1 Introduction: Internet Governance as an Object of Research Inquiry

Laura DeNardis

Why Study Internet Governance?

Governance of the Internet has quickly become one of the most pressing geopolitical issues of the contemporary era. How the Internet is designed and administered implicates a host of public policy concerns such as personal privacy, economic stability, national security, freedom of expression, and digital equality. Governments increasingly discuss issues of Internet governance and cybersecurity in the same breath as other types of global collective action problems such as terrorism, environmental protection, and human rights issues from poverty to child trafficking.

What was once an esoteric set of issues relegated to the technical community and a handful of scholars is now high on the policy agenda of all governments. The reasons for this escalation of interest in how the Internet is administered are absolutely clear. The economic stakes of the digital economy are immense, with all industry sectors dependent on the Internet to function and digital trade measured in trillions of dollars annually. An outage in cyberspace is an outage of the global economy. Internet policies also profoundly affect individual civil liberties and political discourses around elections. Governments have recognized that Internet governance has become a proxy for state power in areas ranging from cyber conflict to systems of filtering and censorship.

A number of Internet conflicts covered extensively in the media—such as Edward Snowden's disclosures about expansive government surveillance, massive data breaches, and Russian hacking during the 2016 US presidential election—have drawn public attention and scrutiny to questions about how the Internet is controlled and administered, whether by content intermediaries like social media companies, by traditional governments, or by

new institutions designed to manage the security and stability of critical Internet resources.

Because of the high stakes of Internet governance questions, there is a tremendous interest in empirical scholarship that provides an evidence base for the decisions of policy makers and the private sector. There is equally a need for scholarship that makes visible to society the sinews of power constructing and controlling the Internet and explaining what the implications are for society and the economy.

There is also an epistemic community of scholars—highly interdisciplinary and distributed around the globe—that self-reflexively identifies as being a global Internet governance research community. The scholarly community has been increasingly organized, at least since the inception of the Global Internet Governance Academic Network (GigaNet) in 2006 and since the rise of interdisciplinary centers on Internet policy, cyber governance, Internet governance, and related initiatives at major universities around the world. Increasing numbers of graduate students, advocacy organizations, academic centers, policy makers, and new kinds of firms that recognize their own Internet policy challenges seek to better understand the choices and implications of how global digital networks are governed.

The defining and original feature of this book is that the topic is research concepts, methods, and frameworks. Numerous books (many by the authors in this book) contain state-of-the-art research *on* Internet governance topics, rather than viewing Internet governance research *as* the topic. How to begin to study Internet governance? This chapter examines the following questions: What is the thing studied when one studies Internet governance? What is the evidence base being examined? Who is studying Internet governance, and what methodologies and conceptual lenses are instructive? This chapter also lays out the organization of the book's chapters—contributed by leading scholars in fields as diverse as law, computer science, communication, science and technology studies, and political science. The rising stakes and increasing visibility of control struggles over Internet governance, as well as the coalescing and increasingly maturing of an interdisciplinary field that epistemically describes what it is doing as Internet governance research, present an important moment of opportunity for this volume.

What Is the Thing Studied When One Studies Internet Governance?

The Internet is and always has been governed, although not in the traditional sense of nation-state governance but in points of coordination and control that cross borders and are distributed among many actors, including the private sector, traditional governmental structures, new global institutions, and sometimes, citizens themselves. Governance is not only about governments. It is enacted via technical design, resource coordination, private ordering, and conflicts at control points.

