by a set of state and non-state actors that share common interests in knowledge regulation. Much as a financialized state sees policy issues through a lens that puts questions of finance first, the information-imperium state sees policy and society primarily through the lens of control over knowledge. For the information-imperium state, the primary policy questions relate to who should control economically and socially valuable knowledge, and for what purposes.

The dominant ideologies of the information-imperium state are those of dataism married to technological solutionism. As we discuss in chapter 5, dataism is the belief that data is a neutral representation of reality and the highest possible form of knowledge. It upends our traditional notions of what knowledge is, shifting perceptions of expertise from subject-matter experts to technicians able to access and process huge quantities of data. Technological solutionism, meanwhile, is an ideology that starts with the answer – technology – and redefines the policy question to fit the abilities and limitations of the technology and those deploying it.

Taken together, our use of Strange and Cox highlights how power resides with those who possess knowledge that is believed to be economically and socially valuable. We've witnessed the rise of knowledge-processing companies like Amazon, Tencent and Google. We've also witnessed how the United States, through the adept use of trade agreements and by nurturing its world-beating companies, has managed to maintain its position atop the global economic order through its control over data and IP flows. We've called this approach knowledge feudalism: the pursuit of ever-stronger controls over knowledge paired with free cross-border flows of the same. It's the strategy of the dominant, and it's designed to place all those who do not possess this knowledge in a subservient position.

Much of this book has focused on this dynamic, whether it involves farmers versus agricultural companies, IP-rich companies that franchise out the risks to others while retaining the monopoly benefits for themselves or welfare recipients at the mercy of far-from-neutral algorithms. As to winners and losers, the spoils go to those who control the knowledge. All others must pay up and adapt.

However, this knowledge feudalism has also been challenged in a number of ways. We have noted the scramble by relatively data- and IP-poor countries to rectify their situation through digital economic nationalism. Success in a knowledge-driven economy requires access to knowledge. Countries and companies lacking such knowledge assets are not well served by a protectionist, knowledge-feudalist regime. As followers, they benefit from strategies

that favour greater sharing of data and IP. Usually, the scale of this sharing occurs at the national level within a country's borders. The goal of a digital economic nationalist strategy is the promotion of homegrown companies that are capable of competing with the dominant knowledge feudalists. While China is usually seen as the typical digital economic nationalist, as chapter 8 explains digital economic nationalism is also practiced by the European Union, Canada and others, through policies designed to grow their own tech industries through the pursuit of domestic initiatives. It is not an authoritarian strategy.

At heart, however, both knowledge feudalism and digital economic nationalism see knowledge as a commodity. Within the logic of a commodified, knowledge-driven society, a digital economic nationalist approach makes sense: create and capture as much IP as possible while ensuring yourself access to the data needed to make advances in machine learning and artificial intelligence.

However, as we have discussed at length, there are real and consequential limits to the adoption of both digital economic nationalist and knowledge-feudalist approaches. Leaning into the data- and knowledge-driven economy in this way comes with a substantial cost. For one, by privileging a country's own businesses and citizens over foreigners, digital economic nationalism recreates international relations of dominance inherent in highly protectionist knowledge-governance regimes. Even well-meaning attempts at data regulation like the EU's General Data Protection Regulation (GDPR) cannot capture fully the complex and different approaches to privacy, either within or across society (chapters 8 and 9). Such efforts end up being neocolonial attempts to impose data standards on non-European countries without their consent (see Bradford 2020), placing European regulators as the ultimate adjudicators over whether a country's regulations meet their own standards.[1]

Drawing on the work of Karl Polanyi, meanwhile, we highlight the belief that the most economically and socially valuable form of knowledge is commodified knowledge, that is, IP and data. They're also what he calls fictitious commodities: things that exist beyond their assigned role as commodities in the marketplace. The knowledge protected by IP rights has purposes beyond being marketplace assets or commodities: they are the knowledge that allows us to create life-saving drugs and the cultural works that define us as humans and as societies.

Polanyi warned that societies that fail to regulate fictitious commodities – that is, anything that is treated as something produced for the market but that is not created for the market (Cioffi et al. 2022) – will tear themselves apart. The purpose of the underlying knowledge – to express a form of culture or to save lives – is obscured and sometimes negated by this knowledge's function as an asset that can earn its owner piles of money. As we've noted, strong IP

protections make it that much more difficult for countries to access the life-saving drugs they need to end the global Covid-19 pandemic, to say nothing of the need to widely disseminate the clean technologies we'll need if we wish to retain any hope of bequeathing a livable planet to the next generation (Drahos 2021).

Data, too, can be thought of as a fictitious commodity. Fitness wearables only work if worn. It's when data is taken out of the context within which it was produced that it becomes a fictitious commodity. This is why personalized advertising online may feel like a privacy violation, as the ads are based on surveillance of our web traffic and purchase habits. It is also why predictive algorithms about people's behaviour or habits are such a problem: both cases amount to a repurposing of data from its original context and turning it into a commodity. More than that, however, such data collection and use are based upon dataist ideas, that our bodies, emotions and ideas can be accurately quantified and rendered into precise actionable forecasts that have commercial or social value. As these examples suggest, data as a fictitious commodity all-too-often is deployed to serve the interests of those doing the harvesting, not the people serving as the sources of data.

BEYOND THE MARKETPLACE: A DEMOCRATIC PATH TOWARDS HUMANE KNOWLEDGE GOVERNANCE

Control over knowledge, and over what counts as knowledge, has always been a foundational element in the expression of power. What has changed is the relative importance of the knowledge structure in the pursuit of power. When data and IP are suffused throughout society, knowledge regulation becomes a first-order policy issue that must be treated as seriously as security, finance and production, Strange's other key forms of structural power.

As we have shown, control over knowledge affects everything from the potential for economic growth and access to medicines to basic principles of ownership and – when data is locked up in a corporation – the ability of governments to enact policy in the public interest. In government circles, data and IP governance should be placed on the same level as monetary policy in terms of the importance of these areas' contribution to citizens' well-being.

Recommendation 1: Build Greater State Capacity

The ability to craft sound policy in the area of IP and data governance requires the capacity to do so. IP continues to be a second-order issue within trade circles.[2] Similarly, the understanding of data in many policy arenas remains so limited that we lack a consensus understanding of how it should be used

or how it should be regulated (Breznitz 2021, 175). Some governments, such as Brazil's and the European Union's, have been working on data-governance issues for decades and thus have been relatively well-placed to address the challenges of a data-driven economy. The United States, meanwhile, has long articulated a consistent knowledge-feudalist approach to IP regulation (Halbert 2016). However, we have reached a point where no government, national or subnational, can afford to ignore or downplay data and IP governance.

We argue that greater state capacity and a clear articulation of the public interest (on which we will say more below) in data and IP governance are now a necessity. Currently, the vast majority of expertise in these areas resides in the private sector. This needs to change.

States are invaluable actors in taming the knowledge-driven society. A vibrant civil society has a role to play in creating this capacity and in promoting justice. Civil society functions best in working to hold states and companies to account via advocacy actions. However, civil society is not an alternative to state capacity. It exists in relation to the state (Germain and Kenny 1998); it cannot rule on its own. Civil-society organizations also possess several limitations in and of themselves, most notably with respect to access to resources and representativeness of the public. Civil society influences governments and companies; it cannot govern.

Industry self-regulation, meanwhile, works best in a fully competitive marketplace, where consumers, unhappy with a service, can take their business elsewhere. In the face of monopolistic markets, which tends to describe the markets we've explored in this book, such threats are largely empty. Absent a competitive market, civil-society proposals for tech reform amount to little more than special pleading, to be accepted or rejected at the company's whim. The need for a dynamic civil society turns on the importance of democratic rule and openness to citizen participation.

The role of the state is especially important when one considers the pressures towards knowledge commodification that characterize our particular knowledge-driven society. Businesses are, by definition, creatures of the marketplace, with little-to-no incentive to resist the commodification of knowledge that, as Polanyi notes, can be so destructive to society. The limiting role must be played by the state.

In the case of smaller countries like Canada, capacity building must start by developing an independent research ability to analyse these issues and to help policymakers formulate their versions of the public interest. While civil society and academia produce helpful work, it is no substitute for democratic governments possessing the ability to evaluate this research according to their own criteria and perception of the public interest.

Building state capacity requires putting this knowledge into practice by strengthening expertise amongst existing policymakers and analysts, as well

as cultivating new talent. Data and IP governance expertise in the public interest is not something that can be outsourced to the private sector. Reactive regulation, spurred by the latest industry whistleblower or public outrage, is a poor governance strategy.

Recommendation 2: Build Greater Academic Capacity

The need to pay attention to data governance extends to academic study as well. Despite its rising importance, IP rights remain an issue dominated by legal studies and legal professionals. It remains a niche topic in economics, the discipline most suited to considering questions of economic development, to say nothing of political science, sociology and international political economy, all of which have valuable perspectives to offer the study of IP and knowledge governance more generally.

The study of data governance itself is still in its early stages, with many questions about what makes for an optimal policy still undecided, particularly in governmental circles (Breznitz 2021, chapter 11). There is, however, a growing interdisciplinary academic field – critical data studies – that is generating excellent research (see, e.g., Kitchin 2014a) and policy-relevant insights (see, e.g., Daly et al. 2019).

One of the challenges for academics in conducting research on data, indeed on the broad topics of the data-driven economy and datafied society, is maintaining independence from industry in general and technology companies in particular. Wealthy tech companies fund many academic centres and conferences, a pattern of industry funding following other sectors like pharmaceuticals and mining.

A perennial question for scholars is where – and how – to draw a line between academic research and industry, particularly when industry funding or access to industry data is integral to scholarship. As doctoral candidates Mohamed Abdalla (computer science) and Moustafa Abdalla (medicine) note, 'big tech' has been funding academic research in ways reminiscent of Big Tobacco, designed 'to put forward a socially responsible public image, influence events hosted by and decisions made by funded universities, influence the research questions and plans of individual scientists, and discover receptive academics who can be leveraged' (Abdalla and Abdalla 2021, 287). Similarly, legal scholar Jake Goldenfein and criminologist Monique Mann note that the active funding of academic research and civil society groups raises questions about 'the alignments and misalignments of their interests' (Goldenfein and Mann 2022, 1). There is an important role for the government here to fund scholarly research, particularly that which challenges industry or addresses under-examined topics.

Recommendation 3: Create Democratic Frameworks

Decisions surrounding data and IP governance must be embedded within a democratic decision-making framework. Insisting on the democratic regulation of knowledge leads us towards certain policy conclusions. Private-sector automated, or algorithmic, regulation, discussed in chapter 6, must not only be made transparent so that we can understand how private companies regulate. It must also be subject to oversight by democratic governments and subject to reforms if these companies are not regulating in the public interest, again as determined by accountable governments via transparent policymaking processes. Governments themselves, however, may have to be pushed into accountability, as chapter 8's exploration of government-operated automated debt-recovery programmes shows.

Understanding data and IP governance issues within an international context is also necessary, including conditions of exploitation between the Global North and Global South, the latter serving as a source of data for the former in ways that resemble a new form of colonialism as expressed in the concept of data colonialism (Couldry and Mejias 2018). This neocolonial relationship also has an environmental angle. Training algorithms and mining cryptocurrencies require massive energy consumption, which needs to be accounted for in any assessment of the utility of these technologies. Software-driven devices – phones, vehicles, fitness wearables and medical devices – all require rare earth minerals (Crawford 2021). The rapid acceleration of planned obsolescence, paired with restrictions on repair, means e-waste is a growing concern, especially in Global South countries where it is dumped (Forti et al. 2020).

The international dimension of a global knowledge-driven economy and society, overseen in large part by companies with a transnational reach, is embedded within bilateral, plurilateral and multilateral agreements and organizations. A knowledge-feudalist approach to global knowledge regulation involves, at heart, harmonizing the regulation of data and IP across societies with different needs and values. In IP, this harmonization has taken the form of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Global data governance is nowhere near as advanced as the centuries-old global IP regime. However, here we see attempts by the larger state and industry powers to impose their own preferences on other countries, even though, as we've discussed throughout this book, what is seen as just and appropriate for one country may not be for another.

We should be particularly cautious in pursuing global regulatory regimes for data, given the lack of consensus and understanding over the very nature of data itself. Global regimes that advocate transnational data flows, for example, would appear to primarily benefit Global North actors that have

the resources and infrastructure to extract value from data at the expense of those in the Global South. Here, we can turn for guidance to economist Dani Rodrik's advocacy for a weak form of globalization (Rodrik 2011). Cross-border exchanges of goods and (in our case) knowledge can provide significant economic and social benefits to all involved – as can the pursuit of technological innovation – provided they are not driven by politics of domination. Instead of harmonization, countries should aim for interoperability: identifying the minimal standards upon which they can agree while ensuring that domestic needs and values are accommodated within democratic frameworks. How states and industries use data, as well as the modes of data governance, as we have argued throughout the book, need to account for the particularities of local contexts. Rather than trying to fit societies into global one-size-fits-all data or IP policies, our efforts should be directed towards accommodating local needs and democratically expressed interests in globally interoperable regimes.

DECOMMODIFICATION AND DATA JUSTICE

Calls for greater capacity and more democratic decision-making leave to the side the question of *how* states should regulate. While there exists no one-size-fits-all policy for either data or IP, we can suggest several starting points and specific recommendations for states to consider.

Recommendation 4: Focus on Decommodification

In a knowledge-driven society, and for the information-imperium state, the most important policy questions are about the control over and use of knowledge. For a country thinking like a knowledge feudalist or a digital economic nationalist, these questions translate into how to control this commodified knowledge, with a particular emphasis on the reappropriation of knowledge for purposes outside the contexts within which it was developed. In the case of data, commodification involves the use of data for purposes beyond the context within which the data was created and collected, potentially against the interests of those individuals and groups from whom the data was extracted in the first place. In the case of IP rights, commodification involves the appropriation of knowledge for profit in and of itself, separate from the instrumental function of knowledge, be it in the form of a cultural expression, like a song, designed to express our very humanity, or a vaccine intended to stave off untimely deaths.

Taking Polanyi's critique of fictitious commodities seriously highlights that governments' data and IP policies should focus on *restricting* the

commodification of knowledge. In terms of IP rights, this would require reducing their terms, scope and duration. For data, it would require severely restricting the trade in data, and reducing the proprietary control over data held by the large data giants. This entails restricting the commercialization of personal data, such as limits on monetizing genetic data or curbing commercial facial-recognition technologies. It also includes the need to limit the commodification of some non-personal data, such as farming data, to counter power asymmetries, in this case between farmers and big agri-data firms.

The purpose of knowledge creation and dissemination – be it data, drug formulas, computer programs, music or literature – is twofold: the betterment of individuals and human society and to encourage human expression. As we've seen throughout this book, knowledge commodification, taken too far, works against these fundamental human interests, which themselves serve as the foundation of every healthy human society. In every case, the problem has been the same: the appropriation of human knowledge, be it as data or IP, by some individuals and groups for their own particular interests. To decommodify knowledge is to ensure that we never lose sight of why this knowledge was developed in the first place, and to be guided by those purposes.

At first glance, our call to decommodify knowledge may seem almost utopian. The sense that it's unrealistic to call for the rolling back of IP protections or for much-stronger constraints on the trade in data is itself reflective of the fact that we live in a (commodified) knowledge-driven society. As we noted in chapter 1, in a society that sees knowledge creation primarily in terms of propertized knowledge and equates knowledge with data collection, any proposed restrictions on the commodification and use of knowledge will be interpreted as a threat to either prosperity or security. However, what we propose – that data and knowledge policymaking begin from a human-centric, rather than market-focused, starting point – is simply about recognizing the need to limit market forces in an area of fundamental societal interest, in the same way that labour policy and environmental policy start from the premise that to fully commodify our labour or the planet is to invite social and ecological ruin. The goal is not the end of technological advancement or the curtailing of human innovation; it is to ensure that such advancements support widespread and sustainable human and societal development.

Just as what we propose is in line with market restrictions in other key areas, much of what we propose here has been discussed and debated for decades, from the 1990s Access to Knowledge (A2K) movement and the push for equitable access to life-saving medicine to treat HIV patients in developing countries (Drahos and Braithwaite 2002) to the current right-to-repair movement (see Perzanowski 2022). What's more, as we highlight next, our proposals would stimulate both innovations and respond to the needs of the many, rather than of the few.

Decommodifying Intellectual Property

As we discussed in chapter 3, the current IP regime serves mainly to protect the incumbents who already own vast amounts of IP, both states and corporations, and to stifle innovation. While free-trade treaties could claim some legitimacy through the appeal to comparative advantage, there is no such legitimation on offer for the ever-stronger IP protection we see in trade agreements today. Although it is possible for companies, countries and regions to situate themselves and even prosper to a degree within such a system (Breznitz 2021), overall it offers a recipe for greater income and wealth disparities and lower productivity growth (Schwartz 2021; Mazzucato 2018).

Restricting the commodification of the knowledge currently protected by IP would ensure that this knowledge is both used for the purpose it was created and also to promote innovation. The current IP regime discourages innovation while protecting incumbents against competition. While restricting IP commodification sounds radical, the restrictions baked into IP policy itself recognize the danger inherent in commodification and the need to limit this commodification. At the very least, any new laws or treaties should be subject to a rigorous empirical analysis that addresses the protection-dissemination paradox head-on: only those laws that can be shown to improve the spread and use of knowledge should be considered, and then only once the interests of Indigenous peoples, from whom much knowledge has already been appropriated, have been addressed. As chapter 3 also noted, such analyses are very sensitive to the model's assumptions, but one has to start somewhere and transparently highlighting one's assumptions is as good a place to start as any.

Greater attention also needs to be given to the argument, made by economist Mariana Mazzucato (2018) and others, that IP is neither the only nor the most effective way to incentivize knowledge creation. She notes that the state, long derided by free-market evangelists, is responsible for the lion's share of the riskiest, most fundamental research, while IP and venture capital funding allows private actors to capture and control an unfair share of the spoils. Mazzucato notes that governments, for example, have directed significant investments in the early, high-risk stage of developing nanotechnology, clean technologies and pharmaceuticals. We need to reacquaint ourselves with the open university approach to knowledge, which sees knowledge as something to be shared, not hoarded (Drahos and Braithwaite 2002). Weakening the IP system could also help to move economic competition away from the franchise model and its attendant societal-level drawbacks.

The climate emergency lends a significant degree of urgency to the task of addressing these structural deficiencies. As regulatory scholar Peter Drahos notes in this same context, some forms of knowledge are too important to be

walled up behind high IP barriers (Drahos 2021). The global dissemination of clean technologies should be an urgent priority. Patent protections should not be allowed to stand in the way. Mandatory licences for clean technologies should be on the table, much as mandatory licensing for Covid-19-related technologies, including vaccines, should have been during the pandemic. As we write this conclusion in October 2022, over two years into the pandemic, countries and pharmaceutical companies are still trying to improve access to patented vaccines. Such proposals to weaken IP are not novel: they echo calls from the A2K movement, which in the early 2000s was already highlighting the role that access to knowledge plays in developing countries' economic development prospects (e.g., Krikorian and Kapczynski 2010). It also echoes the food sovereignty movement championed by such people as noted ecofeminist Vandana Shiva, which has been highly critical of seed patents (e.g., Shiva 2016), as well as ongoing efforts to reduce patent protection on life-saving drugs (Shadlen et al. 2013, 2020) and the right to repair as it relates to medical equipment (Paul 2021). Going even further away from the IP system, the movement to promote traditional and Indigenous knowledge, while multifaceted, can be seen as an attempt by Indigenous groups to assert control over various forms of knowledge in their (self-defined) interests (e.g., Kukutai and Taylor 2016; Walter et al. 2020).

All of these proposals or movements are responding to how the commodification of knowledge ends up locking entire groups, countries and regions out of the ability to access various forms of knowledge that are essential to life itself – textbooks, medicine, food, the ability to repair one's tools – in ways that affect both their life chances and ability to develop economically. Similarly, they all are concerned with improving access to knowledge in ways that create the conditions for individuals and groups to realize their potential and maximize their own freedom. Most importantly for our purposes, they all advocate for restricting and rolling back the further commodification of knowledge via IP rights.

Decommodifying Data

Turning to data, decommodification or limiting commodification requires that data only be used for the purposes for which it was originally collected. Stated more positively, we need to ensure that knowledge is used not as a commodity but for the purposes directly linked to the conditions of its generation. This requirement is linked to, but goes beyond, requirements that individuals provide meaningful, informed consent for how companies and governments use their data. Commodified data is data that is removed from the context within which it was collected, as when marketers repurpose voice data from people using their smart speakers. Data collection via Amazon's

smart speakers is not a problem when the data is used to answer questions in the household, which is the purpose of a voice-activated internet-connected speaker. It is when that same data is extracted to sell ads, or more worrisomely, to develop tools to determine people's possible traits or interests, a practice termed 'voice profiling' (see Turow 2021), that the interests of users is violated.

Decommodification implies putting the consumer or user's interests ahead of the actor collecting the data, be it a business, a government or a non-profit. Data should, in many cases, be understood as a 'social asset, a platform upon which trust and cooperation can be built, enabling a "social license to operate" earned from those who are supplying the data' (Trenham and Steer 2019, 48).