Internet governance can be generally defined as the administration and design of the technologies that keep the Internet operational and the enactment of policy around these technologies. Beneath the things that humans perceive—content, applications, and devices—when using a network, there are thousands of behind-the-scenes control points. There is no one ideal taxonomy for describing these many points of design, coordination, and control, but one way to organize the functions is as follows (see DeNardis 2014; DeNardis and Musiani 2016):

- Administration of critical Internet resources such as names and numbers
- Establishment of Internet technical standards (e.g., protocols for addressing, routing, encryption, compression, error detection, identity systems, authentication)
- Coordination of access and interconnection (e.g., IXPs, net neutrality, access policies)
- Cybersecurity governance
- The policy-making role of private information intermediaries (e.g., via platform governance, algorithmic ordering, terms of service, computational ordering and decisions by artificial intelligence, and policies about security, speech, reputation, and privacy)
- Technical architecture-based intellectual property rights enforcement

These are all in themselves complex and multivariable points of control, and they overlap in many ways. Any of these tasks can be used to keep the Internet free and open; any can be exploited by governments or the private sector to enact censorship or carry out surveillance. This taxonomy, while capacious, actually bounds the scope of Internet governance as a target of research in important ways. For one, it clearly demarcates Internet governance from the enormous body of Internet studies focusing on how people,

businesses, and governments use the Internet, what they say on the Internet (from the mundane to the political), or how user-centric questions such as identity and representation unfold. Those questions are the purview of the larger context of Internet research—obviously, not meaning how the Internet is used for research but meaning research about Internet usage (e.g., Markham and Baym 2008).

To oversimplify the distinction, whereas much of broader Internet research studies what people express on social media—such as content analysis of political expression on Twitter or issues of identity, representation for marginalized communities, or community formation—Internet governance research studies the mechanisms of control beneath the surface layer of content, such as algorithmic ordering, security, platform affordances, privacy policies instantiated in terms of service, mechanisms to detect fake bot accounts, and the regulatory contexts constraining or enabling all this. There is nothing natural about these distinctions, but there is pragmatic utility in bounding the scope of Internet governance.

As a prelude to interrogating Internet governance research, the following presents five distinguishing features about how the Internet is governed in practice: (1) Technical design and coordination decisions establish public policy. (2) Technologies of Internet governance, as currently designed, cross borders in a way that complicates nation-state jurisdiction. (3) Governance is distributed across multiple actors in a model usually described as private-sector-led, multistakeholder governance. (4) Internet security is both converging and diverging with national security. (5) Internet infrastructure control is now a proxy for political and economic power. Some of these serve as points of reference for this book's chapters, either as part of the conceptual framework or as concepts that are challenged and interrogated as Internet governance research enters its next stage.

Technical Design Enacts Governance

One distinguishing feature of the practice of Internet governance is that the design of technical architecture is a significant force enacting public policy. Therefore, a significant body of Internet governance research studies the underlying technologies of the Internet and how they are designed. For example, the technical design of the Internet's domain name system (DNS) has constructed or enabled certain forms of governance both of the DNS

and by the DNS. As Bradshaw and DeNardis (2016) suggest, among other design features, the DNS embeds names (in the form of domain names) and therefore involves speech conflicts, its hierarchical design creates chokepoints at which content can be blocked, it involves a pool of finite resources (binary Internet addresses) and so raises issues of global distribution, and the requirement for unique names and numbers has necessitated centralized administration to ensure global uniqueness. Much prominent research has focused on the DNS and the systems of institutional control (e.g., the Internet Corporation for Assigned Names and Numbers [ICANN], the Internet Assigned Numbers Authority [IANA], registries, registrars) around this system (e.g., Klein 2002; Kleinwächter 2000; Mueller 2002; Paré 2003).

A significant Internet governance enterprise is the establishment of technical standards for universal formats for how to address, encode, compress, encrypt, and exchange information in a way that is interoperable with other devices and software that adhere to these standards. There are hundreds upon hundreds of core standards, but some of the most well-known are Wi-Fi, HTTPS (hypertext transfer protocol secure), VoIP (voice over Internet protocol), and Bluetooth. These specifications are set by many transnational technical institutions, such as the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF). Standards serve a technical function, but their design also establishes public policy. For example, interoperability standards allow economic competition among private actors and promote innovation and global interconnection. The strength of encryption standards establishes conditions for privacy. Web accessibility standards allow those with hearing, sight, movement, or other impairments to use the Internet.

The technological affordances of information intermediary technologies also enact governance. Information intermediaries are the private platforms (e.g., social media platforms, search engines, messaging platforms, access providers, and cloud computing companies) that enable the exchange and aggregation of content. Design features such as tracking mechanisms, real-name identification requirements, and decisions about anonymity construct rights in the same way that the terms of service of these systems construct the conditions of individual civil liberties such as speech rights, privacy, and data ownership.

Cross-Border Technologies and Bordered Policy Often Conflict

Policy making that seeks to stay within national borders does not necessarily stay within national borders. For example, the European Union's General Data Protection Regulation (GDPR) has affected companies that do business all over the world and has affected cross-border technologies such as the WHOIS system, a database of global registered domain holders. Local policies, such as the GDPR, the right to be forgotten rule, and data-localization policies, have global effects because the underlying technologies of the Internet—interconnection points, cloud computing infrastructures, content distribution networks, the DNS—do not correspond to the borders of these local policies.

Yet one political reaction to the growth and success of the Internet, the technological reality of cross-border technologies, and the market reality of private companies shaping human rights online is the rise of cyber sovereignty approaches in which countries are seeking to exert greater control over the Internet. In many cases, they are seeking to impose nation-state borders over the distributed architecture of the Internet. Russia, China, and some other countries have been proponents of cyber sovereignty under the guise of social order, with China's efficient system of content censorship and filtering perhaps the best example.

A long-standing debate in Internet governance involves those advocating for greater government control of the Internet, such as the cyber sovereignty models, and those advocating for the preservation of technical governance that is distributed over actors including international organizations, traditional governance structures, the private sector, new global institutions, and civil society. This has led to many international governance controversies, from debates over international telecommunications regulations at the International Telecommunication Union's World Conference on International Telecommunications in Dubai in 2012 to the controversial and long-coming transition of power from the US Commerce Department to ICANN in overseeing the IANA functions.

While the Internet has always been subject to national statutory contexts, its distributed architecture and other technical features make implementing individual national laws difficult in practice. Transnational private companies have to deal with unique legal requirements in all the markets in which they operate or even simply where users might access their services. Governments are also increasingly establishing policies that place constraints

on technical infrastructure arrangements. For example, relatively new data-localization laws are in place from Russia to Latin America to Asia that place restrictions on how customer information is stored, often requiring data to reside on servers within a country's borders. These policies affect not only traditionally tech companies but any company (e.g., financial services, retail) that stores customer data. Some of these policies arose over concern about citizen privacy and foreign surveillance, but they create complications from an engineering, human rights, and business model standpoint. Concentrating data in one place can actually make it more difficult to protect personal privacy. These requirements also do not map onto the distributed technical design of the Internet or the ways in which content delivery networks (CDNs) decentralize and distribute data around the world. This is one example of the tension between national governance contexts and the distributed nature of the Internet.

The Privatization of Governance and the Multistakeholder Model

The term "Internet governance" is, in some ways, an oxymoron. The power to control and govern the Internet is distributed among private industry, global institutions like ICANN and the IETF, and in some cases by civil society, as well as by governments. This form of distributed governance is often called multistakeholder governance and involves functions such as technical-architecture-based enforcement of intellectual property rights, the private policies of technical intermediaries, the administration of the DNS and Internet names and numbers (i.e., IP addresses), cybersecurity coordination, and the establishment of Internet standards. Collectively, these tasks keep the Internet operational and enact policies that directly establish the conditions of innovation and civil liberties in the digital sphere.

A major line of inquiry in Internet governance studies involves questions about the nature and legitimacy of multistakeholder governance arrangements and the appropriate balance of powers among actors at the various layers of Internet coordination. Frankly, it is not yet a well-understood or much-analyzed framework of governance. There are many models and many contexts of multistakeholder governance. Drawing from John Ruggie's pioneering study of multilateralism, Raymond and DeNardis (2015) offer a taxonomy of different types of multistakeholder institutional forms that vary according to what combination of actor class is participating and the nature of the authority relations among these actors. The international

relations scholar Joseph Nye Jr. describes Internet governance as a "regime complex," applying regime theory to Internet governance to explain the constellation of institutions, actors, norms, and policies that collectively constitute distributed, multistakeholder governance. As Nye explains, Internet governance involves "a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages" (Nye 2014, 9).