The implications of treating data as a social rather than as a commercial asset place limitations on what data should be collected and how it can be used. One concrete step we could take would involve restricting or outright prohibiting commercial forms of biometric data profiling, particularly technologies that claim to identify people's political affiliations, sexuality, creditworthiness or criminality based on biometrics like facial features, fingerprints, voice or gait (Stark and Hutson 2021; Turow 2021). In many of their commercial applications, as explored in chapter 6, these technologies are nothing but a form of pseudoscience that can cause real harm: through their use, people may lose jobs, access to credit or be targeted by repressive governments. Furthermore, given their central role in a data-driven society, promoting a more just knowledge-driven society that centres the interests of citizens over corporations requires the strict regulation of data brokers and the market in data.

Recommendation 5: Hedge against Dataism and Technological Solutionism

Policymakers also should work to avoid the siren song of dataism and technological solutionism. Doing so requires that we avoid the temptation to reduce all problems to the digital data that can be collected about them. Simply recognizing the relevance of contextual knowledge and subject expertise in giving meaning to data can go a long way towards demystifying the latest attempt by a Silicon Valley start-up to rediscover what already exists. Similarly, a healthy respect for context combined with a commitment to starting with the problem rather than the solution – by evaluating all proposals according to pre-existing context-specific criteria, rather than simply assuming that digital can add value to any project – can offer a useful hedge against technological solutionism.

The problems with data and surveillance are not intrinsic to data or its collection, but to the purposes for which data is collected and an unjustifiable

faith in data as a neutral arbiter of reality. Nowhere is this clearer than in the belief that, given enough data, we can accurately predict human behaviour. This is why we argue that the true threat of predictive algorithms is not that they will rob humans of their agency. Rather, it is that government officials and corporate executives will act *as if* such technology is capable of neutral, objective action. In doing so, their actions will create a self-fulfilling prophesy.

Adopting a principle of decommodification involves more than simply ensuring that data is used in the best interests of those from whom it is collected, be it an individual or a community. Identifying what counts as 'best interests', as lawyer and data-governance expert Sean McDonald notes (2022), is itself a political question and one that is open to self-interested justifications. As a result, considering how such questions are decided is a key component of an effective decommodification-focused data-governance regime.

The city of Barcelona offers some important lessons in how to think about what democratic data governance should look like. At the same time that we were virtually attending the Waterfront Toronto–Sidewalk Labs town hall that we discussed in the introduction, Barcelona was becoming famous for its citizen-led approach to data and digital infrastructure and innovation in its own smart-city project. However, in contrast to the top-down model proposed by Sidewalk Labs and mirrored in other examples throughout this book, Barcelona took a bottom-up approach to data collection and system design.

Barcelona did not eschew surveillance or data collection. Rather, it sought to embed data collection within a citizen-focused framework of technological sovereignty based not only on personal autonomy but also on 'collective empowerment and democratic governance' (Mann et al. 2020, 16). Data would be collected via sensors, with appropriate privacy protections and, equally importantly, with collective oversight and decision-making about how the data would be used (Mann et al. 2020, 17). Barcelona's decisions, including its embrace of open-source software, make it easier for the city to avoid the problems with vendor lock-in that can occur when one is stuck using a company's IP-protected proprietary technology (Monge et al. 2022, 8).

In terms of specifics, what worked in Barcelona may not necessarily work elsewhere, as other places have their own particular socio-political and legal contexts. However, Barcelona's overriding objective may provide other cities guidance when it comes to creating appropriate digital and data policies. In the words of Barcelona's Digital Plan, their goal was to place data 'at the service of the people and not the people at the service of technology' (cited in Mann et al. 2020, 16). By taking this type of principled approach, Barcelona's smart city was able to embrace (certain types of) surveillance and data collection. The fears around surveillance and individual privacy that accompanied apps such as the Covid Alert app (chapter 5) didn't materialize because it was clear why

and for whom the data was being used. In Barcelona, residents were not averse to data collection in and of itself, so long as its purpose was clearly identified. Understanding noise or pollution levels in a neighbourhood is a necessary step to making a neighbourhood livable. In this case, however, defining the problem to be fixed, identifying priorities and controlling data rested with both the individual-as-citizen and with the collective, subject to democratic oversight.

The Barcelona approach emphasized the social use of data, not its value as a tradable commodity to be repurposed by a company or government agency far removed from the people who generated it. This is what data, and knowledge, decommodification look like. Data's value should not be in how it can be repurposed (as a commodity), but in how it relates to the specific reason for which it was collected, for the good of those who supplied it.

Recommendation 6: Focus on Data Justice

The concept of data justice, which we explored in chapter 9, offers a more useful framing for creating data-governance policies than relying on individual-based concepts of privacy for assessing the benefits and drawbacks of state and corporate data collection policies. Data justice focuses on the purposes and context within which data-governance decisions are made, specifically adopting a social justice–driven approach (Dencik et al. 2016; Taylor 2017b). It rejects dataism's assumption of data neutrality in favour of a commitment to ensuring that automated systems do not recapitulate historical forms of disadvantage and discrimination (Henman 2019).

A data justice approach, recognizing that there are real harms from states' use of automated decision-making programmes, as discussed in chapter 8, would sharply limit governmental use of automated systems in public service programme delivery or management. Following the Barcelona example, it would also ensure that data collection and use should only be undertaken by and for the interests of those who supply the data. While state use of automated decision-making may be appropriate in some limited circumstances, we contend that it is not appropriate to determine eligibility for or manage the delivery of government services in areas where they can significantly affect people's lives, such as in matters of immigration, criminal justice and the provision of social services.

True to its emphasis on social justice, data justice takes seriously people's agency and right to choose the nature of their engagement in the data economy by arguing that people should be allowed to opt out of data markets (Taylor 2017b; Dencik and Sanchez-Monedero 2022). This is near heresy in the data economy – knowledge feudalism demands data to be siphoned from (nearly) all people, objects and environments – but is an essential step towards data decommodification.

Recommendation 7: Emphasize Group Privacy, Not Only Individual Privacy

Privacy rights may be a helpful starting point for considering the effects of data on society. But whose privacy is to be taken into account, when should data be shared and with whom? Chapter 4 highlighted how attempts by Indigenous communities in British Columbia to get access to pandemic medical data about their communities were initially thwarted by the provincial government on privacy grounds (see Slett and Sayers 2020). As this case of Indigenous data sovereignty demonstrates, knowledge regulation is an inherently political issue that creates winners and losers. It can only be settled through political contestation. Susan Strange (1994) noted that if we wish to understand the power and the political economy, we need to look at bargains like this. Their outcomes tell us a lot about who holds power in a society, who a society values and what values that society holds.

Complementing the concept of data justice is the concept of group privacy. As we explore in chapter 9, group privacy is a collective-rights approach to privacy. Like data justice, group privacy rejects the data economy's foundational myth – embedded in dominant individual-based privacy approaches (Taylor et al. 2017a; Obar 2015) – that people are capable of individually managing companies' collection and use of their personal data within individual-based privacy frameworks. Privacy experts do not intend group privacy to substitute for individual privacy rights, as these rights are fundamental human rights, but rather to 'complement' those individual rights (Taylor et al. 2017, 236). Group privacy is a relatively new, under-theorized concept, and how it may form an additional layer of privacy protection is yet to be determined.

Both group privacy and data justice resist moves by business and state actors to datafy all aspects of human life. Datafication of all social activities is not 'natural' but a policy choice (e.g., Dencik et al. 2019). Both concepts also usefully call into question what type of economy and society we want and how technology might serve those goals.

Both concepts also highlight the need for a prominent role to be played by democratic states. Neither group privacy nor data justice can be fully enacted solely by civil-society groups or achieved through well-meaning but non-legally binding sets of principles subsequently ignored by governments and businesses alike. Instead of continuing to cast people as 'consumers' or 'users', which further entrenches their place within the data economy, data justice and group privacy elevate people to 'citizens' (broadly conceived) 'requiring data protection' (Taylor et al. 2017, 234). It is in and through the democratic state that groups can advocate and enforce these necessary collective rights.

LOOKING TO THE FUTURE

As we write this conclusion in October 2022, we can see some bright spots that reflect elements of the decommodification, democracy and data justice perspective. More governments are at least grappling with issues of data governance, for example, with countries across the world passing data-protection laws that resemble the EU's GDPR. However, these laws may effectively protect people's rights, whether from violations by governments or industry, remains to be seen.

The European Union, meanwhile, has passed legislation, the *Data Services Act* and the *Data Markets Act*, that is designed to regulate and limit some aspects of the data economy and can be seen as a tentative step towards decommodification and data justice. Despite these developments, the world's leading IP powers remain (as of this writing, over two years into the pandemic) extremely reluctant to relax patent protections for life-saving Covid-19 vaccines. While group privacy and data justice as concepts continue to languish in the shadow of individual approaches to privacy rights, the politics of data and IP remain as contested as ever. Similarly, knowledge feudalism is dominant in IP, but awareness of the challenges of the knowledge-driven society is increasing.

Lurking beneath the surface of the knowledge-driven society is the idea that commodified knowledge – be it data or IP – can save us. However, as Karl Polanyi reminds us, the commodification of things like knowledge, labour and land creates existential problems when it is not subject to strict limitations.

In the end, it is a question of balance. Finance, security, production and knowledge are all essential to a functioning society. However, when one structure dominates over the others – when we allow bankers, militaries or advertising companies like Google to steer society – we end up with global financial crises, dictatorships or rampant, harmful technological solutionism. Movements to improve access to life-saving drugs, to fight for farmers' and others' right to repair and to avoid algorithmic discrimination, among the many other actions that we explore in this book, are all expressions of this desire for balance and for technology and knowledge to serve human needs, not the other way around.

The knowledge-driven society and the information-imperium state are human creations. They are a choice. We can say with certainty that this form of state will not last forever. The contest for structural power is also a contest for dominance among actors based within the different structures. Between the largest European war since the 1940s, the global pandemic and the rapidly worsening climate emergency, the 2020s are shaping up to be as unsettled a decade as we have seen in any of our lifetimes. It is not impossible, in such

an environment, to imagine a world in which actors based within the security structure begin to dominate. However, just as the financial structure, so dominant since the 1980s, shaped the emergent knowledge structure, so will the dominant players in the knowledge structure shape whatever lies in our future.

Regardless of what the future holds, the need for a humane and just knowledge-governance regime will persist. The first step to realizing this humane future is that we ask the right questions, which are the questions at the heart of all cities and societies: What kind of world do we want to build? And in whose interest?

NOTES

1. Thank you to Odilile Ayodele of the University of Johannesburg for this insight.
2. Haggart (2022) discusses this phenomenon within the context of the renegotiations of the North American Free Trade Agreement.

References

Abdalla, Mohamed, and Moustafa Abdalla. 2021. 'The Grey Hoodie Project: Big Tobacco, Big Tech, and the Threat on Academic Integrity'. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 287–97. New York, NY: Association for Computing Machinery. http://doi.org/10.1145/3461702.3462563.

Abril, Danielle. 2020. 'Trump Hyped Verily's Coronavirus Testing Tool. It Led to Less Than 1% of All Tests in 2020'. *Fortune*, 29 December. https://fortune.com/2020/12/29/alphabet-verily-coronavirus-tests-2020-trump-google-covid-19/.

Ada Lovelace Institute. 2021. 'Exploring Legal Mechanisms for Data Stewardship'. *Ada Lovelace Institute*. https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.

Aiolfi, Simone, Silvia Bellini, and Davide Pellegrini. 2021. 'Data-Driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising'. *International Journal of Retail & Distribution Management* 49 (7): 1089–110. https://doi.org/10.1108/IJRDM-10-2020-0410.

Alexander, Michelle. 2020. *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*. 10th Anniversary ed. New York, London: The New Press.

Allen, Hilary J. 2022. *Driverless Finance: Fintech's Impact on Financial Stability*. New York: Oxford University Press.

Allsup, Maeve, Erin Mulvaney, and Joyce E. Cutler. 2022. 'Gig Economy Companies Brace for Crucial Year as Challenges Mount'. *Bloomberg Law*, 4 January. https://news.bloomberglaw.com/us-law-week/gig-economy-companies-brace-for-crucial-year-as-challenges-mount.

Amadeo, Ron. 2022. 'Shameful: Insteon Looks Dead—Just Like Its Users' Smart Homes'. *Ars Technica* (Blog), 18 April. https://arstechnica.com/gadgets/2022/04/shameful-insteon-looks-dead-just-like-its-users-smart-homes/.

American Farm Bureau, and John Deere. 2023. 'Memorandum of Understanding'. https://www.fb.org/files/AFBF_John_Deere_MOU.pdf.

Amnesty International. 2021. 'COVID-19: Time for Countries Blocking TRIPS Waiver to Support Lifting of Restrictions'. *Amnesty International*, 1 October.

https://www.amnesty.org/en/latest/news/2021/10/covid-19-time-for-countries-blocking-trips-waiver-to-support-lifting-of-restrictions-2/.

Andeobu, Lynda, Santoso Wibowo, and Srimannarayana Grandhi. 2021. 'A Systematic Review of E-Waste Generation and Environmental Management of Asia Pacific Countries'. *International Journal of Environmental Research and Public Health* 18 (17): 9051. https://doi.org/10.3390/ijerph18179051.

Anderson, Chris. 2008. 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete'. *Wired*, 23 August. https://www.wired.com/2008/06/pb-theory/.

Andrejevic, Mark. 2014. 'Big Data, Big Questions: The Big Data Divide'. *International Journal of Communication* 8 (June): 1673–89. https://ijoc.org/index.php/ijoc/article/view/2161.

Andrejevic, Mark, and Mark Burdon. 2015. 'Defining the Sensor Society'. *Television & New Media* 16 (1): 19–36. https://doi.org/10.1177/15274764145415

Apple. 2021. 'Apple Announces Self Service Repair'. 17 November. https://www.apple.com/ca/newsroom/2021/11/apple-announces-self-service-repair/.

———. n.d. 'App Store Review Guidelines - Apple Developer'. *Apple*. https://developer.apple.com/app-store/review/guidelines/#safety.

Arora, Payal. 2019. 'General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South'. *Surveillance & Society* 17 (5): 717–25. https://doi.org/10.24908/ss.v17i5.13307.

Auditor General of Ontario. 2018. *2018 Annual Report, Sec. 3.15, "Waterfront Toronto"*. 5 December. Queen's Park: Auditor General of Ontario. http://www.auditor.on.ca/en/content/annualreports/arbyyear/ar2018.html.

Austin, Lisa, and David Lie. 2021. 'Data Trusts and the Governance of Smart Environments: Lessons From the Failure of Sidewalk Labs' Urban Data Trust'. *Surveillance & Society* 19 (2): 255–61. https://doi.org/10.24908/ss.v19i2.14409.

Australian Competition and Consumer Commission. 2019. 'Digital Platforms Inquiry - Final Report'. 26 July. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

———. 2020a. *Agricultural Machinery: After-Sales Markets Discussion Paper*. Canberra: Australian Competition and Consumer Commission. 28 February. https://www.accc.gov.au/system/files/Agricultural%20machinery%20-%20After-sales%20markets%20-%20Discussion%20paper%20-%2028%20February%202020.pdf.

———. 2020b. 'Statement of Issues: Google LLC - Proposed Acquisition of Fitbit Inc'. *Australian Competition and Consumer Commission*. 18 June. https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%2018%20June%202020.pdf.

———. 2021. 'Better Access to Servicing and Repairs Needed in Agricultural Machinery Markets'. *Text: Australian Competition and Consumer Commission* (Blog), 4 May. https://www.accc.gov.au/media-release/better-access-to-servicing-and-repairs-needed-in-agricultural-machinery-markets.

AutoCare Association. n.d. 'Massachusetts Right to Repair'. https://www.autocare.org/government-relations/current-issues/right-to-repair.

Avant, Deborah D., Martha Finnemore, and Susan K. Sell. 2010. *Who Governs the Globe*? Cambridge: Cambridge University Press.

Baack, Stefan. 2015. 'Datafication and Empowerment: How the Open Data Movement Re-Articulates Notions of Democracy, Participation, and Journalism'. *Big Data & Society*, December, 1–11. https://doi.org/10.1177/2053951715594634.

Baker, Dean, Arjun Jayadev, and Joseph E. Stiglitz. 2017. 'Innovation, Intellectual Property, and Development: A Better Set of Approaches for the 21st Century'. AccessIBSA: Innovation & Access to Medicines in India, Brazil & South Africa. cepr.net/images/stories/reports/baker-jayadev-stiglitz-innovation-ip-development-2017-07.pdf.

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. https://doi.org/10.1086/674424.

Ball, Kirstie, and Lauren Snider, eds. 2013. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. New York: Routledge.

Balsillie, Jim. 2018. 'Sidewalk Toronto Has Only One Beneficiary, and It Is Not Toronto'. *The Globe and Mail*, 5 October. https://www.theglobeandmail.com/opinion/article-sidewalk-toronto-is-not-a-smart-city/.

Bamford, James. 1982. *The Puzzle Palace: Inside America's Most Secret Intelligence Organization*. New York: Penguin Books.

Banet, Catherine. 2018. 'Techno-Nationalism in the Context of Energy Transition'. In *Innovation in Energy Law and Technology: Dynamic Solutions for Energy Transitions*, edited by Donald Zillman, Lee Godden, LeRoy Paddock and Martha Roggenkamp, 74–100. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198822080.003.0005.

Banks, Timothy M. 2018. 'Will Sidewalk Labs' Civic Data Trust Hush Critics of Waterfront Toronto?' *Timothy M Banks* (Blog), 23 October. https://timothy-banks.com/2018/10/23/will-sidewalk-labs-civic-data-trust-hush-critics-of-waterfront-toronto/.

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

Bannerman, Sara. 2013. *The Struggle for Canadian Copyright: Imperialism to Internationalism, 1842–1871*. Vancouver: UBC Press.

Barlyn, Suzanne. 2018. 'John Hancock Will Only Sell Interactive Life Insurance With Fitness Data Tracking'. *Insurance Journal*, 19 September. https://www.insurancejournal.com/news/national/2018/09/19/501747.htm.

Basu, Arindrajit, Elonnai Hickok, and Aditya Singh Chawla. 2019. 'The Localization Gambit: Unpacking Policy Measures for Sovereign Control of Data in India. The Centre for Internet & Society'. 19 March. https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

Battiste, Marie. 2005. 'Indigenous Knowledge: Foundations for First Nations'. *WINHEC: International Journal of Indigenous Education Scholarship* 1: 1–17. https://journals.uvic.ca/index.php/winhec/article/view/19251.

BBC. 2020. 'French Covid App Relaunches to Bumpy Start'. *BBC News*, 23 October. https://www.bbc.com/news/technology-54660499.

Beede, Emma. 2020. 'Healthcare AI Systems That Put People at the Center'. *Google: The Keyword* (Blog), 25 April. https://blog.google/technology/health/healthcare-ai-systems-put-people-center/.

Beer, David. 2017. 'The Social Power of Algorithms'. *Information, Communication & Society* 20 (1): 1–13. https://doi.org/10.1080/1369118X.2016.1216147.

———. 2018. 'Envisioning the Power of Data Analytics'. *Information, Communication & Society* 21 (3): 465–79. https://doi.org/10.1080/1369118X.2017.1289232.

Bell, Daniel. 1976. *The Coming of Post-Industrial Society*. Reissue ed. New York: Basic Books.

Belsher, Adam. 2016. 'It's Time to Build Canada's 21st-Century Infrastructure'. *The Globe and Mail*, 26 July. https://www.canadianinnovators.org/newscentre/featured_news/its_time_to_build_canadas_21st_century_infrastructure.

Belz, Adam. 2020. 'For Tech-Weary Midwest Farmers, 40-Year-Old Tractors Now a Hot Commodity'. *Star Tribune*, 5 January. https://www.startribune.com/for-tech-weary-midwest-farmers-40-year-old-tractors-now-a-hot-commodity/566737082/.

Benjamin, Ruh. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. New York: Polity.

Benkler, Yochai. 2007. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press.

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York, NY: Oxford University Press.

Bennett, Colin. 2016. 'Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations'. *Canadian Journal of Law and Technology* 16 (2): 195–226.

———. 2022. 'Opinion: B.C. Privacy Ruling Over Political Party Data Collection is a Victory for Voters' Privacy'. *The Globe and Mail*, 22 March. https://www.theglobeandmail.com/opinion/article-bc-privacy-ruling-over-political-party-data-collection-is-a-victory/.

Berg, Jamie, Marianne Furrer, Ellie Harmon, Uma Rani, and M. Six Silberman. 2018. 'Digital Labour Platforms and the Future of Work: Towards Decent Work in the Online World'. *Report*. International Labour Organization. http://www.ilo.org/global/publications/books/WCMS_645337/lang--en/index.htm.

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

Bernards, Nick, and Malcolm Campbell-Verduyn. 2019. 'Understanding Technological Change in Global Finance Through Infrastructures'. *Review of International Political Economy* 26 (5): 773–89. https://doi.org/10.1080/09692290.2019.1625420.

Bernstien, Jaela. 2021. 'Canada's Museums Are Slowly Starting to Return Indigenous Artifacts'. *Macleans.ca*, 22 June. https://www.macleans.ca/culture/canadas-museums-are-slowly-starting-to-return-indigenous-artifacts/.

Bertuzzi, Luca. 2022. 'MEPs Try to Gain First-Mover Advantage on Right to Repair'. euractiv.com, 9 March. https://www.euractiv.com/section/digital/news/meps-try-to-gain-first-mover-advantage-on-right-to-repair/.

Biber, Eric, Sarah E. Light, J. B. Ruhl, and James Salzman. 2017. 'Regulating Business Innovation as Policy Disruption: From the Model T to Airbnb'. *Vanderbilt Law Review* 70 (5): 1561–626. https://scholarship.law.vanderbilt.edu/vlr/vol70/iss5/4/.

Bigo, Didier, Isin Engin, and Evelyn Ruppert. 2019. 'Data Politics'. In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert. Abingdon: Taylor & Francis.

Birch, Kean. 2020. 'Technoscience Rent: Toward a Theory of Rentiership for Technoscientific Capitalism'. *Science, Technology, & Human Values* 45 (1): 3–33. https://doi.org/10.1177/0162243919829567.

Birch, Kean, and Fabian Muniesa, eds. 2020. *Assetization: Turning Things into Assets in Technoscientific Capitalism.* Cambridge, MA: MIT Press.

Birhane, Abeba. 2021. 'Cheap AI'. In *Fake AI*, 41–52. Manchester: Meatspace Press.

Birnhack, Michael, and Niva Elkin-Koren. 2003. 'The Invisible Handshake: The Reemergence of the State in the Digital Environment'. *Virginia Journal of Law and Technology* 8 (6): 1–57. http://law.bepress.com/taulwps/art54.

Black, Julia. 2008. 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes'. *Regulation & Governance* 2 (2): 137–64. https://doi.org/10.1111/j.1748-5991.2008.00034.x.

Bloustein, Edward J. 1978. *Individual and Group Privacy*. New York: Routledge.

———. 2017. 'Group Privacy: The Right to Huddle'. In Edward J. Bloustein and Nathaniel J. Pallone, *Individual & Group Privacy,* 123–186. New York: Routledge.

Bode, Karl, and Matthew Gault. 2020. 'Sonos Makes It Clear: You No Longer Own the Things You Buy'. *Vice.com*, 22 January. https://www.vice.com/en/article/3a8dpn/sonos-makes-it-clear-you-no-longer-own-the-things-you-buy.

Bogost, Ian. 2022. 'The Internet is Just Investment Banking Now'. *The Atlantic*, 4 February. https://www.theatlantic.com/technology/archive/2022/02/future-internet-blockchain-investment-banking/621480/.

Boldrin, Michele, and David K. Levine. 2007. *Against Intellectual Monopoly*. Cambridge, UK: Cambridge University Press.

Bonafide, Christopher P., David T. Jamison, and Elizabeth E. Foglia. 2017. 'The Emerging Market of Smartphone-Integrated Infant Physiologic Monitors'. *JAMA* 317 (4): 353–54. https://doi.org/10.1001/jama.2016.19137.

Borgesius, Frederik J. Zuiderveen, Judith Möller, Sanne Kruikemeier, Ronan Ó. Fathaigh, Kristina Irion, Tom Dobber, Balazs Bodo, and Claes de Vreese. 2018. 'Online Political Microtargeting: Promises and Threats for Democracy'. *Utrecht Law Review* 14 (1): 82–96. https://doi.org/10.18352/ulr.420.

Borland, Kelsi Maree. 2020. 'An Update on Bill Gates' New Smart City in Arizona'. *globest.com*, 5 March. https://www.globest.com/2020/03/05/an-update-on-bill-gates-new-smart-city-in-arizona/.

Bourdieu, Pierre. 2013. *Outline of a Theory of Practice*. Cambridge, UK: Cambridge University Press.

Bovens, Mark, and Stavros Zouridis. 2002. 'From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control'. *Public Administration Review* 62 (2): 174–84. https://doi.org/10.1111/0033-3352.00168.

Bowker, Geoffrey C., and Susan Leigh Star. 2000. *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press.

boyd, danah, and Kate Crawford. 2012. 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon'. *Information, Communication & Society* 15 (5): 662–79. https://doi.org/10.1080/1369118X.2012.678878.

Bozikovic, Alex, 2017. 'Google's Sidewalk Labs signs deal for 'smart city' makeover of Toronto's waterfront'. *The Globe and Mail*, 17 October. https://www.theglobeandmail.com/news/toronto/google-sidewalk-toronto-waterfront/article36612387/

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001.

Braithwaite, John, and Peter Drahos. 2000. *Global Business Regulation*. Cambridge, UK: Cambridge University Press.

Brander, James A. 2007. 'Intellectual Property Protection as Strategic Trade Policy'. *Asia-Pacific Journal of Accounting & Economics* 14 (3): 195–217. https://doi.org/10.1080/16081625.2007.9720797.

Brass, Irina, Leonie Tanczer, Madeline Carr, and Jason Blackstock. 2017. 'Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things?' *Risk & Regulation* 33: 12–15. http://www.lse.ac.uk/accounting/CARR/pdf/Risk&Regulation/r&r-33/riskandregulation-33-web.pdf.

Brayne, Sarah. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford: Oxford University Press.

Breznitz, Dan. 2021. *Innovation in Real Places: Strategies for Prosperity in an Unforgiving World*. Oxford: Oxford University Press.

Bria, Francesca, Cristina Caffarra, Gregory Crawford, Wolfie Christl, Tomaso Duso, Johnny Ryan, and Tommaso Valletti. 2020. 'Europe Must Not Rush Google-Fitbit Deal'. *Politico*, 22 July. https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/.

Bronson, Kelly, and Irena Knezevic. 2016. 'Big Data in Food and Agriculture'. *Big Data & Society* 3 (1): 1–5. https://doi.org/10.1177/2053951716648174.

Bronson, Kelly, Sarah Rotz, and Adrian D'Alessandro. 2021. 'The Human Impact of Data Bias and the Digital Agricultural Revolution'. In Harvey S. James, Jr., ed, *Handbook on the Human Impact of Agriculture*, 119–137. Cheltenham: Edward Elgar Publishing. https://www.elgaronline.com/view/edcoll/9781839101731/9781839101731.00017.xml.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Bryan, Dick, Michael Rafferty, and Duncan Wigan. 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.

Buckley, Peter J., Roger Strange, Marcel P. Timmer, and Gaaitzen J. de Vries. 2022. 'Rent Appropriation in Global Value Chains: The Past, Present, and Future of Intangible Assets'. *Global Strategy Journal*. https://doi.org/10.1002/gsj.1438.

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

Burke, Peter. 2000. *A Social History of Knowledge: From Gutenberg to Diderot*. Cambridge, MA: Polity Press.

Burt, Jemima. 2018. 'Tractor-Hacking Farmers in the US Fight for Right to Repair'. *ABC News*, 21 February. https://www.abc.net.au/news/rural/2018-02-22/tractor-hacking-farmers-in-the-us-fight-for-right-to-repair/9470658.

Buttarelli, Giovanni. 2016. 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard'. *International Data Privacy Law* 6 (2): 77–8. https://doi.org/10.1093/idpl/ipw006.

Byrne, David. 2012. *How Music Works*. New York: Three Rivers Press.

Calo, Ryan, and Alex Rosenblat. 2017. 'The Taking Economy: Uber, Information, and Power'. *Columbia Law Review* 117 (6): 1623–90. http://www.jstor.org/stable/44392959.

Campbell, John L. 1998. 'Institutional Analysis and the Role of Ideas in Political Economy'. *Theory and Society* 27: 377–409. https://www.jstor.org/stable/657900.

Carbonell, Isabelle. 2016. 'The Ethics of Big Data in Big Agriculture'. *Internet Policy Review* 5 (1): 1–13. https://doi.org/10.14763/2016.1.405.

Cardoso, Tom, and Josh O'Kane. 2019. 'Sidewalk Labs Document Reveals Company's Early Vision for Data Collection, Tax Powers, Criminal Justice'. *The Globe and Mail*, 30 October. https://www.theglobeandmail.com/business/article-sidewalk-labs-document-reveals-companys-early-plans-for-data/.

Carmichael, Kevin. 2018. 'Google is as Big as Big Banks to Canada's Economy, But Before You Get Too Excited…'. *National Post*, 12 September. https://business.financialpost.com/news/economy/google-contributes-billions-to-canadas-economy-new-study-finds.

Carney, Terry. 2019. 'Robo-Debt Illegality: The Seven Veils of Failed Guarantees of the Rule of Law?' *Alternative Law Journal* 44 (1): 4–10. https://doi.org/10.1177/1037969X18815913.

———. 2020. 'Artificial Intelligence in Welfare: Striking the Vulnerability Balance'. *Monash University Law Review* 46 (2): 1–30.

Carolan, Michael. 2018. '"Smart" Farming Techniques as Political Ontology: Access, Sovereignty and the Performance of Neoliberal and Not-So-Neoliberal Worlds'. *Sociologia Ruralis* 58 (4): 745–64. https://doi.org/10.1111/soru.12202.

Carr, Madeline. 2015. 'Power Plays in Global Internet Governance'. *Millennium: Journal of International Studies* 43 (2): 640–59. https://doi.org/10.1177/0305829814562655.

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

Carr, Madeline, and Jose Tomas Llanos. 2022. 'Data'. In *Global Governance Futures*, edited by Thomas G. Weiss and Rorden Wilkinson, 286–98. Oxfordshire: Routledge.

Casalini, Francesca, and Javier López González. 2019. 'Trade and Cross-Border Data Flows'. 220. *OECD Trade Policy Papers*. Paris: OECD. http://dx.doi/org/10.1787/b2023a47-en.

Castells, Manuel. 1996. *The Rise of the Network Society. Vol. 1, The Information Age: Economy, Society and Culture*. Cambridge, UK: Blackwell.

———. 1997. *The Power of Identity. Vol. 2, The Information Age: Economy, Society and Culture*. Cambridge, UK: Blackwell.

———. 2009. *End of Millennium. Vol. 3, The Information Age: Economy, Society and Culture*. 2nd ed. Cambridge, UK: Blackwell.

———. 2015. *Networks of Outrage and Hope: Social Movements in the Internet Age*. 2nd ed. Cambridge, UK: Polity.

Cavalli, Olga, and Jan Aart Scholte. 2021. 'The Role of States in Internet Governance at ICANN'. In *Power and Authority in Internet Governance: Return of the State?*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 37–55. Abingdon: Routledge.

Cavoukian, Ann, and Khaled El Emam. 2014. *De-Identification Protocols: Essential for Protecting Privacy*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/resource/de-identification-protocols-essential-for-protecting-privacy/.

Cevolini, Alberto, and Elena Esposito. 2020. 'From Pool to Profile: Social Consequences of Algorithmic Prediction in Insurance'. *Big Data & Society* 7 (2): 1–11. https://doi.org/10.1177/2053951720939228.

Chamary, J. V. 2020. 'How Genetic Genealogy Helped Catch the Golden State Killer'. *Forbes*, 30 June. https://www.forbes.com/sites/jvchamary/2020/06/30/genetic-genealogy-golden-state-killer/.

Chamberlain, Elizabeth. 2022. 'Apple's Self-Repair Vision is Here, and It's Got a Catch'. *IFixit* (Blog), 30 April. https://www.ifixit.com/News/59239/apples-self-repair-vision-is-here-and-its-got-a-catch.

Chang, Ha-Joon. 2002. *Kicking Away the Ladder: Development Strategy in Historical Perspective.* London: Anthem Press.

Chen, Yujie, Zhifei Mao, and Jack Linchuan Qiu. 2018. *Super-Sticky Wechat and Chinese Society*. Bingley: Emerald Publishing Limited.

Chenou, Jean-Marie. 2021. 'Varieties of Digital Capitalism and the Role of the State in Internet Governance: A View From Latin America'. In *Power and Authority in Internet Governance: Return of the State?*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 195–218. Abingdon: Routledge.

Christl, Wolfie. 2017. 'Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions'. *Cracked Labs, Institute for Critical Digital Culture*. http://crackedlabs.org/en/corporate-surveillance.

Christl, Wolfie, and Sarah Spiekermann. 2016. *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Vienna: Facultas. http://crackedlabs.org/en/networksofcontrol.

Cioffi, John W., Martin F. Kenney, and John Zysman. 2022. 'Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century'. *New Political Economy* 27 (5): 820–836. https://doi.org/10.1080/13563467.2022.2027355.

Ciuriak, Dan. 2018a. *Digital Trade: Is Data Treaty-Ready?* 162. Centre for International Governance Innovation. https://www.cigionline.org/publications/digital-trade-data-treaty-ready/.

———. 2018b. 'From Digital Trade Wars to Governance Solutions: The G20 and the Digitally-Enabled Economy'. *SSRN Scholarly Paper*. Rochester, NY. https://papers.ssrn.com/abstract=3239892.

Ciuriak, Dan, and Maria Ptashkina. 2021. 'The Data-Driven Economy and the Role of the State'. In *Power and Authority in Internet Governance*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 76–94. Abingdon: Routledge.

Clarke, Warren. 2017. *A Worthwhile Intervention? The Potential Role for a Sovereign Patent Fund in Canada*. Waterloo: Centre for International Governance Innovation. https://www.cigionline.org/articles/worthwhile-intervention-potential-role-sovereign-patent-fund-canada/.

Climate FieldView. 2021. 'Climate FieldView™ Terms of Service'. *Climate FieldView*, 30 July. https://climate.com/fieldview-terms-of-service/.

Cohen, Julie E. 2019. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press.

Comor, Edward. 1996. *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*. New York: St. Martin's Press.

Conditt, Jess. 2019. 'Health and Beauty Tech Continues to Fail Pregnant Women'. *Engadget*, 11 January. https://www.engadget.com/2019-01-11-health-beauty-tech-pregnant-women-ignore-ces-2019.html.

Cooper, Richard N. 1980. *The Economics of Interdependence*. New York: Columbia University Press.

Cooper, Sam, and Roberta Bell. 2021. 'Toronto-Area Startup Switch Health Accused of Fumbling Canada's COVID-19 Border Testing'. *Global News*, 26 April. https://globalnews.ca/news/7783633/switch-health-delays-covid-testing/.

Copeland, Rob. 2019. 'Google's "Project Nightingale" Gathers Personal Health Data on Millions of Americans'. *Wall Street Journal*, 11 November. https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

Corbin, Bethany A. 2019. 'Digital Micro-Aggressions and Discrimination: Femtech and the "Othering" of Women'. *Nova Law Review* 44: 337.

Couldry, Nick, and Andreas Hepp. 2017. *The Mediated Construction of Reality*. Cambridge, UK: Polity.

Couldry, Nick, and Ulises A. Mejias. 2018. 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject'. *Television & New Media* 20 (4): 336–49. https://doi.org/10.1177/1527476418796632.

———. 2019. *The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, CA: Stanford University Press.

Couture, Stephane, and Sophie Toupin. 2019. 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?' *New Media & Society* 21 (10): 2305–22. https://doi.org/10.1177/1461444819865984.

Cox, Robert W. 1987. *Production, Power, and World Order: Social Forces in the Making of History*. New York: Columbia University Press.

———. 1996a. 'Social Forces, States, and World Orders: Beyond International Relations Theory'. In *Approaches to World Order*, edited by Robert W. Cox and Timothy J. Sinclair, 85–122. Cambridge: Cambridge University Press.

———. 1996b. 'Take Six Eggs': Theory, Finance, and the Real Economy in the Work of Susan Strange (1992)'. In *Approaches to World Order*, edited by Robert W. Cox and Timothy J. Sinclair, 174–88. Cambridge, UK: Cambridge University Press.

Crain, Matthew. 2018. 'The Limits of Transparency: Data Brokers and Commodification'. *New Media & Society* 20 (1): 88–104. https://doi.org/10.1177/1461444816657096.

———. 2021. *Profit Over Privacy: How Surveillance Advertising Conquered the Internet*. Minneapolis: University of Minnesota Press.

Cranor, Lorrie Faith. 2012. 'Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice'. *Journal on Telecommunications and High Technology Law* 10: 273–307.

Crawford, Kate. 2021. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT: Yale University Press.

Crawford, Kate, Jessa Lingel, and Tero Karppi. 2015. 'Our Metrics, Ourselves: A Hundred Years of Self-Tracking From the Weight Scale to the Wrist Wearable Device'. *European Journal of Cultural Studies* 18 (4–5): 479–96. https://doi.org/10.1177/1367549415584857.

Crawford, Kate, Kate Miltner, and Mary L. Gray. 2014. 'Critiquing Big Data: Politics, Ethics, Epistemology'. *International Journal of Communications* 8: 1663–72. https://ijoc.org/index.php/ijoc/article/view/2167.

Crawford, Kate, and Tarleton Gillespie. 2016. 'What is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint'. *New Media & Society* 18 (3): 410–28. https://journals.sagepub.com/doi/10.1177/1461444814543163.

Creemers, Rogier. 2022. 'China's Emerging Data Protection Framework'. *Journal of Cybersecurity* 8 (1): 1–22. https://doi.org/10.1093/cybsec/tyac011.

Cross, Miriam. 2022. 'How Amazon, Apple, Facebook, Google Are Infiltrating Financial Services'. *American Banker*, 29 March. https://www.americanbanker.com/list/how-amazon-apple-facebook-google-are-infiltrating-financial-services.

Cummings, Mary. 2004. 'Automation Bias in Intelligent Time Critical Decision Support Systems'. In *AIAA 1st Intelligent Systems Technical Conference*. Infotech@Aerospace Conferences, American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2004-6313.

Curzon, James, Tracy Ann Kosa, Rajen Akalu, and Khalil El-Khatib. 2021. 'Privacy and Artificial Intelligence'. *IEEE Transactions on Artificial Intelligence*, April, 96-108. https://doi.org/10.1109/TAI.2021.3088084.

Cusumano, Michael A., Yiorgos Mylonadis, and Richard S. Rosenbloom. 1992. 'Strategic Maneuvering and Mass-Market Dynamics: The Triumph of VHS Over Beta'. *The Business History Review* 66 (1): 51–94. https://doi.org/10.2307/3117053.

Cutler, A. Claire, Virginia Haufler, and Tony Porter. 1999. *Private Authority and International Affairs*. Albany: SUNY Press.

Dai, Xin. 2020. 'Toward a Reputation State: A Comprehensive View of China's Social Credit System Project'. In *Social Credit Rating: Reputation Und Vertrauen Beurteilen*, edited by Oliver Everling, 139–63. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-29653-7_7.

———. 2021. 'Toward a Reputation State: The Social Credit System Project of China'. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193577.

Daly, Angela. 2021. 'Neoliberal Business-As-Usual or Post-Surveillance Capitalism With European Characteristics? The EU's General Data Protection Regulation in a Multipolar Internet'. In *Infrastructure: A Critique of the New in a Multipolar World*, edited by Rolien Hoyng and Gladys Pak Lei Chong, 66–95. East Lansing, MI: Michigan State University Press.

Daly, Angela, S. Kate Devitt, and Monique Mann, eds. 2019. *Good Data*. Amsterdam: Institute of Network Cultures.

Daniels, Jessie. 2013. 'Race and Racism in Internet Studies: A Review and Critique'. *New Media & Society* 15 (5): 695–719. https://doi.org/10.1177/1461444812462849.

Dastin, Jeffrey. 2018. 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women'. *Reuters*, 10 October. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

Daum, Jeremy. 2019. 'Untrustworthy: Social Credit Isn't What You Think It Is'. *Verfassungsblog* (Blog), 27 June. https://verfassungsblog.de/untrustworthy-social-credit-isnt-what-you-think-it-is/.

de Beer, Jeremy. 2020. *International Intellectual Property After the New NAFTA*. 235. Waterloo: Centre for International Governance Innovation. https://www.cigionline.org/publications/international-intellectual-property-after-new-nafta/.

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.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*. Plattsburgh, NY: Signal.

———. 2020. *Reset: Reclaiming the Internet for Civil Society*. Toronto: House of Anansi Press.

Delacroix, Sylvie, and Neil D. Lawrence. 2019. 'Bottom-Up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance'. *International Data Privacy Law* 9 (4): 236–52. https://doi.org/10.1093/idpl/ipz014.

Demarais, Agathe. 2022. 'How the U.S.-Chinese Technology War is Changing the World'. *Foreign Policy* (Blog), 19 November. https://foreignpolicy.com/2022/11/19/demarais-backfire-sanctions-us-china-technology-war-semiconductors-export-controls-biden/.

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

DeNardis, Laura, and Mark Raymond. 2017. 'The Internet of Things as a Global Policy Frontier'. *UC Davis Law Review* 51: 475–97.

Dencik, Lina, Arne Hintz, and Jonathan Cable. 2016. 'Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism'. *Big Data & Society* 3 (2): 1–12. https://doi.org/10.1177/2053951716679678.

———. 2019. 'Towards Data Justice: Bridging Anti-Surveillance and Social Justice Activism'. In *Data Politics*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 167–86. New York: Routledge.

Dencik, Lina, Arne Hintz, Joanna Redden, and Harry Warne. 2018. *Data Scores as Governance: Investigating the Uses of Citizen Scoring in Public Services - Project*

Report. Cardiff University, UK: Data Justice Lab. https://datajusticelab.org/data-scores-as-governance/.

Dencik, Lina, and Javier Sanchez-Monedero. 2022. 'Data Justice'. *Internet Policy Review* 11 (1): 1–11. https://doi.org/10.14763/2022.1.1615.

Department of Finance Canada. 2022a. 'A Plan to Grow Our Economy and Make Life More Affordable (Federal Budget 2022)'. Government of Canada. https://budget.gc.ca/2022/pdf/budget-2022-en.pdf.

———. 2022b. 'News Release: Government of Canada Releases Budget 2022'. Government of Canada, 7 April. https://www.canada.ca/en/department-finance/news/2022/04/government-of-canada-releases-budget-2022.html.

Desai, Pranav N. 2007. 'Traditional Knowledge and Intellectual Property Protection: Past and Future'. *Science and Public Policy* 34 (3): 185–97. https://doi.org/10.3152/030234207X213995.