A critical point for understanding Internet governance is that there is not a single system of oversight and coordination but an entire constellation of functions, each overseen by different governance structures distributed over one or more actors. Collectively, this administration and coordination of the technologies necessary to keep the Internet operational and the heterogeneous policies enacted around these technologies is viewed as distributed, multistakeholder governance, even if in practice multistakeholder arrangements rarely match the rhetoric around multistakeholderism. Thus, scholars study the policy-making role of private industry (DeNardis 2014; Gillespie 2014; MacKinnon 2011), national and international law (Goldsmith and Wu 2006; Weber 2010), technical coordination institutions (Klein 2002; Kleinwächter 2000; Mathiason 2008; Mueller 2002), international organizations (Levinson and Marzouki 2015), and as mentioned in the previous section, technical design itself (Braman 2011; DeNardis 2009).

Internet Security Is Converging and Diverging with National Security

There has long been a peculiar rhetorical distinction between "cyber" and "Internet" for historical and cultural reasons beyond the scope of this book. A person using the term "cyber" often refers to cybersecurity or national security domains of Internet warfare and international relations. Using "Internet" refers to either digital economy issues, the free and open Internet, or the Internet of Things (IoT).

From an engineering perspective, the distinction makes no sense, because the underlying infrastructure is the same, and when using "Internet governance" this book does not imply a distinction between cyber issues and Internet issues. They are the same.

It may be helpful, however, to acknowledge the ways in which the discourses and communities of practice around these nomenclatures are both converging and diverging, because this helps illustrate another feature of

Internet governance: that points of control are points of mediation between often-conflicting values.

Internet security and national security, on one hand, are converging because the stability of the economy, democracy, and public sphere is now completely predicated on Internet stability and security. Every sector of the global economy is digitally mediated and in some way connected to the public Internet. Security breaches have significant effects on basic societal functioning. Ransomware attacks have cryptographically locked and therefore crippled health care systems until the affected institutions succumb to paying ransom, usually in the form of Bitcoin. High-profile, massive consumer data breaches such as those at Equifax, Target, and the Office of Personnel Management have chilling effects on citizen trust in the digital economy and sometimes chilling effects on speech and behavior online. Even more significant, the proliferation of the IoT raises the stakes for security because an outage or disruption of cyber-physical systems can mean the loss of life and not just loss of access to communications. Stable systems of democracy also increasingly require strong cybersecurity, considering the stunning disclosure by US intelligence agencies about Russian probing of voter rolls and other cyber incursions during the 2016 US presidential election.

On the other hand, cybersecurity and national security are diverging. Other security trends, such as governmental stockpiling of zero-day exploits and the rise of cyber offensive capabilities such as the Stuxnet code targeting Iranian nuclear reactors, speak to cyber as the fifth domain of warfare and the emerging front for conflict between nation-states. The need for strong security for the digital economy and for individual privacy and trust in cyberspace comes into conflict with national security requirements for law enforcement, intelligence gathering, and the amassing of cyber offense capability. The clash of market-driven trends toward greater encryption with law enforcement requirements for access to data materialized in the aftermath of the San Bernardino, California, terrorist attack when authorities sought access to an encrypted Apple smartphone belonging to the attacker. Values are always in tension around Internet control points.

Control of Internet Governance Infrastructure Is a Proxy for Political Power

Global conflicts over control of cyberspace have existed at least since the commercialization and internationalization of the Internet. One prominent

example was the long-standing geopolitical contention over the US Commerce Department oversight of names and numbers, including its contractual arrangement with ICANN and authority over changes to the root zone file, until this unique US coordinating function was transitioned to the global multistakeholder community. As the Internet's importance to the economy and the political sphere has increased, so has contention over the infrastructure of the Internet.