Dingman, Shane. 2017. 'With Toronto, Alphabet Looks to Revolutionize City-Building'. *The Globe and Mail*, 17 October. https://www.theglobeandmail.com/report-on-business/with-toronto-alphabet-looks-to-revolutionize-city-building/article36634779/.

Dobson, Wendy, Julia Tory, and Daniel Trefler. 2017. 'NAFTA Modernization: A Canadian Perspective'. In *A Positive NAFTA Renegotiation*, edited by Fred Bergsten, 36–49. Washington, DC: Petersen Institute for International Economics.

Dobush, Grace. 2020. 'Uber's Real Advantage is Data'. *Marker* (Blog), 23 April. https://marker.medium.com/ubers-real-advantage-is-data-e54984ff524c.

Doctoroff, Daniel L. 2016. 'Reimagining Cities From the Internet Up'. Sidewalk Labs (Blog), 30 November. https://medium.com/sidewalk-talk/reimagining-cities-from-the-internet-up-5923d6be63ba.

———. 2019. 'Testimony'. House of Commons Standing Committee on Access to Information, Privacy and Ethics, 42nd Parliament, 1st session, 2 April. Ottawa, ON. https://www.ourcommons.ca/DocumentViewer/en/42-1/ethi/meeting-141/evidence.

Doern, G. Bruce, and Markus Sharaput. 2000. *Canadian Intellectual Property: The Politics of Innovating Institutions and Interests*. Toronto: University of Toronto Press.

Dolber, Brian, Michelle Rodino-Colocino, Chenjerai Kumanyika, and Todd Wolfson, eds. 2021. *The Gig Economy: Workers and Media in the Age of Convergence*. London, New York: Routledge.

Domingos, Pedro. 2012. 'A Few Useful Things to Know About Machine Learning'. *Communications of the ACM* 55 (10). https://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf.

Doran, Matthew. 2020. 'Federal Government Ends Robodebt Class Action With Settlement Worth $1.2 Billion'. *ABC News*, 16 November. https://www.abc.net.au/news/2020-11-16/government-response-robodebt-class-action/12886784.

Dosi, Giovanni, and Joseph E. Stiglitz. 2014. 'The Role of Intellectual Property Rights in the Development Process, With Some Lessons From Developed Countries: An Introduction'. In *Intellectual Property Rights: Legal and Economic Challenges for Development*, edited by Mari Cimoli, Giovanni Dosi, Keith E. Maskus, Jerome H. Reichman, and Joseph E. Stiglitz, 1–53. Oxford: Oxford University Press.

Döttling, Robin, and Enrico C. Perotti. 2019. 'Secular Trends and Technological Progress'. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.2996998.

Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock, and Bridget Harris. 2018. 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms'. *Feminist Media Studies* 18 (4): 609–25. https://doi.org/10.1080/14680777.2018.1447341.

Drahos, Peter. 1995. 'Information Feudalism in the Information Society'. *The Information Society* 11 (3): 209–22. https://doi.org/10.1080/01972243.1995.9960193.

———. 1996. *A Philosophy of Intellectual Property*. Aldershot: Dartmouth.

———. 2021. *Survival Governance*. Oxford: Oxford University Press.

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

Drezner, Daniel W. 2005. 'Globalization, Harmonization, and Competition: The Different Pathways to Policy Convergence'. *Journal of European Public Policy* 12 (5): 841–59. https://doi.org/10.1080/13501760500161472.

———. 2021. 'Introduction: The Uses and Abuses of Weaponized Interdependence'. In *The Uses and Abuses of Weaponized Interdependence*, edited by Daniel W. Drezner, Henry Farrell and Abraham L. Newman, 1–16. Washington, DC: Brookings Institution.

Duan, Charles. 2016. 'Roundtable Discussion: Will Technology Make Ownership Obsolete?'. Presented at the Future of Ownership, Washington, DC, 25 October. https://slate.com/technology/2016/10/will-technology-make-ownership-obsolete-a-future-tense-event-recap.html.

Dunne, Niamh. 2021. 'Platforms as Regulators'. *Journal of Antitrust Enforcement* 9 (2): 244–69. https://doi.org/10.1093/jaenfo/jnaa052.

Durán, Juan I., Rainer Reisenzein, and José-Miguel Fernández-Dols. 2017. 'Coherence Between Emotions and Facial Expressions: A Research Synthesis'. In *The Science of Facial Expression*. New York: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190613501.003.0007.

Durand, Cédric, and William Milberg. 2020. 'Intellectual Monopoly in Global Value Chains'. *Review of International Political Economy* 27 (2): 404–29. https://doi.org/10.1080/09692290.2019.1660703.

Dutfield, Graham, and Uma Suthersanen. 2008. *Global Intellectual Property Law*. Um. Cheltenham: Edward Elgar Publishing.

Ecker, Ullrich K. H., Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa K. Fazio, Nadia Brashier, Panayiota Kendeou, Emily K. Vraga, and Michelle A. Amazeen. 2022. 'The Psychological Drivers of Misinformation Belief and Its Resistance to Correction'. *Nature Reviews Psychology* 1 (1): 13–29. https://doi.org/10.1038/s44159-021-00006-y.

Edwards, Lillian. 2016. 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective'. *European Data Protection Law Review* 2 (1): 28–58. https://doi.org/10.21552/EDPL/2016/1/6.

———. 2018. 'Data Protection: Enter the General Data Protection Regulation'. In *Law, Policy and the Internet*, edited by Lillian Edwards, 77–118. Oxford: Hart Publishing.

Ekman, Elle. 2019. 'Here's One Reason the U.S. Military Can't Fix Its Own Equipment'. *The New York Times*, 20 November. https://www.nytimes.com/2019/11/20/opinion/military-right-to-repair.html.

Eubanks, Virginia. 2014. 'Want to Predict the Future of Surveillance? Ask Poor Communities.' *The American Prospect*, 15 January. https://prospect.org/api/content/36656b9e-c446-5205-9257-0120f64aabdb/.

———. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

European Commission. 2017. 'Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service - Factsheet'. *European Commission Official Webpage*, 27 June. https://ec.europa.eu/commission/presscorner/detail/es/MEMO_17_1785.

———. 2018. 'Artificial Intelligence for Europe'. *COM(2018) 237 Final*. Brussels: European Commission. https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe.

———. 2020. 'Mergers: Commission Clears Acquisition of Fitbit by Google'. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

European Parliament. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA Relevance)*. *OJ L*. Vol. 119. http://data.europa.eu/eli/reg/2016/679/oj/eng.

Evans, Dayna. 2021. 'Philly Learned the Hard Way to Pick Its Vaccine Distributors Carefully'. *Bloomberg Businessweek*, 30 June. https://www.bloomberg.com/news/features/2021-06-30/philly-fighting-covid-scandal-how-the-vaccine-distribution-partnership-failed.

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 (June): 5–17. https://doi.org/10.18601/16571959.n23.01.

Farrell, Maria. 2020. 'The Prodigal Techbro'. *The Conversationalist*, 6 March 2020. https://conversationalist.org/2020/03/05/the-prodigal-techbro/.

Federal Communications Commission. 2012. 'On Google Inc.' *Federal Communications Commission*. 13 April. https://assets.documentcloud.org/documents/351298/fcc-report-on-googles-street-view.pdf.

Federal Trade Commission. 2014. *Data Brokers: A Call for Transparency and Accountability: A Report of the Federal Trade Commission*. Washington, DC: Federal Trade Commission. May. http://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

———. 2021a. *Nixing the Fix: An FTC Report to Congress on Repair Restrictions*. Washington, DC: Federal Trade Commission. May. https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

———. 2021b. 'FTC Finalizes Order With Flo Health, a Fertility-Tracking App That Shared Sensitive Health Data With Facebook, Google, and Others'. 22 June. https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

———. 2021c. 'FTC to Ramp Up Law Enforcement Against Illegal Repair Restrictions'. 21 July. http://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-ramp-law-enforcement-against-illegal-repair-restrictions.

Feldman, Nina. 2022. 'Philly Fighting COVID CEO Doroshin Banned From Working in Pa.' *WHYY PBS*, 11 February. https://whyy.org/articles/philly-fighting-covid-andrei-doroshin-ag-shapiro-complaint/.

Feldstein, Steven. 2019. *The Global Expansion of AI Surveillance*. New York: Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

Feliciano Reyes, Juliana, Ellie Silverman, Ellie Rushing, and Oon Goodin-Smith. 2021. 'How Philly Fighting COVID's Vaccine Success Story Quickly Crumbled'. *The Philadelphia Inquirer*, 31 January. https://www.inquirer.com/health/coronavirus/philly-fighting-covid-vaccine-signup-andrei-doroshin-20210131.html.

Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. 'Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control With Digital Contact Tracing'. *Science* 368 (6491). https://doi.org/10.1126/science.abb6936.

Fife, Robert, and Steven Chase. 2021. 'Alberta Calls for National Security Rules for Academics to Prevent Intellectual Property Transfer to China'. *The Globe and Mail*, 25 May. https://www.theglobeandmail.com/politics/article-alberta-calls-for-national-security-rules-for-academics-to-prevent/.

Financial Stability Board. 2022. *Assessment of Risks to Financial Stability From Crypto-Assets*. Basel: Financial Stability Board. https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/.

First Nations Information Governance Centre (FNIGC). 2016. 'Pathways to First Nations' Data and Information Sovereignty'. In *Indigenous Data Sovereignty: Toward an Agenda*, edited by Tahu Kukutai and John Taylor, 139–56. Canberra: ANU Press.

Flonk, Daniëlle. 2021. 'Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control'. *International Affairs* 97 (6): 1925–44. https://doi.org/10.1093/ia/iiab146.

Floridi, Luciano. 2014. 'Open Data, Data Protection, and Group Privacy'. *Philosophy & Technology* 27 (1): 1–3. https://doi.org/10.1007/s13347-014-0157-8.

Forsyth, Miranda, and Blayne Haggart. 2014. 'The False Friends Problem for Foreign Norm Transplantation in Developing Countries'. *Hague Journal on the Rule of Law* 6 (2): 202–29. https://doi.org/10.1017/S1876404514001092.

Forti, Vanessa, Cornelis P. Balde, Ruediger Kuehr, and Garam Bel. 2020. *The Global E-Waste Monitor 2020: Quantities, Flows and the Circular Economy Potential*. Bonn: United Nations University/United Nations Institute for Training and Research, International Telecommunication Union, and International Solid Waste Association. https://collections.unu.edu/view/UNU:7737.

Fortune Business Insights. 2022. 'Internet of Things [IoT] Market Size, Share & Trends, 2022–2029'. FBI100307. *Fortune Business Insights*. https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307.

Foster, John Bellamy, and Robert W. McChesney. 2014. 'Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age'. *Monthly Review* 66 (3). https://monthlyreview.org/2014/07/01/surveillance-capitalism/.

Foucault, Michel. 1980. *Power and Knowledge: Selected Interviews and Other Writings 1972–1977*. New York: Vintage Press.

Franks, Mary Anne. 2019. *The Cult of the Constitution:* Palo Alto, CA: Stanford University Press.

Fuchs, Christian. 2008. *Internet and Society: Social Theory in the Information Age*. Abingdon: Routledge.

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

Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. 1st ed. New York: Oxford University Press.

Gartenberg, Chaim. 2020. 'European Parliament Vote Takes Another Big Step toward "Right to Repair" Rules'. *The Verge*, 25 November. https://www.theverge.com/2020/11/25/21719701/european-parliament-right-to-repair-resolution-hardware-eu-commission-2021.

Gault, Matthew. 2019. 'After Being Sold to a VC Firm, This $899 IoT Robot Will Soon Brick Itself'. *Vice.com*, 4 March. https://www.vice.com/en/article/wjm73w/after-being-sold-to-a-vc-firm-this-dollar899-iot-robot-will-soon-brick-itself.

Gehl, Robert W., and Sean T. Lawson. 2022. *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication*. Cambridge, MA: MIT Press.

Geist, Michael. 2020a. 'Why I Installed the COVID Alert App'. *michaelgeist.ca* (Blog), 2 August. https://www.michaelgeist.ca/2020/08/why-i-installed-the-covid-alert-app/.

———. 2020b. 'Four Million Downloads and Counting: Everyone Should Install the COVID Alert App'. *michaelgeist.ca* (Blog), 9 October. https://www.michaelgeist.ca/2020/10/four-million-downloads-and-counting-everyone-should-install-the-covid-alert-app/.

———. 2020c. 'What You Need to Know About the COVID Alert App'. *michaelgeist.ca* (Blog), 4 December. https://www.michaelgeist.ca/2020/12/what-you-need-to-know-about-the-covid-alert-app/.

Gerard, David. 2020. *Libra Shrugged: How Facebook Tried to Take Over the Money*. David Gerard.

Gereffi, Gary. 2011. 'Global Value Chains and International Competition'. *The Antitrust Bulletin* 56 (1): 37–56. https://doi.org/10.1177/0003603X1105600104.

———. 2014. 'Global Value Chains in a Post-Washington Consensus World'. *Review of International Political Economy* 21 (1): 9–37. https://doi.org/10.1080/09692290.2012.756414.

Germain, Randall D., and Michael Kenny. 1998. 'Engaging Gramsci: International Relations Theory and the New Gramscians'. *Review of International Studies* 24 (1): 3–21. http://www.jstor.org/stable/20097503.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Redwood City: Stanford University Press.

Gillespie, Tarleton. 2010. 'The Politics of "Platforms"'. *New Media & Society* 12 (3): 347–64. https://doi.org/10.1177/1461444809342738.

———. 2014. 'The Relevance of Algorithms'. In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, 167–93. Cambridge, MA: MIT Press.

———. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press.

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

Glaeser, D. 1987. *The Green Revolution Revisited: Critique and Alternatives*. Abingdon: Routledge.

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

Glasius, Marlies, and Marcus Michaelsen. 2018. 'Illiberal and Authoritarian Practices in the Digital Sphere'. *International Journal of Communication* 12: 3795–3813. https://ijoc.org/index.php/ijoc/article/view/8536/2458.

Gold, E. Richard, Jean-Frédéric Morin, and Erica Shadeed. 2019. 'Does Intellectual Property Lead to Economic Growth? Insights From a Novel IP Dataset'. *Regulation & Governance* 13 (1): 107–24. https://doi.org/10.1111/rego.12165.

Goldenfein, Jake, and Monique Mann. 2022. 'Tech Money in Civil Society: Whose Interests Do Digital Rights Organisations Represent?' *Cultural Studies* 1–35. https://doi.org/10.1080/09502386.2022.2042582.

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

Goodman, Ellen P., and Julia Powles. 2019. 'Urbanism Under Google: Lessons From Sidewalk Toronto'. *Fordham Law Review* 88 (2): 457–98.

Graber, Christoph Beat. 2015. 'Tethered Technologies, Cloud Strategies and the Future of the First Sale/Exhaustion Defence in Copyright Law'. *Queen Mary Journal of Intellectual Property* 5 (4): 389–408. https://doi.org/10.5167/uzh-119963.

Grabher, Gernot, and Jonas König. 2020. 'Disruption, Embedded: A Polanyian Framing of the Platform Economy'. *Sociologica* 14 (1): 95–118. https://doi.org/10.6092/issn.1971-8853/10443.

Grabosky, Peter. 2013. 'Beyond Responsive Regulation: The Expanding Role of Non-State Actors in the Regulatory Process'. *Regulation & Governance* 7 (1): 114–23. https://doi.org/10.1111/j.1748-5991.2012.01147.x.

Granick, Jennifer Stisa. 2017. *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It*. Cambridge: Cambridge University Press.

Gray, Jeff. 2018. 'Cracks in Sidewalk Labs' Toronto Waterfront Plan After Fanfare'. *The Globe and Mail*, 23 February. https://www.theglobeandmail.com/news/toronto/cracks-appear-in-sidewalk-labs-plan-afterfanfare/article38103236/.

Greenfield, Adam. 2018. 'China's Dystopian Tech Could Be Contagious'. *The Atlantic*, 14 February. https://www.theatlantic.com/technology/archive/2018/02/chinas-dangerous-dream-of-urban-control/553097/.

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

Gribakov, Andrei. 2019. 'Cross-Border Privacy Rules in Asia: An Overview'. *Lawfareblog* (Blog), 3 January. https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

Grisdale, Sean. 2021. 'Mobilizing the Platform Economy: Regulating Short-Term Stays in Toronto'. In *The Platform Economy and the Smart City: Technology and the Transformation of Urban Policy*, editedby Austin Zwick and Zachary Spicer, 15–44. Montreal and Kingston: McGill-Queen's University Press.

Guo, Eileen, and Karen Hao. 2020. 'This Is the Stanford Vaccine Algorithm That Left Out Frontline Doctors'. *MIT Technology Review*, 21 December. https://www.technologyreview.com/2020/12/21/1015303/stanford-vaccine-algorithm/.

Haggart, Blayne. 2011. 'International Copyright Treaties and Digital Works: Implementation Issues in Canada and Mexico'. *Australian Journal of Communication* 38 (3): 33–46.

———. 2014. *Copyfight: The Global Politics of Digital Copyright Reform*. Toronto: University of Toronto Press.

———. 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 (2017): 176–203. https://doi.org/10.5325/jinfopoli.7.2017.0176

———. 2018a. ''New economic models, new forms of state: The rise of the "info-imperium state"'. In *Kritika: Essays on Intellectual Property*, Volume 3, edited by Hanns Ullrich, Peter Drahos, and Gustavo Ghidini, 159-187. Cheltenham: Edward Elgar. https://doi.org/10.4337/9781788971164.00014.

———. 2018b. 'The Government's Role in Constructing the Data-Driven Economy'. In *Data Governance in the Digital Age*, edited by Rohinton Medhora, 20–25. Waterloo: Centre for International Governance Innovation. https://www.cigionline.org/publications/data-governance-digital-age.

———. 2019a. 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, S. Zuboff (2018) (Book Review)'. *Journal of Digital Media & Policy* 10 (2): 229–43. https://doi.org/10.1386/jdmp.10.2.229_5.

———. 2019b. 'Liveblogging Sidewalk Labs' Master Innovation and Development Plan, Entry 5: Enter the Gondola! Every Sidewalk Labs Promise to Toronto in Its Project Vision Document, and the One Thing They Won't Do'. *Blayne Haggart's Orangespace* (Blog), 19 July 2019. https://blaynehaggart.com/2019/07/19/liveblogging-sidewalk-labs-master-innovation-and-development-plan-entry-5-enter-the-gondola-every-sidewalk-labs-promise-to-toronto-in-its-project-vision-document-and-the-one-thing-they-wo/.

———. 2019c. 'Taking knowledge seriously: Toward an International Political Economy theory of knowledge governance.' In *Information, Technology and*

Control in a Changing World: Understanding Power Structures in the 21st Century, edited by Blayne Haggart, Kathryn Henne and Natasha Tusikov, 25-51, New York: Palgrave-Macmillan.

———. 2020a. 'Global Platform Governance and the Internet-Governance Impossibility Theorem'. *Journal of Digital Media & Policy* 11 (3): 321–39. https://doi.org/10.1386/jdmp_00028_1.

———. 2020b. 'Canada's COVID Alert App is a Case of Tech-Driven Bad Policy Design'. *The Conversation*, 13 August. http://theconversation.com/canadas-covid-alert-app-is-a-case-of-tech-driven-bad-policy-design-144448.

———. 2022. 'Canada and the Global Knowledge Economy: Between Knowledge Feudalism and Digital Economic Nationalism'. In *Canada and Great Power Competition: Canada Among Nations 2021*, edited by David Carment, Laura Macdonald, and Jeremy Paltiel, 169–190. New York: Palgrave Macmillan.

Haggart, Blayne, and Clara Iglesias Keller. 2021. 'Democratic Legitimacy in Global Platform Governance'. *Telecommunications Policy* 45 (6): 102152. https://doi.org/10.1016/j.telpol.2021.102152.

Haggart, Blayne, Jan Aart Scholte, and Natasha Tusikov. 2021. 'Introduction: Return of the State?' In *Power and Authority in Internet Governance: Return of the State?*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 1–12. Abingdon: Routledge.

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): 1–16. https://doi.org/10.1080/01972243.2017.1294128.

Haggart, Blayne, Natasha Tusikov, and Jan Aart Scholte, eds. 2021. *Power and Authority in Internet Governance: Return of the State?* Abingdon: Routledge.

Hailu, Ruth. 2019. 'Fitbits and Other Wearables May Not Accurately Track Heart Rates in People of Color'. *STAT*, 24 July. https://www.statnews.com/2019/07/24/fitbit-accuracy-dark-skin/.

Halbert, Debora. 2016. 'Intellectual Property Theft and National Security: Agendas and Assumptions'. *The Information Society* 32 (4): 256–68. https://doi.org/10.1080/01972243.2016.1177762.

———. 2019. 'Weaponising Copyright: Cultural Governance and Regulating Speech in the Knowledge Economy'. In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 165–86. Cham: Palgrave Macmillan.

Hallinan, Dara, and Paul de Hert. 2017. 'Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law'. In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bart van der Sloot, 175–96. Cham: Springer.

Harb, Jenna, and Kathryn Henne. 2019. 'Disinformation and Resistance in the Surveillance of Indigenous Protesters'. In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 187–212. Cham: Palgrave Macmillan.

Harding, Luke. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man*. New York: Vintage Press.

Hardinges, Jack. 2018. 'Defining a "Data Trust"'. *Open Data Institute* (Blog), 19 October. https://theodi.org/article/defining-a-data-trust/.

Harris, Shane. 2015. *@War: The Rise of the Military-Internet Complex*. New York: Eamon Dolan/Mariner Books.

Hartt, Maxwell, Austin Zwick, and Brian Webb. 2021. 'The Promise and the Peril of the Smart City'. In *The Platform Economy and the Smart City: Technology and the Transformation of Urban Policy*, edited by Zachary Spicer and Austin Zwick, 213-228. Montreal: McGill-Queen's University Press.

Hartzog, Woodrow, and Evan Selinger. 2016. 'The Internet of Heirlooms and Disposable Things'. *North Carolina Journal of Law & Technology* 17 (4): 581. https://scholarship.law.unc.edu/ncjolt/vol17/iss4/2.

Harwell, Drew. 2018. 'The Accent Gap: How Amazon's and Google's Smart Speakers Leave Certain Voices behind'. *Washington Post*, 19 July. https://www.washingtonpost.com/graphics/2018/business/alexa-does-not-understand-your-accent/.

———. 2019. 'Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?' *Washington Post*, 10 April. https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

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

Hayward, Keith J., and Matthijs M. Maas. 2021. 'Artificial Intelligence and Crime: A Primer for Criminologists'. *Crime, Media, Culture* 17 (2): 209–33. https://doi.org/10.1177/1741659020917434.

He, Shuhan, Debbie Lai, and Jarone Lee. 2021. 'The Medical Right to Repair: The Right to Save Lives'. *The Lancet* 397 (10281): 1260–61. https://doi.org/10.1016/S0140-6736(21)00445-1.

Health Canada. 2020a. 'COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment'. *Assessments*, 29 October. https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy/assessment.html.

———. 2020b. 'COVID Alert Privacy Notice (Google-Apple Exposure Notification)'. *Education and Awareness*, 30 October. https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/privacy-policy.html.

Helleiner, Eric. 2019. 'Conservative Economic Nationalism and the National Policy: Rae, Buchanan and Early Canadian Protectionist Thought'. *Canadian Journal of Political Science* 52 (3): 521–38. https://doi.org/10.1017/S0008423918001026.

Heller, Nathan. 2017. 'Estonia, the Digital Republic'. *The New Yorker*, 11 December. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

Henman, Paul. 2019. 'Of Algorithms, Apps and Advice: Digital Social Policy and Service Delivery'. *Journal of Asian Public Policy* 12 (1): 71–89. https://doi.org/10.1080/17516234.2018.1495885.

Henne, Kathryn. 2019. 'Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India'. In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 223–45. Cham: Palgrave-Macmillan. https://doi.org/10.1007/978-3-030-14540-8_11.

Hildebrandt, Mireille. 2008a. 'Defining Profiling: A New Type of Knowledge?' In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 17–45. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-6914-7_2.

———. 2008b. 'Profiling and the Identity of the European Citizen'. In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 303–43. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-6914-7_15.

Hildebrandt, Mireille, and Serge Gutwirth, eds. 2008. *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Dordrecht: Springer Netherlands. http://link.springer.com/book/10.1007/978-1-4020-6914-7

Hill, Brian, Jasmine Pazzano, Andrew Russell, Roberta Bell, Sam Cooper, and Jigar Patel. 2021. 'Company Behind COVID-19 Border Testing Says Medical Professionals "Always" Oversee Testing'. *Global News*, 28 May. https://globalnews.ca/news/7903029/switch-health-covid-19-border-testing-parliament/.

Hill, Jonah. 2014. 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders'. Presented at the Conference on the Future of Cyber Governance, The Hague Institute for Global Justice, 1 May.

Hintz, Arne, Lina Dencik, and Karin Wahl-Jorgensen. 2018. *Digital Citizenship in a Datafied Society*. Cambridge: Polity Press.

Ho, Filum. 2021. 'New Right-to-Repair Rules Radically Broaden Car Maintenance Options'. *Daily Maverick*, 18 February. https://www.dailymaverick.co.za/article/2021-02-18-new-right-to-repair-rules-radically-broaden-car-maintenance-options/.

Hoen, Ellen F. M. T. 2009. *The Global Politics of Pharmaceutical Monopoly Power: Drug Patents, Access, Innovation and the Application of the WTO Doha Declaration on TRIPS and Public Helath*. Diemen: AMB.

Hoofnagle, Chris Jay. 2018. 'Designing for Consent'. *Journal of European Consumer and Market Law* 7 (4): 162–71. https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/7.4/EuCML2018033.

Horan, Caley. 2021. *Insurance Era: Risk, Governance, and the Privatization of Security in Postwar America*. Chicago, IL: University of Chicago Press.

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

Horton, David. 2010. 'The Shadow Terms: Contract Procedure and Unilateral Amendments'. *UCLA Law Review* 605 (3): 605–667.

Hruska, Joel. 2017. 'Investors Backing Juicero and Its $400, DRM-Laden Juicer Surprised to Discover They Were Fleeced'. *Extreme Tech*, 20 April. https://www.extremetech.com/electronics/248034-investors-backing-juicero-400-drm-laden-juicer-surprised-discover-fleeced.

Hu, Jane C. 2022. 'Do You Really Need to Worry About Your Period Tracking App in a Post-Roe World?' *Slate*, 10 May 2022. https://slate.com/technology/2022/05/period-tracking-apps-privacy-roe-abortion.html.

Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. 2021. 'Data Sovereignty: A Review'. *Big Data & Society* 8 (1): 1–17. https://doi.org/10.1177/2053951720982012.

Hutchinson, Christophe Samuel. 2022. 'Potential Abuses of Dominance by Big Tech Through Their Use of Big Data and AI'. *Journal of Antitrust Enforcement*, March. https://doi.org/10.1093/jaenfo/jnac004.

Hwang, Tim. 2020. *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*. New York: FSG Originals.

Igo, Sarah E. 2018. *The Known Citizen: A History of Privacy in Modern America*. Cambridge, MA: Harvard University Press.

Innis, Harold. 1950. *Empire and Communications*. Toronto: University of Toronto Press.

Innovation, Science and Economic Development Canada. 2021. 'About Canada's Innovation Superclusters Initiative'. *Government of Canada*, 22 June. https://ised-isde.canada.ca/site/innovation-superclusters-initiative/en/about-canadas-innovation-superclusters-initiative.

Irani, Lilly. 2015a. 'Difference and Dependence among Digital Workers: The Case of Amazon Mechanical Turk'. *South Atlantic Quarterly* 114 (1): 225–34. https://doi.org/10.1215/00382876-2831665.

———. 2015b. 'Justice for "Data Janitors"'. *Public Books* (Blog), 15 January. https://www.publicbooks.org/justice-for-data-janitors/.

Jackson, Patrick Thaddeus. 2016. *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics*. 2nd ed. Abingdon: Routledge.

Jacobs, Karrie. 2022. 'Toronto Wants to Kill the Smart City Forever'. *MIT Technology Review*, 29 June. https://www.technologyreview.com/2022/06/29/1054005/toronto-kill-the-smart-city/.

Jansen, Fieke, and Corrine Cath. 2021. 'Algorithmic Registers and Their Limitations as a Governance Practice'. In *Fake AI*, edited by Frederike Kaltheuner, 183–92. Manchester: Meatspace Press.

Jaquet-Chiffelle, David-Olivier. 2008. 'Reply: Direct and Indirect Profiling in the Light of Virtual Persons'. In *Profiling the European Citizen*, edited by Mireille Hildebrandt and Serge Gutwirth, 35–46. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-6914-7_15.

Jasanoff, Sheila, ed. 2004. *States of Knowledge: The Co-Production of Science and Social Order*. London: Routledge.

Jessop, Bob. 2007. 'Knowledge as a Fictitious Commodity: Insights and Limits of a Polanyian Analysis'. In *Reading Karl Polanyi for the Twenty-First Century*, edited by Ava Buğra and Kaan Ağartan, 115–34. Basingstoke, UK: Palgrave.

———. 2010. 'Cultural Political Economy and Critical Policy Studies'. *Critical Policy Studies* 3 (3–4): 336–56. https://doi.org/10.1080/19460171003619741.

Jessop, Bob, Agnès Labrousse, Thomas Lamarche, and Julien Vercueil. 2012. 'Crossing Boundaries: Towards Cultural Political Economy'. *Revue de La Régulation. Capitalisme, Institutions, Pouvoirs* 12 (December). https://doi.org/10.4000/regulation.9943.

Jia, Lianrui. 2020. 'Unpacking China's Social Credit System: Informatization, Regulatory Framework, and Market Dynamics'. *Canadian Journal of Communication* 45 (1): 113–27. https://doi.org/10.22230/cjc.2020v45n1a3483.

———. 2021. 'Building China's Tech Superpower: State, Domestic Champions and Foreign Capital'. In *Power and Authority in Internet Governance*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 97–122. Abingdon: Routledge.

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

Jiang, Min, and King-Wa Fu. 2018. 'Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?' *Policy & Internet* 10 (4): 372–92. https://doi.org/10.1002/poi3.187.

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

Joh, Elizabeth E. 2017. 'Feeding the Machine: Policing, Crime Data, & Algorithms'. *William & Mary Bill of Rights Journal* 26 (2): 287–302.

John, Deere. 2021. 'John Deere Data Services & Subscriptions Statement'. *John Deere*, 1 November. https://www.deere.com/en/privacy-and-data/data-services/?cid=VURL_trust.

———. 2022. 'John Deere Expands Access to Self-Repair Resources'. *John Deere,* 21 March. https://www.deere.com/en/news/all-news/john-deere-expands-access-to-self-repair-resources/.

Jones, Peter. 2016. 'Group Rights'. In *Stanford Encyclopedia of Philosophy Archive*. Stanford, CA: Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2016/entries/rights-group/.

Kaltheuner, Frederike. 2021. 'AI Snake Oil, Pseudoscience and Hype: An Interview With Arvind Narayanan'. In *Fake AI*, edited by Frederike Kaltheuner, 21–38. Manchester: Meatspace Press.

Kammourieh, Lanah, Thomas Baar, Jos Berens, Emmanuel Letouzé, Julia Manske, John Palmer, David Sangokoya, and Patrick Vinck. 2017. 'Group Privacy in the Age of Big Data'. In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bart van der Sloot, 37–66. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_3.

Kansa, Eric C., Jason Schultz, and Ahrash N. Bissell. 2005. 'Protecting Traditional Knowledge and Expanding Access to Scientific Data: Juxtaposing Intellectual Property Agendas Via a "Some Rights Reserved" Model'. *International Journal of Cultural Property* 12 (3): 285–314. https://doi.org/10.1017/S0940739105050204.

Kenney, Martin, Dafna Bearson, and John Zysman. 2021. 'The Platform Economy Matures: Measuring Pervasiveness and Exploring Power'. *Socio-Economic Review* 19 (4): 1451–83. https://doi.org/10.1093/ser/mwab014.

Kenyon, Miles. 2018. *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System*. Toronto: The Citizen Lab. https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.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*, vol. 1, edited by Peter Yu, 321–360. London: Praeger Publishers.

Khan, Lina M. 2019. 'The Separation of Platforms and Commerce'. *Columbia Law Review* 119 (4): 973–1098. https://columbialawreview.org/content/the-separation-of-platforms-and-commerce/.

Kieler, Ashlee. 2016. 'Samsung Software Update Will Deliberately "Brick" Remaining Galaxy Note 7 Phones'. *Consumer Reports* (Blog), 9 December. https://www.consumerreports.org/consumerist/samsung-software-update-will-deliberately-brick-remaining-galaxy-note-7-phones/.

Kim, Min-hyung. 2019. 'A Real Driver of US–China Trade Conflict: The Sino–US Competition for Global Hegemony and Its Implications for the Future'. *International Trade, Politics and Development* 3 (1): 30–40. https://doi.org/10.1108/ITPD-02-2019-003.

Kimery, Anthony. 2019. 'IARPA Seeks Information on Long-Range Biometric Recognition and Identification Technologies'. *biometricupdate.com*, 17 September 2019. https://www.biometricupdate.com/201909/iarpa-seeks-information-on-long-range-biometric-recognition-and-identification-technologies.

Kingsley-Hughes, Adrian. 2016. 'Nest to Brick Revolv Smart Hubs on Sunday, and There's Nothing Owners Can Do About It'. *ZDNet*, 17 June. https://www.zdnet.com/article/nest-to-brick-revolv-smart-hubs-on-sunday-and-theres-nothing-owners-can-do-about-it/.

Kirchner, Lauren. 2020. 'When Zombie Data Costs You a Home'. *The Markup*, 6 October. https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks.

Kitchin, Rob. 2014a. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. London: Sage.

———. 2014b. 'The Real Time City? Big Data and Smart Urbanism'. *GeoJournal* 79: 1–14.

Klauser, Francisco. 2018. 'Surveillance Farm: Towards a Research Agenda on Big Data Agriculture'. *Surveillance & Society* 16 (3): 370–78. https://doi.org/10.24908/ss.v16i3.12594.

Klein, Jennifer. 2006. *For All These Rights: Business, Labor, and the Shaping of America's Public-Private Welfare State*. Princeton, NJ: Princeton University Press.

Knopf, Howard P. 2018. 'Canada's Role in the Relationship of Trade and Intellectual Property'. 17. In *Canada in International Law at 150 and Beyond*. Waterloo:

Centre for International Governance Innovation. https://www.cigionline.org/publications/canadas-role-relationship-trade-and-intellectual-property/.

Knubley, John. 2021. *Building Superclusters for Canada*. Toronto: Brookfield Institute for Innovation + Entrepreneurship. https://brookfieldinstitute.ca/wp-content/uploads/Superclusters_Final2.pdf.

Koch, Bernard, Emily Denton, Alex Hanna, and Jacob G. Foster. 2021. 'Reduced, Reused and Recycled: The Life of a Dataset in Machine Learning Research'. *ArXiv*, December. http://arxiv.org/abs/2112.01716.

Koebler, Jason. 2017a. 'Apple Tells Lawmaker That Right to Repair IPhones Will Turn Nebraska into a "Mecca" for Hackers'. *Vice.com*, 17 February. https://www.vice.com/en/article/pgxgpg/apple-tells-lawmaker-that-right-to-repair-iphones-will-turn-nebraska-into-a-mecca-for-hackers.

———. 2017b. 'Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware'. *Vice.com*, 21 March. https://www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware.

———. 2020. 'Hospitals Need to Repair Ventilators. Manufacturers Are Making That Impossible'. *Vice.com*, 18 March. https://www.vice.com/en/article/wxekgx/hospitals-need-to-repair-ventilators-manufacturers-are-making-that-impossible.

Koenecke, Allison, Andrew Nam, Emily Lake, Joe Nudell, Minnie Quartey, Zion Mengesha, Connor Toups, John R. Rickford, Dan Jurafsky, and Sharad Goel. 2020. 'Racial Disparities in Automated Speech Recognition'. *Proceedings of the National Academy of Sciences* 117 (14): 7684–89. https://doi.org/10.1073/pnas.1915768117.

Kohl, Uta. 2013. 'Google: The Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond (Part 2)'. *International Journal of Law and Information Technology* 21 (2): 187–234. https://doi.org/10.1093/ijlit/eat004.

Koops, Bert-Jan. 2014. 'On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy'. *Politica e Società* 3 (2): 247–64.

Krikorian, Gaëlle, and Amy Kapczynski, eds. 2010. *Access to Knowledge in the Age of Intellectual Property*. New York: Zone Books.

Kuempel, Ashley. 2016. 'The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry'. *Northwestern Journal of International Law & Business* 36 (1): 207–34.

Kukutai, Tahu, and John Taylor, eds. 2016. *Indigenous Data Sovereignty*. Canberra: ANU Press. http://doi.org/10.22459/CAEPR38.11.2016.

La Grassa, Jennifer. 2020. 'Ontario Health Defends Hiring Private Company for COVID-19 Farm Testing'. *CBC News*, 15 July. https://www.cbc.ca/news/canada/windsor/ontario-health-private-company-covid-19-testing-natyshak-1.5650967.

———. 2022. 'Automotive Right-to-Repair Bill Introduced by Windsor West MP'. *CBC*, 8 February. https://www.cbc.ca/news/canada/windsor/windsor-essex-right-to-repair-automotive-industry-1.6340391.

Langenderfer, Jeff. 2009. 'End-User License Agreements: A New Era of Intellectual Property Control'. *Journal of Public Policy & Marketing* 28 (2): 202–11. https://doi.org/10.1509/jppm.28.2.202.

LaReau, Jamie L. 2018. 'How General Motors is Leading the Race for Self-Driving Cars'. *Detroit Free Press*, 19 July. https://www.freep.com/story/money/cars/general-motors/2018/07/19/general-motors-cruise-av-autonomous-car/782570002/.

Latour, Bruno. 1988. *Science in Action: How to Follow Scientists and Engineers Through Society*. Cambridge, MA: Harvard University Press.

Lauer, Josh. 2017. *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York: Columbia University Press.

Lauriault, Tracey P. 2022. 'Looking Back Toward a "Smarter" Open Data Future'. In *The Future of Open Data*, edited by Pamela Robinson and Teresa Scassa, 19–53. Ottawa: University of Ottawa Press.

Lee-Makiyama, Hosuk, and Patrick Messerlin. 2014. 'Sovereign Patent Funds (SPFs): Next-Generation Trade Defence?' 6/2014. *ECIPE Policy Briefs*. Brussels: European Centre for International Political Economy. https://ecipe.org/wp-content/uploads/2014/12/PB06.pdf.

Lemos, André, Rodrigo Jose Firmino, Daniel Marques, Eurico Matos, and Catarina Lopes. 2022. 'Smart Pandemic Surveillance?: A Neo-Materialist Analysis of the "Monitora Covid-19" Application in Brazil'. *Surveillance & Society* 20 (1): 82–99. https://doi.org/10.24908/ss.v20i1.14282.

Lepore, Jill. 2020. *If/Then: How the Simulmatics Corporation Invented the Future*. New York: Liveright Publishing.

Lerman, Rachel. 2020. 'Trump Touted Google as a Solution to Coronavirus Testing. A Month Later, Verily Has Barely Made a Dent'. *Washington Post*, 1 May. https://www.washingtonpost.com/technology/2020/05/01/google-verily-covid-testing/.

Levine, Sam. 2023. 'FTX Founder Sam Bankman-Fried Charged with 12 Counts in New Indictment'. *The Guardian*, 23 February. https://www.theguardian.com/business/2023/feb/23/ftx-sam-bankman-fried-cryptocurrency-exchange-charges.

Levitz, Stephanie. 2021. 'Under Fire, the Company Managing COVID-19 Testing at Canada's Border Insists It's Ready for the Next Phase of the Pandemic'. *The Toronto Star*, 25 May. https://www.thestar.com/politics/federal/2021/05/25/under-fire-the-company-managing-covid-19-testing-at-canadas-border-insists-its-ready-for-the-next-phase-of-the-pandemic.html.

Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain. 2018. 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure'. *Policy & Internet* 10 (4): 415–53. https://doi.org/10.1002/poi3.183.

Linsi, Lukas, and Daniel K. Mügge. 2019. 'Globalization and the Growing Defects of International Economic Statistics'. *Review of International Political Economy* 26 (3): 361–83. https://doi.org/10.1080/09692290.2018.1560353.

Litman, Jessica. 1990. 'The Public Domain'. *Emory Law Journal* 39 (4): 965–1023. https://heinonline.org/HOL/Page?handle=hein.journals/emlj39&id=979&div=&collection=.

Liu, Yangyue. 2012. 'The Rise of China and Global Internet Governance'. *China Media Research* 8 (2): 46–56.

Lohr, Steve. 2015. 'Sidewalk Labs, a Start-Up Created by Google, Has Bold Aims to Improve City Living'. *New York Times*, 10 June. https://www.nytimes.com/2015/06/11/technology/sidewalk-labs-a-start-up-created-by-google-has-bold-aims-to-improve-city-living.html.

Loi, Michele, and Markus Christen. 2020. 'Two Concepts of Group Privacy'. *Philosophy & Technology* 33 (2): 207–24. https://doi.org/10.1007/s13347-019-00351-0.

Loukissas, Yanni Alexander. 2019. *All Data Are Local: Thinking Critically in a Data-Driven Society*. Cambridge, MA: MIT Press.

Lovejoy, Ben. 2020. 'Third Antitrust Investigation into Apple/Amazon Deal Which Excluded Independent Resellers'. *9to5Mac* (Blog), 29 October. https://9to5mac.com/2020/10/29/apple-amazon-deal-germany/.

Lovett, Laura. 2020. 'US Senators Question Ascension on Its Google Collaboration Project Nightingale'. *MobiHealthNews*, 4 March. https://www.mobihealthnews.com/news/us-senators-question-ascension-its-google-collaboration-project-nightingale.

Lubarsky, Boris. 2017. 'Re-Identification of "Anonymized Data"'. *Georgetown Law Technology Review* 1: 202–13. https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Lubarsky-1-GEO.-L.-TECH.-REV.-202.pdf.

Luo, Ting, and Aofei Lv. 2021. '"Nine Dragons Run the Water" Fragmented Internet Governance in China'. In *Power and Authority in Internet Governance*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 123–46. Abingdon: Routledge.

Lupton, Deborah. 2014. 'Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps'. *Societies* 4 (4): 606–22. https://doi.org/10.3390/soc4040606.

———. 2016. *The Quantified Self: A Sociology of Self-Tracking*. Cambridge: Polity Press.