Governments and other forces recognize that power over technical infrastructure points of control can serve as a proxy for control of ideas, the economy, and the political sphere (DeNardis 2012; Musiani et al. 2016). For example, the DNS has become a tool of content control—for example, used by China's extensive censorship system and used to block access to sites that illegally share pirated content or sell counterfeit products. Encryption standards and implementations, historically always politically charged, have increasingly become targets of governments wishing to weaken or create backdoors to cryptography for national security or intelligence purposes, in some cases pitting law enforcement values against the need to provide strong security for the digital economy. As with all areas of Internet governance, battles over control of infrastructure are sites of conflict among competing values and interests.

The Ensuing Challenge to Internet Governance Scholarship

The preceding five themes in Internet governance practice translate directly into challenges, ab initio, for Internet governance research. A goal of this book is to demonstrate how to overcome clear research challenges in studying Internet governance.

Making the invisible visible. The technical architectures and institutions of governance are not visible in the same way that Internet content and usage is visible to end users. Scholarship has to excavate and make visible these hidden infrastructures, in some cases, before research even commences.

Understanding complex technologies. Studying the design and governance of the Internet requires understanding the underlying technologies. Technologies of Internet governance include thousands of protocols, platforms, algorithms, systems of routing and interconnection, the DNS, encryption standards, the Internet of things, and public key cryptography and other authentication mechanisms. These systems constitute the underlying infrastructure

supporting both cyberspace and the integrated cyber-physical world. The application of machine learning and artificial intelligence as mechanisms of governance further complicates the topic of study. This complexity of technologies either enacting governance or being governed requires scholars, regardless of discipline, to have a proficient technical understanding of how stuff works.

The difficulty in studying the private sector. The private sector owns and operates the vast majority of the Internet's infrastructure and platforms, further complicating access to data and sometimes concealing technology in proprietary enclosure such as algorithms protected by trade secrecy or standards-based patents.

Navigating conflicting values. Because Internet governance points of control are increasingly political points of control, scholarship about these conflicts often takes on a normative stance. Even the choice of what to study in Internet governance intervenes. Almost every question of Internet governance embeds conflicting values, such as law enforcement versus individual civil liberties, privacy versus free speech, technical expediency versus security, surveillance capitalism versus privacy, and consumer safety in the IoT versus economic competition. Is a universal and interoperable Internet desirable or does a fragmented Internet that, for example, isolates industry-specific IoT applications have advantages? Even if objectivity in research is possible, Internet governance research, especially considering the high stakes to society, often involves some type of a normative stance, such as the assumption that a free and open Internet is desirable.

Multistakeholder governance and multistakeholder research. Because of how technology crosses borders and because even local governance decisions can have global effects, studying any one actor or issue area can sometimes miss important contextual or empirical factors. At the same time, collaborative research initiatives that combine input from actor classes have promise for tackling very large issue areas.

Overstudying open systems. The traditions of Internet governance in practice have been generally open in that dominant coordinating institutions like the IETF and ICANN allow participant observation and have made proceedings and mailing lists generally accessible relative to other more insular institutions. Because of the availability of more data, these institutions and underlying systems are asymmetrically overstudied relative to systems involving greater proprietary enclosure. The institutions that are more

closed, including consortia and institutions in many emerging areas of technology, are very difficult to study.

Research often involves creation of technological tools. Because of the massive size and complexity of Internet infrastructure, as well as the need to sometimes digitally reach across borders to gather data, research often involves software mediation and the coproduction of technological tools. This is especially the case for studies that assess politically motivated outages and cybersecurity incursions but also for studies of how traffic flows through interconnection points and for large-scale network analysis of all kinds.

Who Studies Internet Governance and How Do They Study It?

Internet governance researchers excavate and examine the invisible Internet control points and the social, economic, and political implications of these control points. Internet governance research, commensurate with Internet governance itself, is hardly a monolithic practice but, rather, made up of discipline-independent but interacting fields as well as intrinsically interdisciplinary fields such as science and technology studies and communication studies.

The methodological approaches and tools are diverse: large-scale text analysis, network analysis, traditional statistical methods, discourse analysis, participant observation, interviews, and ethnomethodologies of all kinds. Even among this diversity, there is clearly an epistemic community of interdisciplinary scholars who have studied dimensions of Internet governance for decades but perhaps most visibly coalescing with the founding of the GigaNet in 2006 just before the inaugural United Nations Internet Governance Forum in Athens. In other words, scholars from law, economics, history, political science, science and technology studies, sociology, and beyond self-reflexively situate what they are doing as Internet governance research.