———. 2017. 'Feeling Your Data: Touch and Making Sense of Personal Digital Data'. *New Media & Society* 19 (10): 1599–614. https://doi.org/10.1177/1461444817717515.

———. 2018. *Digital Health: Critical and Cross-Disciplinary Perspectives*. New York: Routledge.

Lynch, Shana. 2017. 'Andrew Ng: Why AI is the New Electricity'. *Stanford Graduate School of Business* (Blog), 11 March. https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity.

———. 2015. *Surveillance After Snowden*. Cambridge, MA: Harvard University Press.

———. 2022. *Pandemic Surveillance*. 1st ed. Medford: Polity.

Maalsen, Sophia, and Jathan Sadowski. 2019. 'The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance'. *Surveillance & Society* 17 (1/2): 118–24. https://doi.org/10.24908/ss.v17i1/2.12925.

MacFarlane, Jane. 2019. 'Your Navigation App is Making Traffic Unmanageable'. *IEEE Spectrum*, 19 September. https://spectrum.ieee.org/your-navigation-app-is-making-traffic-unmanageable.

MacKinnon, Rebecca. 2013. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Magnet, Shoshana Amielle. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Chapel Hill, NC: Duke University Press. https://doi.org/10.1215/9780822394822.

Mahdawi, Arwa. 2018. 'Spotify Can Tell If You're Sad. Here's Why That Should Scare You'. *The Guardian*, 16 September. https://www.theguardian.com/commentisfree/2018/sep/16/spotify-can-tell-if-youre-sad-heres-why-that-should-scare-you.

Maki, Krystle. 2011. 'Neoliberal Deviants and Surveillance: Welfare Recipients Under the Watchful Eye of Ontario Works'. *Surveillance & Society* 9 (1/2): 47–63. https://doi.org/10.24908/ss.v9i1/2.4098.

Mann, Michael. 1984. 'The Autonomous Power of the State: Its Origins, Mechanisms and Results'. *European Journal of Sociology* 25 (2): 185–213. http://www.jstor.org/stable/23999270.

———. 1986. *The Sources of Social Power: A History of Power From the Beginning to A.D. 1760,* Vol. 1. New York: Cambridge University Press.

Mann, Monique. 2020. 'Technological Politics of Automated Welfare Surveillance: Social (and Data) Justice Through Critical Qualitative Inquiry'. *Global Perspectives* 1 (1): 1–12. https://doi.org/10.1525/gp.2020.12991.

Mann, Monique, Peta Mitchell, Marcus Foth, and Irina Anastasiu. 2020. '#BlockSidewalk to Barcelona: Technological Sovereignty and the Social License to Operate Smart Cities'. *Journal of the Association for Information Science and Technology* 71 (9): 1103–15. https://doi.org/10.1002/asi.24387.

Manning, Paddy. 2020. 'Robo-Dead'. *The Monthly*, 1 June. https://www.themonthly.com.au/today/paddy-manning/2020/01/2020/1590990618/robo-dead.

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

Mantelero, Alessandro. 2017. 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era'. In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bert van der Sloot, 139–58. New York: Springer.

Manwaring, Kayleen. 2017. 'Emerging Information Technologies: Challenges for Consumers'. *Oxford University Commonwealth Law Journal* 17 (2): 265–89. https://doi.org/10.1080/14729342.2017.1357357.

Mao, Frances. 2020. 'The Human Cost of Australia's Illegal "Robo" Hunt for Welfare Cheats'. *BBC News*, 18 November. https://www.bbc.com/news/world-australia-54970253.

Marks, Isobel H., Hannah Thomas, Marize Bakhet, and Edward Fitzgerald. 2019. 'Medical Equipment Donation in Low-Resource Settings: A Review of the Literature and Guidelines for Surgery and Anaesthesia in Low-Income and Middle-Income Countries'. *BMJ Global Health* 4 (5). https://doi.org/10.1136/bmjgh-2019-001785.

Martineau, Paris. 2019. 'Inside Airbnb's "Guerrilla War" Against Local Governments'. *Wired*, 28 March. https://www.wired.com/story/inside-airbnbs-guerrilla-war-against-local-governments/.

Masiero, Silvia, and S. Shakthi. 2020. 'Grappling With Aadhaar: Biometrics, Social Identity and the Indian State'. *South Asia Multidisciplinary Academic Journal* 23 (September): 1–10. https://doi.org/10.4000/samaj.6279.

Matsakis, Louise. 2019. 'Security Experts Unite Over the Right to Repair'. *Wired*, 30 April. https://www.wired.com/story/right-to-repair-security-experts-california/.

May, Christopher. 1996. 'Strange Fruit: Susan Strange's Theory of Structural Power in the International Political Economy'. *Global Society* 10 (2): 167–89. https://doi.org/10.1080/13600829608443105.

———. 2006. 'The Denial of History: Reification, Intellectual Property Rights and the Lessons of the Past'. *Capital & Class* 30 (1): 33–56. https://doi.org/10.1177/030981680608800103.

———. 2010. *A Global Political Economy of Intellectual Property Rights: The New Enclosures?* 2nd ed. New York: Routledge.

May, Christopher, and Susan K. Sell. 2006. *Intellectual Property Rights: A Critical History*. Boulder, CO: Lynne Rienner Publishers.

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

Maynard, Robyn. 2017. *Policing Black Lives: State Violence in Canada From Slavery to the Present*. Winnipeg: Fernwood Publishing.

Mazzucato, Mariana. 2018. *The Value of Everything: Making and Taking in the Global Economy*. London: Allen Lane.

Mazzucato, Mariana, and Jayati Ghosh. 2021. 'Health Innovation for All'. *Project Syndicate*, 9 December. https://www.project-syndicate.org/commentary/health-innovation-for-all-by-mariana-mazzucato-and-jayati-ghosh-2021-12.

McBride, Kurtis. 2018. 'Monetizing Smart Cities: Framing the Debate'. *Centre for International Governance Innovation*, 28 March. https://www.cigionline.org/articles/monetizing-smart-city-data/.

McChesney, Robert W. 2007. *Communication Revolution: Critical Junctures and the Future of Media*. New York: W.W. Norton & Company.

McCoy, Alfred W. 2009. *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State*. Madison, WI: University of Wisconsin Press.

McDonald, Sean. 2019. 'Affidavit of Sean McDonald. Between Corporation of the Canadian Civil Liberties Association and Lester Brown and Toronto Waterfront Revitalization Corporation, City of Toronto, Her Majesty in Right of Ontario as Represented by the Minster of Infrastructure, Her Majesty in Right of Canada, as Represented by the Minister of Communities and Infrastructure, and the Attorney General of Canada. Ontario Superior Court of Justice (Divisional Court)'. *Ontario Superior Court of Justice (Divisional Court)*. https://ccla.org/wp-content/uploads/2021/06/Affidavit-of-Sean-McDonald-2019-05-28_2.pdf.

McDonald, Sean, and Bianca Wylie. 2020. 'Notification: Apps Won't Contain the Outbreak of COVID-19'. *Centre for International Governance Innovation*.

25 June. https://www.cigionline.org/articles/notification-apps-wont-contain-outbreak-covid-19/.

McDonald, Sean Martin. 2019. 'Reclaiming Data Trusts'. *Centre for International Governance Innovation*, 5 March. https://www.cigionline.org/articles/reclaiming-data-trusts/.

———. 2020. 'Covid-19 Lessons: Building Disaster-Ready Technologies', *Centre for International Governance Innovation*. 20 October. https://www.cigionline.org/articles/covid-19-lessons-building-disaster-ready-technologies/

———. 2022. 'A Crisis of Loyalty'. *Centre for International Governance Innovation*, 3 March. https://www.cigionline.org/articles/a-crisis-of-loyalty/.

McIntyre, Catherine. 2018. 'How Google Won Over Kitchener-Waterloo'. *The Logic*, 24 October. https://thelogic.co/news/the-big-read/how-google-won-over-kitchener-waterloo/.

McKinsey Global Institute. 2016. 'Digital Globalization: The New Era of Global Flows'. Report. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

McLeod, Kembrew, and Peter DiCola. 2011. *Creative License: The Law and Culture of Digital Sampling*. Durham, NC: Duke University Press.

Medhora, Shalailah. 2019. 'Over 2000 People Died After Receiving Centrelink Robo-Debt Notice, Figures Reveal'. *Triple J Hack*, 17 February. https://www.abc.net.au/triplej/programs/hack/2030-people-have-died-after-receiving-centrelink-robodebt-notice/10821272.

Meijer, Albert, and Manuel Pedro Rodríguez Bolívar. 2016. 'Governing the Smart City: A Review of the Literature on Smart Urban Governance'. *International Review of Administrative Sciences* 82 (2): 392–408. https://doi.org/10.1177/0020852314564308.

Melanson, Stewart. 2009. 'Learning From the Past - Volume 1: The Automotive Industry and Economic Development in Ontario; A Historical Perspective (1904 to the Present)'. 2009-WPONT-006. *Working Paper Series: Ontario in the Creative Age*. Toronto: Martin Prosperity Institute, University of Toronto.

Milner, Yeshimabeit, and Amy Traub. 2021. *Data Capitalism and Algorithmic Racism*. Report. New York: Demos. https://www.demos.org/research/data-capitalism-and-algorithmic-racism.

Möhlmann, Mareike, and Lior Zalmanson. 2017. 'Hands on the Wheel: Navigating Algorithmic Management and Uber Drivers' Autonomy'. *ICIS 2017 Proceedings*, December. https://aisel.aisnet.org/icis2017/DigitalPlatforms/Presentations/3.

Molnar, Petra, and Lex Gill. 2018. *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*. Toronto: International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy).

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

Monge, Fernando, Sarah Barns, Rainer Kattel, and Francesca Bria. 2022. 'A New Data Deal: The Case of Barcelona'. 2022/02. *Working Paper Series*. UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/public-purpose/publications/2022/feb/new-data-deal-case-barcelona.

Montjoye, Yves-Alexandre de, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. 2013. 'Unique in the Crowd: The Privacy Bounds of Human Mobility'. *Scientific Reports* 3 (1): 1376. https://doi.org/10.1038/srep01376.

Montjoye, Yves-Alexandre de, Samuel S. Wang, and Alex (Sandy) Pentland. 2012. 'On the Trusted Use of Large-Scale Personal Data'. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*.

Morgan, Jacob. 2014. 'A Simple Explanation of "The Internet of Things"'. *Forbes* (Blog), 13 May. https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/.

Morozov, Evgeny. 2014. *To Save Everything, Click Here*. New York: Public Affairs.

———. 2019. 'Capitalism's New Clothes'. *The Baffler*, 4 February 2019. https://thebaffler.com/latest/capitalisms-new-clothes-morozov.

———. 2022. 'Critique of Techno-Feudal Reason'. *New Left Review* 133/134 (April): 89–126. https://newleftreview.org/issues/ii133/articles/evgeny-morozov-critique-of-techno-feudal-reason.

Morozov, Evgeny, and Francesca Bria. 2018. 'Rethinking the Smart City: Democratizing Urban Technology'. New York: Rosa Luxemburg Stiftung. http://www.rosalux-nyc.org/wp-content/files_mf/morozovandbria_eng_final55.pdf.

Morse, Susan C. 2019. 'Government-to-Robot Enforcement'. *Illinois Law Review*, 1497–1525. https://law.utexas.edu/faculty/publications/2020-government-to-robot-enforcement.

Mosco, Vincent. 2009. *The Political Economy of Communication*. 2nd ed. Los Angeles: Sage Publications, Ltd.

Moser, Petra. 2013. 'Patents and Innovation: Evidence From Economic History'. *Journal of Economic Perspectives* 27 (1): 23–44. https://doi.org/10.1257/jep.27.1.23.

Mulligan, Christina. 2016. 'Personal Property Servitudes on the Internet of Things'. *Georgia Law Review* 50 (4): 1121–1168. https://www.georgialawreview.org/article/2566-personal-property-servitudes-on-the-internet-of-things.

Muñiz, Manuel. 2019. 'The Coming Technological Cold War'. *Project Syndicate*, 30 April. https://www.project-syndicate.org/commentary/us-china-technology-cold-war-by-manuel-muniz-2019-04.

Murphy, Hannah, and Kiran Stacey. 2022. 'Facebook Libra: The Inside Story of How the Company's Cryptocurrency Dream Died'. *Financial Times*, 10 March. https://www.ft.com/content/a88fb591-72d5-4b6b-bb5d-223adfb893f3.

Musiani, Francesca. 2022. 'Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices'. *Information, Communication & Society*, March, 1–16. https://doi.org/10.1080/1369118X.2022.2049850.

Myre, Greg. 2021. 'How Bitcoin Has Fueled Ransomware Attacks'. *NPR*, 10 June. https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks.

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*, edited by Thomas C. Lawton, James N. Rosenau, and Amy C. Verdun, 39–56. Aldershot: Ashgate.

Narayanan, Arvind, and Vitaly Shmatikov. 2008. 'Robust De-Anonymization of Large Sparse Datasets'. *IEEE Symposium on Security and Privacy* 29: 111–25. https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

———. 2019. 'Robust De-Anonymization of Large Sparse Datasets: A Decade Later'. May. https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

Nieborg, David B., Chris J. Young, and Daniel Joseph. 2020. 'App Imperialism: The Political Economy of the Canadian App Store'. *Social Media + Society* 6 (2): 1–11. https://doi.org/10.1177/2056305120933293.

Nissenbaum, Helen. 2004. 'Privacy as Contextual Integrity'. *Washington Law Review* 79 (1): 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

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

Norwegian Consumer Council. 2020. 'Out of Control: How Consumers Are Exploited by the Online Advertising Industry'. *Norwegian Consumer Council*. https://www.conpolicy.de/en/news-detail/out-of-control-how-consumers-are-exploited-by-the-online-advertising-industry/.

Noto La Diega, Guido, and Ian Walden. 2016. 'Contracting for the "Internet of Things": Looking into the Nest'. *European Journal of Law and Technology* 7 (2): 1–38. https://ejlt.org/index.php/ejlt/article/view/450.

Obar, Jonathan A. 2015. 'Big Data and the Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management'. *Big Data & Society*, December, 1–16. https://doi.org/10.1177/2053951715608876.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2020. 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services'. *Information, Communication & Society* 23 (1): 128–47. https://doi.org/10.1080/1369118X.2018.1486870.

Obermeyer, Ziad, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. 2019. 'Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations'. *Science* 366 (6464): 447–53. https://doi.org/10.1126/science.aax2342.

O'Brien, Danny. 2018. 'The Year of the GDPR: 2018's Most Famous Privacy Regulation in Review'. *EFF Deeplinks* (Blog), 28 December. https://www.eff.org/deeplinks/2018/12/year-gdpr-2018s-most-famous-privacy-regulation-review.

Ocean Tomo, LLC. 2015. 'Annual Study of Intangible Asset Market Value'. *Ocean Tomo, LLC*. www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study.

O'Connor, Joe. 2020. 'How Four Millennials Came Out of Nowhere to Dominate the Mobile COVID-19 Testing Industry'. *Financial Post*, 14 September. https://financialpost.com/entrepreneur/small-business/how-four-millennials-came-out-of-nowhere-to-dominate-the-mobile-covid-19-testing-industry.

Oever, Niels ten. 2021. 'The Metagovernance of Internet Governance'. In *Power and Authority in Internet Governance: Return of the State?*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 76–94. Abingdon: Routledge.

Office of the Privacy Commissioner of Canada. 2014. 'Data Brokers: A Look at the Canadian and American Landscape'. *Office of the Privacy Commissioner*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/db_201409/.

———. 2016. *Consent and Privacy - A Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic Documents Act*. Ottawa: Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.

———. 2020. 'Privacy Review of the COVID Alert Exposure Notification Application'. 31 July. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/.

Ohlheiser, Abby. 2017. 'A Guide to the Things Silicon Valley "Invented" That Already Existed'. *Chicago Tribune*, 14 September. https://www.chicagotribune.com/business/blue-sky/ct-silicon-valley-bodega-20170914-story.html.

Ohm, Paul. 2010. 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization'. *UCLA Law Review* 57 (6): 1701–78.

O'Kane, Josh. 2019a. 'Inside the Mysteries and Missteps of Toronto's Smart-City Dream'. *The Globe and Mail*, 17 May. https://www.theglobeandmail.com/business/article-inside-the-mysteries-and-missteps-of-torontos-smart-city-dream/.

———. 2019b. New Sidewalk Deal Strikes Better Balance on IP and Innovation but Questions Still Unanswered, Experts Say'. *The Globe and Mail*, 1 November. https://www.theglobeandmail.com/business/article-experts-and-others-weigh-in-on-new-sidewalk-deal/.

2020. 'Sidewalk's End: How the Downfall of a Toronto "Smart City" Plan Began Long Before COVID-19'. *The Globe and Mail*, 24 May 2020. https://www.theglobeandmail.com/business/article-sidewalks-end-how-the-downfall-of-a-toronto-smart-city-plan-began/.

———. 2022. *Sideways: The City Google Couldn't Buy*. Toronto: Penguin-Random House.

O'Kane, Josh, and Alex Bozikovic. 2018. 'Sidewalk Labs Taking Steps to Control Intellectual Property on Toronto's "Smart City," Document Shows'. *The Globe and Mail*, 31 August. https://www.theglobeandmail.com/business/article-sidewalk-labs-taking-steps-to-control-intellectual-property-on-toronto/.

Osterloch, Rick. 2021. 'Google Completes Fitbit Acquisition'. *Google: The Keyword* (Blog), 14 January. https://blog.google/products/devices-services/fitbit-acquisition/.

Ostry, Sylvia, and Richard R. Nelson. 1995. 'Techno-Nationalism and Techno-Globalism: Conflict and Cooperation'. *The Brookings Institution*.

Pagano, U. 2014. 'The Crisis of Intellectual Monopoly Capitalism'. *Cambridge Journal of Economics* 38 (6): 1409–29. https://doi.org/10.1093/cje/beu025.

Palan, Ronen. 1999. 'Susan Strange 1923–1998: A Great International Relations Theorist'. *Review of International Political Economy* 6 (2): 121–32. http://www.jstor.org/stable/4177305.

Park, Kevin A., and Roberto G. Quercia. 2020. 'Who Lends Beyond the Red Line? The Community Reinvestment Act and the Legacy of Redlining'. *Housing Policy Debate* 30 (1): 4–26. https://doi.org/10.1080/10511482.2019.1665839.

Pasquale, Frank. 2015. *Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Cambridge University Press.

Patel, Nilay. 2019. 'Taking the Smarts Out of Smart TVs Would Make Them More Expensive'. *The Verge*, 7 January. https://www.theverge.com/2019/1/7/18172397/airplay-2-homekit-vizio-tv-bill-baxter-interview-vergecast-ces-2019.

———. 2021. 'John Deere Turned Tractors into Computers: What's Next?' *The Verge*, 15 June 2021. https://www.theverge.com/22533735/john-deere-cto-hindman-decoder-interview-right-to-repair-tractors.

Paul, Kari. 2021. 'Why Right to Repair Matters – According to a Farmer, a Medical Worker, a Computer Store Owner'. *The Guardian*, 2 August. https://www.theguardian.com/technology/2021/aug/02/why-right-to-repair-matters-according-to-a-farmer-a-medical-worker-a-computer-store-owner.

Pentikainen, Paul. 2021. 'Innisfil Transit - 2020 Results and Updates'. *DSR-0048-21*. Innisfil: Town of Innisfil. https://innisfil.civicweb.net/FileStorage/67E5E5EC62774DFB89763D9B08AAE73E-Innisfil%20Transit%20-%202020%20Results%20and%20Updates.pdf.

Perzanowski, Aaron. 2021. 'Consumer Perceptions of the Right to Repair'. *Indiana Law Journal* 96 (2): 361–94. https://www.repository.law.indiana.edu/ilj/vol96/iss2/1.

———. 2022. *The Right to Repair: Reclaiming the Things We Own*. New ed. Cambridge, UK; New York, NY: Cambridge University Press.

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

Peters, Anne, Lucy Koechlin, and Gretta Fenner Zinkernagel. 2009. 'Non-State Actors as Standard Setters: Framing the Issue in an Interdisciplinary Fashion'. In *Non-State Actors as Standard Setters*, edited by Anne Peters, Gretta Fenner Zinkernagel, Lucy Koechlin, and Till Förster, 1–32. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511635519.002.

Pfluger, Ryan. 2019. 'How SoftBank Ate the World'. *Wired UK*, 2 July. https://www.wired.co.uk/article/softbank-vision-fund.

Pink, Sarah, Minna Ruckenstein, Robert Willim, and Melisa Duque. 2018. 'Broken Data: Conceptualising Data in an Emerging World'. *Big Data & Society* 5 (1): 1–13. https://doi.org/10.1177/2053951717753228.

Plant, Arnold. 1934. 'The Economic Aspects of Copyright in Books'. *Economica* 1 (2): 167–95. https://doi.org/10.2307/2548748.

Plantin, Jean-Christophe, and Gabriele de Seta. 2019. 'WeChat as Infrastructure: The Techno-Nationalist Shaping of Chinese Digital Platforms'. *Chinese Journal of Communication*, February, 1–17. https://doi.org/10.1080/17544750.2019.1572633.

Pohle, Julia, and Daniel Voelsen. 2022. 'Centrality and Power: The Struggle Over the Techno-Political Configuration of the Internet and the Global Digital Order'. *Policy & Internet* 14 (1): 13–27. https://doi.org/10.1002/poi3.296.

Polanyi, Karl. 2001. *The Great Transformation: The Political and Economic Origins of Our Time*. Boston: Beacon 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*, edited by Tahu Kuktai and John Tailor, 57–76. Canberra: ANU Press.

Posadzki, Alexandra. 2022. 'How a Coding Error Caused Rogers Outage That Left Millions Without Service'. *The Globe and Mail*, 25 July. https://www.theglobeandmail.com/business/article-how-a-coding-error-caused-rogers-outage-that-left-millions-without/.

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

Powles, Julia, and Hal Hodson. 2017. 'Google DeepMind and Healthcare in an Age of Algorithms'. *Health and Technology* 7 (4): 351–67. https://doi.org/10.1007/s12553-017-0179-1.

Prabhakaran, Aiswarya. 2022. 'Cab-Aggregator App Yatri to Give Uber and Ola a Run for Their Money in Kochi'. *The New Indian Express*, 3 January. https://www.newindianexpress.com/cities/kochi/2022/jan/03/cab-aggregator-app-yatrito-give-uber-and-ola-a-run-for-their-money-in-kochi-2402377.html.

Press, Jordan, 2018. 'Canadians at Risk of Becoming "Data Cows" without a National Data Strategy, Documents Show'. *Financial Post*, 20 June. https://financialpost.com/technology/canadians-at-risk-of-being-data-cows-absent-big-data-strategy-documents-show.

Productivity Commission. 2020. 'Right to Repair: Terms of Reference'. Canberra: Australian Government Productivity Commission. https://www.pc.gov.au/inquiries/completed/repair/terms-of-reference.

———. 2021. *Right to Repair - Productivity Commission Inquiry Report*. 97. Canberra: Australian Government Productivity Commission. https://www.pc.gov.au/inquiries/completed/repair/report.

Puri, Anuj. 2021. 'A Theory of Group Privacy'. *Cornell Journal of Law and Public Policy* 30 (3): 477–538.

Radin, Margaret Jane. 2012. *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*. Princeton, NJ: Princeton University Press.

Rahman, K. Sabeel. 2018. 'Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities'. *Georgetown Law Technology Review* 2: 234–251.

Rajkomar, Alvin, and Eyal Oren. 2018. 'Deep Learning for Electronic Health Records'. *Google AI Blog* (Blog), 8 May. http://ai.googleblog.com/2018/05/deep-learning-for-electronic-health.html.

Redden, Joanna, Lina Dencik, and Harry Warne. 2020. 'Datafied Child Welfare Services: Unpacking Politics, Economics and Power'. *Policy Studies* 41 (5): 507–26. https://doi.org/10.1080/01442872.2020.1724928.

Repair Cafe. 2022. 'EU Delays Right to Repair for at Least Six Months'. *Repaircafe* (Blog), 24 October. https://www.repaircafe.org/en/eu-delays-right-to-repair-for-at-least-six-months/.

Reuters. 2021. 'Germany Rejects U.S. Proposal to Waive Patents on COVID-19 Vaccines'. *Reuters*, 6 May. https://www.reuters.com/business/healthcare-pharmaceuticals/germany-opposes-us-plan-waive-patents-covid-19-vaccines-2021-05-06/.

Rich, Jessica. 2016. 'What Happens When the Sun Sets on a Smart Product?' *Federal Trade Commission* (Blog), 13 July 2016. http://www.ftc.gov/business-guidance/blog/2016/07/what-happens-when-sun-sets-smart-product.

Right to Repair South Africa. 2022. 'Q & A - Explanation of the R2R Guidelines'. *Right to Repair South Africa* (Blog), 2022. https://www.right2repair.org.za/q-a-and-explanation-of-the-r2r-guidelines/.

Rimmer, Matthew. 2015. 'Introduction: Mapping Indigenous Intellectual Property'. In *Indigenous Intellectual Property: A Handbook of Contemporary Research*, edited by Matthew Rimmer, 1–44. Northampton, MA: Edward Elgar Publishing.

Rinik, Christine. 2020. 'Data Trusts: More Data Than Trust? The Perspective of the Data Subject in the Face of a Growing Problem'. *International Review of Law, Computers & Technology* 34 (3): 342–63. https://doi.org/10.1080/13600869.2019.1594621.

Robertson, Kate, Cynthia Kohh, and Yolanda Song. 2020. *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*. Toronto: Citizen Lab, Munk School of Global Affairs & Public Policy. https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/.

Robinson, Pamela, and Teresa Scassa, eds. 2022. *The Future of Open Data*. Ottawa: University of Ottawa Press.

Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. 2019. 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models'. *Nature Communications* 10 (3069). https://doi.org/10.1038/s41467-019-10933-3.

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

Rogerson, Kenneth S. 2003. 'Karl Polanyi'. In *Key Thinkers for the Information Society*, edited by Christopher May, 135–53. London: Routledge.

Romm, Tony. 2020. 'Google Taps Vast Trove of Location Data to Aid Global Effort to Combat Coronavirus'. *Washington Post*, 3 April. https://www.washingtonpost.com/technology/2020/04/03/google-data-distancing-coronavirus/.

Rone, Julia. 2021. 'The Return of the State? Power and Legitimacy Challenges to the EU's Regulation of Online Disinformation'. In *Power and Authority in Internet*

Governance, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 171–94. Abingdon: Routledge.

Rose, Mark. 1993. *Authors and Owners: The Invention of Copyright*. Cambridge, MA: Cambridge University Press.

Rosenblat, Alex. 2018. *Uberland: How Algorithms Are Rewriting the Rules of Work*. Oakland, CA: University of California Press.

Roth, Amanda. 2018. 'Fleissig, CEO of Waterfront Toronto, Pressured Out by Board'. *The Logic*, 6 July. https://thelogic.co/news/exclusive/fleissig-ceo-of-waterfront-toronto-pressured-out-by-board/.

Rothstein, Richard. 2017. *The Color of Law: A Forgotten History of How Our Government Segregated America*. New York; London: Liveright.

Rubin, Ben Fox. 2018. 'Apple Pumps Up Its Amazon Listings With IPhones, IPads and More'. *CNET*, 11 November. https://www.cnet.com/tech/mobile/apple-pumps-up-its-amazon-listings-with-iphones-ipads-and-more-xr-xs-watch/.

Rubinstein, Dana, and Joe Anuta. 2020. 'City Hall Calls Google-Backed LinkNYC Consortium "Delinquent"'. *Politico*, 3 March. https://politi.co/39nf7Mi.

Rudin, Cynthia, Caroline Wang, and Beau Coker. 2020. 'The Age of Secrecy and Unfairness in Recidivism Prediction'. *Harvard Data Science Review* 2 (1): 1–54. https://doi.org/10.1162/99608f92.6ed64b30.

Ruggles, Ellie. 2021. 'Innisfil and Uber: A Rural Municipality's Misadventures in Smart Public Transit'. In *Smart Cities in Canada: Digital Dreams, Corporate Designs*, edited by Mariana Valverde and Alexandra Flynn, 145–55. Toronto: James Lorimer Ltd.

Ruppert, Evelyn, Engin Isin, and Didier Bigo. 2017. 'Data Politics'. *Big Data & Society* 4 (2): 1–7. https://doi.org/10.1177/2053951717717749.

Saab, Anne. 2019. *Narratives of Hunger in International Law: Feeding the World in Times of Climate Change*. New York, NY: Cambridge University Press.

Sadowski, Jathan, and Roy Bendor. 2019. 'Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary'. *Science, Technology, & Human Values* 44 (3): 540–63. https://doi.org/10.1177/0162243918806061.

Saint-Arnaud, Pierre. 2021. 'COVID Alert App Cost Feds $20M But Results "Did Not Meet Expectations": New Data'. *Global News*, 5 July. https://globalnews.ca/news/8003920/covid-alert-app-expensive-ineffective/.

Šajn, Nikolina. 2022. 'Right to Repair'. PE 698.869. European Parliament, Members' Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)698869.

Salus Coop. n.d. 'Manifesto'. *Salus Coop* (Blog). https://www.salus.coop/en/manifest-salus-coop-en-referencia-a-la-covid-19-3/.

Samal, Adyasha. 2021. 'Special 301 Report 2021: US's Great U-Turn on Compulsory Licensing'. *SpicyIP* (Blog), 10 May. https://spicyip.com/2021/05/special-301-report-2021-uss-great-u-turn-on-compulsory-licensing.html.

Samsel, Haley. 2019. 'Estonia Creates World's First-Ever "Data Embassy" to Improve Information Security'. *Security Today*, 3 July. https://securitytoday.com/articles/2019/07/03/estonia-creates-worlds-firstever-data-embassy-to-improve-information-security.aspx.

Samuelson, Pamela. 2016. 'Freedom to Tinker'. *Theoretical Inquiries in Law* 17 (2): 563–600. http://www7.tau.ac.il/ojs/index.php/til/article/view/1431.

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. 2018. 'Back on the Data Trail: The Evolution of Canada's Data Broker Industry'. *Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic*. https://databrokers.cippic.ca/wp-content/uploads/2019/04/CIPPIC-Back_on_the_Data_Trail.pdf.

Sargsyan, Tatevik. 2016. 'Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security'. *International Journal of Communication* 10: 2221–37. https://ijoc.org/index.php/ijoc/article/view/3854.

Savage, Mark. 2021. 'Spotify Wants to Suggest Songs Based on Your Emotions'. *BBC News*, 28 January. https://www.bbc.com/news/entertainment-arts-55839655.

Scassa, Teresa. 2017. 'Sharing Data in the Platform Economy: A Public Interest Argument for Access to Platform Data'. *UBC Law Review* 50 (4): 1017–71.

———. 2018a. *Data Ownership*. Waterloo: Centre for International Governance Innovation. https://www.cigionline.org/publications/data-ownership.

———. 2018b. 'Enforcement Powers Key to PIPEDA Reform'. *Policy Options*, 7 June. https://policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/.

Scassa, Teresa, and Pamela Robinson. 2022. 'Introduction'. In *The Future of Open Data*, edited by Pamela Robinson and Teresa Scassa, 1–18. Ottawa: University of Ottawa Press.

Schauenberg, Tim. 2019. 'Patents on Plants: Is the Sellout of Genes a Threat to Farmers and Global Food Security?' *DW.COM*, 3 September 2019. https://p.dw.com/p/3NOqe.

Schepel, Harm. 2005. *The Constitution of Private Governance: Roduct Standards in the Regulation of Integrating Markets*. London: Bloomsbury Publishing.

Scher, Isaac. 2020. 'Hospitals Need Ventilators to Keep Severe COVID-19 Patients Alive. They Might Not Be Able to Fix Them Without Paying the Manufacturer $7,000 Per Technician'. *Business Insider*, 3 June. https://www.businessinsider.com/ventilator-manufacturers-dont-let-hospitals-fix-coronavirus-right-to-repair-2020-5.

Schiller, Dan. 1999. *Digital Capitalism: Networking the Global Market System*. Cambridge, MA: MIT Press.

———. 2015. 'Digital Capitalism: Stagnation and Contention?' *OpenDemocracy*, 13 October. https://www.opendemocracy.net/en/digital-capitalism-stagnation-and-contention/.

Schiller, Herbert I. 1975. 'Communication and Cultural Domination'. *Journal of Politics* 5 (4): 1–127.

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

Scholz, Trebor. 2017. 'Platform Cooperativism Vs. the Sharing Economy'. In *Big Data & Civic Engagement*, edited by Nicholas Douay and Annie Wan, 47–54. Rome: Planum Publisher.

Scholz, Trebor, and Nathan Schneider, eds. 2017. *Ours to Hack and to Own: The Rise of Platform Cooperativism, a New Vision for the Future of Work and a Fairer Internet*. New York: OR Books.

Schwartz, Herman Mark. 2017. 'Elites and American Structural Power in the Global Economy'. *International Politics* 54 (3): 276–91. https://doi.org/10.1057/s41311-017-0038-8.

———. 2021. 'Global Secular Stagnation and the Rise of Intellectual Property Monopoly'. *Review of International Political Economy* 29 (5): 1448–1476. https://doi.org/10.1080/09692290.2021.1918745.

Scott, Colin. 2010. 'Standard-Setting in Regulatory Regimes'. In *The Oxford Handbook of Regulation*, edited by Robert Baldwin, Martin Cave, and Martin Lodge, 104–19. New York: Oxford University Press.

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

Segal, Adam. 2021. 'Huawei, 5G, and Weaponized Interdependence'. In *The Uses and Abuses of Weaponized Interdependence*, edited by Henry Farrell and Abraham L. Newman, 149–66. Washington, DC: Brookings Institution.

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

———. 2004. 'Intellectual Property and Public Policy in Historical Perspective: Contestation and Settlement'. *Loyola of Los Angeles Law Review* 38: 267–322. https://www.semanticscholar.org/paper/Intellectual-Property-and-Public-Policy-in-and-Sell/08fac56bd7a215a4c65c8cb1d4539fedc9164f73.

Semeniuk, Ivan. 2020. 'Ottawa Launches "COVID Alert" App That Notifies Users About Contact With Coronavirus Cases'. *The Globe and Mail*, 31 July. https://www.theglobeandmail.com/canada/article-ottawa-launches-covid-alert-app-that-notifies-users-about-contact/.

Shadlen, Kenneth C., Bhaven N. Sampat, and Amy Kapczynski. 2020. 'Patents, Trade and Medicines: Past, Present and Future'. *Review of International Political Economy* 27 (1): 75–97. https://doi.org/10.1080/09692290.2019.1624295.

Shadlen, Kenneth C., Samira Guennif, Alenka Guzmán, and Narayanan Lalitha, eds. 2013. *Intellectual Property, Pharmaceuticals and Public Health*. Cheltenham: Edward Elgar Publishing.

Shallu, Deepika Shimar, and Kumar Meena Ravi. 2019. 'Digitalization in India: An Innovative Concept'. *International Journal of Engineering Development and Research* 7 (1): 452–56. https://www.ijedr.org/viewfull.php?&p_id=IJEDR1901081.

Shand, Hope J. 2002. 'Intellectual Property: Enhancing Corporate Monopoly and Bi oserfdom'. In *Fatal Harvest: The Tragedy of Industrial Agriculture*, edited by Andrew Kimbrell, 240–248. Washington, DC: Foundation for Deep Ecology.

Sharon, Tamar. 2016. 'The Googlization of Health Research: From Disruptive Innovation to Disruptive Ethics'. *Personalized Medicine* 13 (6): 563–74. https://doi.org/10.2217/pme-2016-0057.

———. 2018. 'When Digital Health Meets Digital Capitalism, How Many Common Goods Are at Stake?' *Big Data & Society* 5 (2): 1–12. https://doi.org/10.1177/2053951718819032.

———. 2020. 'Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers'. *Ethics and Information Technology* 23 (Suppl 1): 545–57. https://doi.org/10.1007/s10676-020-09547-x.

Shaw, James A., and Joseph Donia. 2021. 'The Sociotechnical Ethics of Digital Health: A Critique and Extension of Approaches From Bioethics'. *Frontiers in Digital Health* 3 (September): 725088. https://doi.org/10.3389/fdgth.2021.725088.

Sheehan, Matt. 2022. 'Biden's Unprecedented Semiconductor Bet'. *Carnegie Endowment for International Peace* (Blog), 27 October. https://carnegieendowment.org/2022/10/27/biden-s-unprecedented-semiconductor-bet-pub-88270.

Shelton, Taylor, Matthew Zook, and Alan Wiig. 2015. 'The "Actually Existing Smart City"'. *Cambridge Journal of Regions, Economy and Society* 8 (1): 13–25. https://doi.org/10.1093/cjres/rsu026.

Shen, Hong. 2016. 'China and Global Internet Governance: Toward an Alternative Analytical Framework'. *Chinese Journal of Communication* 9 (3): 304–24. https://doi.org/10.1080/17544750.2016.1206028.

Shen, Hong, Cori Faklaris, Haojian Jin, Laura Dabbish, and Jason I. Hong. 2020. '"I Can't Even Buy Apples If I Don't Use Mobile Pay?": When Mobile Payments Become Infrastructural in China'. *Proceedings of the ACM on Human-Computer Interaction* 4 (CSCW2): 170:1–170:26. https://doi.org/10.1145/3415241.

Sherwood, Juanita, and Thalia Anthony. 2020. 'Ethical Conduct in Indigenous Research: It's Just Good Manners'. In *Indigenous Research Ethics: Claiming Research Sovereignty Beyond Deficit and the Colonial Legacy*, edited by Lily George, Juan Tauri, and Lindsey Te Ata o Tu MacDonald, 19–40. Bingley: Emerald Publishing Limited.

Shiva, Vandana, ed. 2016. *Seed Sovereignty, Food Security: Women in the Vanguard of the Fight Against GMOs and Corporate Agriculture*. Berkeley, CA: North Atlantic Books.

Sidewalk Labs. 2017a. 'Project Vision (Response to Waterfront Toronto RFP)'. https://quaysideto.ca/wp-content/uploads/2019/04/SWL-Vision-Sections-of-RFP-Submission-October-27-2017.pdf.

———. 2017b. 'Project Vision (Response to Waterfront Toronto RFP), Technical Appendix'. https://quaysideto.ca/wp-content/uploads/2019/04/SWL-Vision-Sections-of-RFP-Submission-October-27-2017.pdf.

———. 2018. *Digital Governance Proposals for DSAP Consultation*. Toronto: Sidewalk Labs. https://quaysideto.ca/wp-content/uploads/2019/07/Digital-Governance-Proposals-for-DSAP-Consultation.pdf.

———. 2019a. 'Toronto Tomorrow (Sidewalk Labs' Master Innovation and Development Plan), Vol. 0: Overview'.

———. 2019b. 'Toronto Tomorrow (Sidewalk Labs' Master Innovation and Development Plan), Vol. 1: The Plans'.

———. 2019c. 'Toronto Tomorrow (Sidewalk Labs' Master Innovation and Development Plan), Vol. 2: The Urban Innovations'.

———. 2019d. 'Master Innovation & Development Plan Digital Innovation Appendix'. *Sidewalk Labs*. https://quaysideto.ca/wp-content/uploads/2019/11/Sidewalk-Labs-Digital-Innovation-Appendix.pdf.

Sidewalk Toronto. 2017. 'New District in Toronto Will Tackle the Challenges of Urban Growth'. *Sidewalk Toronto*. https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/13214335/Sidewalk-Toronto-Press-Release.pdf.

Siegel, Rachel. 2018. 'Remember How Play-Doh Smells? U.S. Trademark Officials Get It'. *Washington Post*, 24 May. https://www.washingtonpost.com/news/business/wp/2018/05/24/remember-how-play-doh-smells-u-s-trademark-officials-get-it/.

Sikor, Thomas, and Christian Lund. 2009. 'Access and Property: A Question of Power and Authority'. *Development and Change* 40 (1): 1–22. https://doi.org/10.1111/j.1467-7660.2009.01503.x.

Simon, Felix M. 2019. '"We Power Democracy": Exploring the Promises of the Political Data Analytics Industry'. *The Information Society* 35 (3): 158–69. https://doi.org/10.1080/01972243.2019.1582570.

Slett, Marylin, and Judith Sayers. 2020. 'First Nations Have the Right to #KeepSafe From COVID-19'. *The Georgia Straight*, 21 September. https://www.straight.com/news/marilyn-slett-and-judith-sayers-first-nations-have-right-to-keepsafe-from-covid-19.

Solove, Daniel. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Spar, Debora L. 2001. *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth, From the Compass to the Internet*. New York: Houghton Mifflin Harcourt.

Spencer, Keith A. 2017. 'Silicon Valley Has a Bad Habit of "Inventing" Things That Already Exist'. *Salon*, 25 June. https://www.salon.com/2017/06/25/silicon-valley-has-a-bad-habit-of-inventing-things-that-already-exist/.

Spicer, Zachary. 2021. 'A New Public-Private Partnership for the Platform Age? Uber as Public Transit'. In *The Platform Economy and the Smart City: Technology and the Transformation of Urban Policy*, edited by Zachary Spicer and Austin Zwick, 165–87. Montreal and Kingston: McGill-Queen's University Press.

Spicer, Zachary, Gabriel Eidelman, and Austin Zwick. 2019. 'Patterns of Local Policy Disruption: Regulatory Responses to Uber in Ten North American Cities'. *Review of Policy Research* 36 (2): 146–67. https://doi.org/10.1111/ropr.12325.

Spurr, Ben. 2018. 'Crowded Buses, Long Commutes—Why Transit is Top of Mind for Toronto Voters'. *The Toronto Star*, 25 September. https://www.thestar.com/news/toronto-election/2018/09/25/crowded-buses-long-commutes-why-transit-is-top-of-mind-for-toronto-voters.html.

———. 2021. 'Toronto's Gridlock is Already Back—And Your Commute May Get Worse Than Ever After COVID-19'. *The Toronto Star*, 7 October. https://www.thestar.com/news/gta/2021/10/07/torontos-gridlock-is-already-back-and-your-commute-may-get-worse-than-ever-after-covid-19.html.

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

———. 2018. 'The Social Wealth Fund: The Social Wealth of Data'. *Autonomy* 3 (June): 2–4. autonomy.work/wp-content/uploads/2018/05/Nick-Christine-Social-wealth.pdf.

Stadnik, Ilona. 2021. 'Russia: An Independent and Sovereign Internet?' In *Power and Authority in Internet Governance*, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte, 147–68. Abingdon: Routledge.

Stark, Luke, and Jevan Hutson. 2021. 'Physiognomic Artificial Intelligence'. *Fordham Intellectual Property, Media & Entertainment Law Journal*, September. https://doi.org/10.2139/ssrn.3927300.

Statt, Nick. 2019. 'How Apple's Deal With Amazon Screwed Over Small Recycling Businesses'. *The Verge*, 21 May. https://www.theverge.com/2019/5/21/18624846/amazon-marketplace-apple-deal-iphones-mac-third-party-sellers-john-bumstead.

Steele, Dale. 2017. *Analysis of Precision Agriculture Adoption & Barriers in Western Canada: Producer Survey of Western Canada*. Ottawa: Agriculture and Agri-Food Canada. April. http://static.albertafarmexpress.ca/wp-content/uploads/2017/05/Final-Report-Analysis-of-Precision-Agriculture-Adoption-and-Barriers-in-western-Canada-April-2017.pdf.

Stevens, Amy, and James Allen-Robertson. 2021. 'Encrypting Human Rights: The Intertwining of Resistant Voices in the UK State Surveillance Debate'. *Big Data & Society* 8 (1): 1–15. https://doi.org/10.1177/2053951720985304.

Stone, Maddie. 2020. 'Apple's Independent Repair Program is Invasive to Shops and Their Customers, Contract Shows'. *Vice.com*, 6 February. https://www.vice.com/en/article/qjdjnv/apples-independent-repair-program-is-invasive-to-shops-and-their-customers-contract-shows.

Strange, Susan. 1970. 'International Economics and International Relations: A Case of Mutual Neglect'. *International Affairs* 46 (2): 304–15. http://www.jstor.org/stable/2613829.

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

Sundquist, Christian. 2021. 'Pandemic Surveillance Discrimination'. *Seton Hall Law Review* 51 (January): 1535–47. https://scholarship.law.pitt.edu/fac_articles/507.

Tanczer, Leonie, Isabel Lopez-Neira, and Simon Parkin. 2021. '"I Feel Like We're Really Behind the Game": Perspectives of the United Kingdom's Intimate Partner Violence Support Sector on the Rise of Technology-Facilitated Abuse'. *Journal of Gender-Based Violence* 5 (3): 431–50. https://doi.org/10.2139/ssrn.3931045.

Taylor, Linnet. 2017a. 'Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World'. In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bart van der Sloot, 13–36. New York: Springer.

———. 2017b. 'What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally'. *Big Data & Society* 4 (2): 1–14. https://doi.org/10.1177/2053951717736335.

———. 2021. 'Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector'. *Philosophy & Technology* 34 (4): 897–922. https://doi.org/10.1007/s13347-020-00441-4.

Taylor, Linnet, Bert van der Sloot, and Luciano Floridi. 2017. 'Conclusion: What Do We Know About Group Privacy?' In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bert van der Sloot, 225–37. New York: Springer.

Taylor, Linnet, Gargi Sharma, Aaron Martin, and Shazade Jameson, eds. 2021. *Data Justice and Covid-19*. London: Meatspace Press.

Taylor, Linnet, Luciano Floridi, and Bert van der Sloot, eds. 2017a. *Group Privacy: New Challenges of Data Technologies*. New York: Springer.

———. 2017b. 'Introduction: A New Perspective on Privacy'. In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bert van der Sloot, 1–12. Philosophical Studies Series 126. New York: Springer.

Teece, David J. 1998. 'Capturing Value From Knowledge Assets: The New Economy, Markets for Know-How, and Intangible Assets'. *California Management Review* 40 (3): 55–79. https://doi.org/10.2307/41165943.

Tene, Omer, and Jules Polonetsky. 2013. 'A Theory of Creepy: Technology, Privacy and Shifting Social Norms'. *Yale Journal of Law & Technology* 16 (1): 59–92.

Thatcher, Jim, David O'Sullivan, and Dillon Mahmoudi. 2016. 'Data Colonialism Through Accumulation by Dispossession: New Metaphors for Daily Data'. *Environment and Planning D: Society and Space* 34 (6): 990–1006. https://doi.org/10.1177/0263775816633195.

The British Academy and the Royal Society. 2017. 'Data Management and Use: Governance in the 21st Century'. https://royalsociety.org/~/media/policy/projects/data-governance/data-managementgovernance.pdf.

The Canadian Press. 2020. 'B.C. Privacy Commissioner Will Hear First Nations Complaints About COVID'. *The Globe and Mail*, 21 September. https://www.theglobeandmail.com/canada/british-columbia/article-bc-privacy-commissioner-will-hear-first-nations-complaints-about/.

———. 2021. 'Ottawa Awards COVID-19 Border Testing Contracts Worth $631M'. *Global News*, 6 December. https://globalnews.ca/news/8428125/covid-border-testing-rules-canada/.

The Repair Association. n.d. 'Legislation'. *The Repair Association*. https://www.repair.org/legislation.

The White House. 2021. 'Executive Order on Promoting Competition in the American Economy'. United States Government. 9 July. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

The White House. 2022. 'Executive Order on Ensuring Responsible Development of Digital Assets'. United States Government. 9 March. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

Thelen, Kathleen. 1999. 'Historical Institutionalism in Comparative Politics'. *Annual Review of Political Science* 2 (1): 369–404. https://doi.org/10.1146/annurev.polisci.2.1.369.

Thomas, Gareth M., and Deborah Lupton. 2016. 'Threats and Thrills: Pregnancy Apps, Risk and Consumption'. *Health, Risk & Society* 17 (7–8): 495–509. https://doi.org/10.1080/13698575.2015.1127333.

Thumm, Nikolaus. 2000. *Intellectual Property Rights: National Systems and Harmonisation in Europe*. New York: Physica-Verlag.

Tiller, Jane, Susan Morris, Toni Rice, Krystal Barter, Moeen Riaz, Louise Keogh, Martin B. Delatycki, Margaret Otlowski, and Paul Lacaze. 2020. 'Genetic Discrimination by Australian Insurance Companies: A Survey of Consumer Experiences'. *European Journal of Human Genetics* 28 (1): 108–13. https://doi.org/10.1038/s41431-019-0426-1.

Ting, Daniel Shu Wei, Louis R. Pasquale, Lily Peng, John Peter Campbell, Aaron Y. Lee, Rajiv Raman, Gavin Siew Wei Tan, Leopold Schmetterer, Pearse A. Keane, and Tien Yin Wong. 2019. 'Artificial Intelligence and Deep Learning in Ophthalmology'. *British Journal of Ophthalmology* 103 (2): 167–75. https://doi.org/10.1136/bjophthalmol-2018-313173.

Tomaskovic-Devey, Don. 2011. 'Financialization and Income Inequality'. *Sociological Images*, 2011. https://thesocietypages.org/socimages/2011/11/10/financialization-and-income-inequality/.

Tooze, Adam. 2022. 'Chartbook #116: The End of Crypto's "Wild West"? The Battle to Shape the Future of Digital Assets in US-UK-EU'. Substack Newsletter. *Chartbook* (Blog), 24 April. https://adamtooze.substack.com/p/chartbook-116-the-end-of-cryptos.

Towse, Ruth. 2013. 'The Quest for Evidence on the Economic Effects of Copyright Law'. *Cambridge Journal of Economics* 37 (5): 1187–202. https://doi.org/10.1093/cje/bet014.

Tréguer, Félix. 2019. 'Seeing Like Big Tech: Security Assemblages, Technology, and the Future of State Bureaucracy'. In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 145–64. New York: Routledge.

Trenham, Claire, and Adam Steer. 2019. 'The Good Data Manifesto'. In *Good Data*, edited by Angela Daly, S. Kate Devitt, and Monique Mann, 37–53. Amsterdam: Institute of Network Cultures.

Triolo, Paul, Kevin Allison, Clarise Brown, and Kelsey Broderick. 2020. *The Digital Silk Road: Expanding China's Digital Footprint*. Report. 29 April. New York, NY: Eurasia Group. https://www.eurasiagroup.net/live-post/digital-silk-road-expanding-china-digital-footprint.

Tuhiwai-Smith, Lind. 1999. *Decolonizing Methodologies: Research and Indigenous Peoples*. New York: Zed Books.

Turber, Stefanie, Jan vom Brocke, Oliver Gassmann, and Elgar Fleisch. 2014. 'Designing Business Models in the Era of Internet of Things'. In *Advancing the Impact of Design Science: Moving From Theory to Practice*, edited by Monica Chiarini Tremblay, Debra VanderMeer, Marcus Rothenberger, Ashish Gupta, and Victoria Yoon, 17–31. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-06701-8_2.

Turow, Joseph. 2021. *The Voice Catchers: How Marketers Listen in to Exploit Your Feelings, Your Privacy, and Your Wallet*. New Haven, CT: Yale University Press.

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

———. 2019a. 'Precarious Ownership of the Internet of Things in the Age of Data'. In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 121–48. Cham: Palgrave-Macmillan.

———. 2019b. 'How US-Made Rules Shape Internet Governance in China'. *Internet Policy Review: Journal on Internet Regulation* 8 (2): 1–22. https://doi.org/10.14763/2019.2.1408.

———. 2021. 'Internet Platforms Weaponizing Chokepoints'. In *The Uses and Abuses of Weaponized Interdependence*, edited by Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, 133–48. Washington, DC: Brookings Institution.

United Nations Conference on Trade and Development (UNCTAD). 2021. 'Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow'. *UNCTAD/DER/2021*. New York: United Nations. https://unctad.org/webflyer/digital-economy-report-2021.

United States Council of Economic Advisers. 2023. 'Economic Report of the President 2023'. Washington, DC: The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/ERP-2023.pdf.

United States Department of Commerce. 2022. 'Global Cross-Border Privacy Rules Declaration'. https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

United States Government Accountability Office. 2021. 'Exposure Notification: Benefits and Challenges of Smartphone Applications to Augment Contact Tracing'. *GAO-21-104622*. 9 September. Washington, DC: United States Government Accountability Office. https://www.gao.gov/products/gao-21-104622.

United States Senate Subcommittee on Fiscal Responsibility and Economic Growth. 2021. 'Hearing: "Promoting Competition, Growth, and Privacy Protection in the Technology Sector"'. Washington, DC, 7 December.

Vaidhyanathan, Siva. 2012. *The Googlization of Everything: (And Why We Should Worry).* Updated ed. Berkeley, CA: University of California Press.

———. 2018. *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford: Oxford University Press.

Valverde, Mariana, and Alexandra Flynn. 2020. 'Introduction: Smart Cities in Canada'. In *Smart Cities in Canada: Digital Dreams, Corporate Designs*, edited by Alexandra Flynn and Mariana Valverde, 7–20. Toronto: James Lorimer Ltd.

van Bekkum, Marvin, and Frederik Zuiderveen Borgesius. 2021. 'Digital Welfare Fraud Detection and the Dutch SyRI Judgment'. *European Journal of Social Security* 23 (4): 323–40. https://doi.org/10.1177/13882627211031257.

van der Burg, Simone, Leanne Wiseman, and Jovana Krkeljas. 2021. 'Trust in Farm Data Sharing: Reflections on the EU Code of Conduct for Agricultural Data Sharing'. *Ethics and Information Technology* 23 (3): 185–98. https://doi.org/10.1007/s10676-020-09543-1.

van Dijck, José. 2014. 'Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology'. *Surveillance and Society* 12 (2): 197–208. https://doi.org/10.24908/ss.v12i2.4776.

van Dijck, José, and Thomas Poell. 2016. 'Understanding the Promises and Premises of Online Health Platforms'. *Big Data & Society* 3 (1): 1–10. https://doi.org/10.1177/2053951716654173.

van Dijck, José, Thomas Poell, and Martijn de Waal. 2018. *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press.

Vanderklippe, Nathan. 2018. 'China's Military Scientists Target Canadian Universities'. *The Globe and Mail*, 29 October. https://www.theglobeandmail.com/world/article-chinas-military-scientists-target-canadian-universities/.

Veale, Michael, and Irina Brass. 2019. 'Public Management Meets Public Sector Machine Learning'. In *Algorithmic Regulation*, edited by Karen Yeung and Martin Lodge, 121–49. Oxford: Oxford University Press.

Venkatadri, Giridhari, Athanasios Andreou, Yabing Liu, Alan Mislove, Krishna P. Gummadi, Patrick Loiseau, and Oana Goga. 2018. 'Privacy Risks With Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface'. In *39th IEEE Symposium on Security and Privacy (S&P)*. Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P): 89–107. San Francisco, United States. https://hal.archives-ouvertes.fr/hal-01955327.

Verdegem, Pieter. 2021. 'Introduction: Why We Need Critical Perspectives on AI'. In *AI for Everyone? Critical Perspectives*, edited by Pieter Verdegem, 1–18. London: University of Westminster Press.

Vervloesem, Koen. 2020. 'How Dutch Activists Got an Invasive Fraud Detection Algorithm Banned'. *AlgorithmWatch* (Blog), 6 April. https://algorithmwatch.org/en/syri-netherlands-algorithm/.

Viitanen, Jenni, and Richard Kingston. 2014. 'Smart Cities and Green Growth: Outsourcing Democratic and Environmental Resilience to the Global Technology Sector'. *Environment and Planning A: Economy and Space* 46 (4): 803–19. https://doi.org/10.1068/a46242.

Waldman, Peter, and Lydia Mulvany. 2020. 'Farmers Fight John Deere Over Who Gets to Fix an $800,000 Tractor'. *Bloomberg.com*, 5 March. https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor.

Walter, Maggie, and Stephanie Russo Carroll. 2020. 'Indigenous Data Sovereignty, Governance and the Link to Indigenous Policy'. In *Indigenous Data Sovereignty and Policy*, edited by Maggie Walter, Tahu Kukutai, Stephanie Russo Carroll, and Desi Rodriguez-Lonebear, 1–20. London: Routledge.

Walter, Maggie, Tahu Kukutai, Stephanie Russo Carroll, and Desi Rodriguez-Lonebear, eds. 2020. *Indigenous Data Sovereignty and Policy*. London: Routledge. https://doi.org/10.4324/9780429273957.

Ward, Jacob W., Jeremy J. Michalek, and Constantine Samaras. 2021. 'Air Pollution, Greenhouse Gas, and Traffic Externality Benefits and Costs of Shifting Private Vehicle Travel to Ridesourcing Services'. *Environmental Science & Technology* 55 (19): 13174–85. https://doi.org/10.1021/acs.est.1c01641.

Warnica, Richard. 2021. 'Ford Government Pledged $2.5 Million to Facedrive for Bracelets to Fight COVID – But Employees Say the Tech "Never Worked Like It Should" How Were So Many Alarms Missed?' *The Toronto Star*, 28 October. https://www.thestar.com/business/2021/10/28/ford-government-pledged-25m-to-a-startup-for-bracelets-to-fight-covid-facedrives-sky-high-value-has-plunged-and-employees-say-the-tech-never-worked-like-it-should-how-were-so-many-alarms-missed.html.

Waterfront Toronto. 2017. 'Request for Proposals: Innovation and Funding Partner for the Quayside Development Opportunity'. Request for Proposals 2017–13. Waterfront Toronto.

Wayland, Michael. 2017. 'GM-Lyft Relationship? It's Complicated'. *Automotive News*, 8 December. https://www.autonews.com/article/20171211/MOBILITY/171219939/gm-lyft-relationship-it-s-complicated.

Weber, Valentin, and Vasilis Ververis. 2021. 'China's Surveillance State: A Global Project'. *Top 10 VPN* (Blog), 3 August. https://www.top10vpn.com/research/huawei-china-surveillance-state/.

Wendt, Alexander. 1999. *Social Theory of International Politics*. Cambridge, UK: Cambridge University Press.

West, Sarah Myers. 2019. 'Data Capitalism: Redefining the Logics of Surveillance and Privacy'. *Business & Society* 58 (1): 20–41. https://doi.org/10.1177/0007650317718185.

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

Westin, A. F. 1967. *Privacy and Freedom*. New York: Atheneum.

Wheeler, Brad. 2022. 'Why Was the Weeknd's Concert Called Off in Toronto? The Doors to Rogers Centre Wouldn't Open'. *The Globe and Mail*, 14 July. https://www.theglobeandmail.com/arts/music/article-why-was-the-weeknds-concert-called-off-the-doors-to-rogers-centre/.

Whitman, James Q. 2004. 'The Two Western Cultures of Privacy: Dignity Versus Liberty'. *Yale Law Journal* 113: 1151–221. https://doi.org/10.2307/4135723.

Williams, Glen. 1994. *Not for Export: Toward a Political Economy of Canada's Arrested Industrialization*. 3rd ed. Toronto: McClelland and Stewart.

Winseck, Dwayne. 2019. 'Internet Infrastructure and the Persistent Myth of U.S. Hegemony'. In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 93–120. Cham: Palgrave-Macmillan.

Wiseman, Leanne, and Jay Sanderson. 2017. 'Accelerating Precision to Decision Agriculture: Enabling Digital Agriculture in Australia'. *Griffith University, USC Australia and Cotton Research and Development Corporation*. https://www.crdc.com.au/accelerating-precision-decision-agriculture.

Wiseman, Leanne, Jay Sanderson, Airong Zhang, and Emma Jakku. 2019. 'Farmers and Their Data: An Examination of Farmers' Reluctance to Share Their Data Through the Lens of the Laws Impacting Smart Farming'. *NJAS: Wageningen Journal of Life Sciences* 90–91 (1): 1–10. https://doi.org/10.1016/j.njas.2019.04.007.

Woodcock, Jamie, and Mark Graham. 2020. *The Gig Economy: A Critical Introduction*. Cambridge: Polity.

World Bank. 2020. *World Development Report 2020: Trading for Development in the Age of Global Value Chains*'. Report. Washington, DC: The World Bank. https://www.worldbank.org/en/publication/wdr2020.

Wu, Tim. 2016. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*. New York: Knopf.

———. 2018. *The Curse of Bigness: Antitrust in the New Gilded Age*. New York: Columbia Global Reports.

Wylie, Bianca. 2022. 'Canada's COVID Alert App Needs to Be Shut Down. Here's Why'. *medium.com* (Blog), 20 April. https://biancawylie.medium.com/canadas-covid-alert-app-needs-to-be-shut-down-here-s-why-dc5037ecdcf.

Wymant, Chris, Luca Ferretti, Daphne Tsallis, Marcos Charalambides, Lucie Abeler-Dörner, David Bonsall, Robert Hinch, M. Kendall, L. Milsom, M. Ayres, and C. Holmes. 2021. 'The Epidemiological Impact of the NHS COVID-19 App'. *Nature* 594 (7863): 408–12. https://doi.org/10.1038/s41586-021-03606-z.

Yates, Charlotte, and John Holmes. 2019. *The Future of the Canadian Auto Industry*. Ottawa: Canadian Centre for Policy Alternatives. February. https://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2019/02/Future%20of%20the%20Canadian%20auto%20industry.pdf.

Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. 2021. 'Regulating Libra'. *Oxford Journal of Legal Studies* 41 (1): 80–113. https://doi.org/10.1093/ojls/gqaa036.

Zhang, Chenchen. 2020. 'Governing (Through) Trustworthiness: Technologies of Power and Subjectification in China's Social Credit System'. *Critical Asian Studies* 52 (4): 565–88. https://doi.org/10.1080/14672715.2020.1822194.

Ziewitz, Malte. 2016. 'Governing Algorithms: Myth, Mess, and Methods'. *Science, Technology, & Human Values* 41 (1): 3–16. https://doi.org/10.1177/0162243915608948.

Zittrain, Jonathan. 2009. *The Future of the Internet – And How to Stop It*. Illustrated ed. New Haven, CT: Yale University Press.

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.

———. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Zuckerberg, Mark. 2020. 'Mark Zuckerberg: How Data Can Aid the Fight Against Covid-19'. *Washington Post*, 20 April. https://www.washingtonpost.com/opinions/2020/04/20/how-data-can-aid-fight-against-covid-19/.

Zweifel-Keeegan, Cobun. 2021. 'A Globalized CBPR Framework: Peering into the Future of Data Transfers'. *The Privacy Advisor* (Blog), 23 November. https://iapp.org/news/a/a-globalized-cbpr-framework-peering-into-the-future-of-data-transfers/.

Zwick, Austin. 2018. 'Welcome to the Gig Economy: Neoliberal Industrial Relations and the Case of Uber'. *GeoJournal*: 679–91. https://doi.org/10.1007/s10708-017-9793-8.

Index

Page references for tables are italicized.

About the Authors

Blayne Haggart is an associate professor of political science at Brock University in St. Catharines, Ontario, Canada, and a senior fellow at the Centre for International Governance Innovation in Waterloo, Ontario. He is the author of *Copyfight: The Global Politics of Digital Copyright Reform* (2014), the co-editor of *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (2019, with Kathryn Henne and Natasha Tusikov) and co-editor of *Power and Authority in Internet Governance: Return of the State?* (2021, with Natasha Tusikov and Jan Aart Scholte), in addition to several journal articles on the subject of the political economy of knowledge. In his pre-academic life, he worked as a reporter and as an economist with the Canadian Parliamentary Information and Research Service.

Natasha Tusikov is an associate professor in the Department of Social Science at York University in Toronto and a research fellow with the Justice and Technoscience Lab (JusTech Lab), School of Regulation and Global Governance (RegNet) at the Australian National University. Her research examines the intersection among law, crime, technology and regulation. She is the author of *Chokepoints: Global Private Regulation on the Internet* (2016). She is a co-editor of *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (2019) and co-editor of *Power and Authority in Internet Governance: Return of the State?* (2021). Her research has also been published in *Surveillance & Society* and *Internet Policy Review*. Before obtaining her PhD at the Australian National University, she was a strategic criminal intelligence analyst and researcher at the Royal Canadian Mounted Police in Ottawa.