Because of the technical complexity of systems of Internet architecture governance, many of these scholars have a strong background knowledge in computer science, engineering, information technology, and specific expert knowledge about the Internet's underlying technical architecture. Indeed, this technical expertise, even when one studies laws (about technology), institutions (that design and administer technology), or private ordering (the companies that own and operate the Internet).

Research is often policy engaged or policy adjacent. Internet governance researchers are interested in real-world problems and the opportunity for creating an evidence base for policy decisions. Not surprisingly, policy initiatives have directly engaged researchers and commissioned work on specific topics. For example, the Global Commission on Internet Governance, a two-year initiative chaired by Carl Bildt, a former prime minister of Sweden, included the global, interdisciplinary Research Advisory Network that produced more than 50 original research papers in six research volumes on cybersecurity, fragmentation, access and interconnection, and more (Global Commission on Internet Governance 2016–2017).

A related feature of this research is that it sometimes overlaps with the practice of Internet governance. Scholars have been actively involved as participants in ICANN working groups, contributing to standards-setting initiatives, moving between higher education and policy appointments, serving as advisors to policy makers, and sometimes serving as consultants to industry. This translational and pragmatic role of some scholars is similar to scholarly engagement in other topical disciplines that engage in great problems in contemporary society.

One could divide Internet governance research in many ways—disciplinary approach, topical area of study, research methodology, or thematic or conceptual framework. The editors of this volume choose to highlight some disciplinary perspectives on studying Internet governance. Although a wide variety of fields—from computer science to political science to science and technology studies—are included in this book, it is of course a single volume and thus not sufficiently inclusive of all disciplines. The authors were selected according to who could provide a diversity of perspectives and are influential Internet governance thought leaders in their respective fields.

The book commences with historically grounded chapters by two experts in Internet governance and communication policy. In chapter 2, "The Irony of Internet Governance Research: Metagovernance as Context," the information policy expert Sandra Braman sets the stage by broadly defining Internet governance as including "not only efforts to regulate institutional, communal, and individual practices, content, and uses by geopolitically recognized governments but also decision-making and efforts with regulatory effects by private sector entities, whether those that have a legal status (such as third-party intermediaries that have legal identities as corporations) or those that do not (such as autonomous networks)."

Her chapter then situates questions of Internet governance in the longer trajectory of network regulation and socio-technical governance and explains how Internet governance entanglements are challenging concepts such as liability, governance, the rule of law, and the state. In chapter 3, "Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field," Milton Mueller and Farzaneh Badiei examine the emergence and trajectory of Internet governance as a label, as an area of scholarly study, and as a real-world policy arena and explore the interplay among these spheres.

To policy makers and some scholars, Internet governance is too often exclusively understood through institutional lenses—governments, private companies, systems of politics, international organizations, ICANN, the IETF, and so on—with less attention to the agency and affordances of technology itself. The Internet at its core is a collection of technologies—protocols, routing and addressing infrastructures; physical equipment like fiber-optic cable, antennas, switches, and interconnection sites; algorithm-driven platforms; the DNS; applications; code; firewalls; encryption; and the like. Arrangements of technology are also arrangements of public policy. Not surprisingly, then, the field of science and technology studies (STS) has been influential in examining and making visible the reciprocal relationship between, on one hand, technologies of Internet governance and architecture and, on the other, society and the economy. Francesca Musiani explains the contributions and perspective of STS in chapter 4, "Science and Technology Studies Approaches to Internet Governance: Controversies and Infrastructures as Internet Politics." The chapter pays particular attention to how studies of controversies contribute to understandings of Internet governance. Most notably, and speaking to the urgent need to look beyond institutional frames, Musiani explains how STS perspectives—and especially approaches to infrastructure studies—examine the agency of nonhuman actors and the mediating governance role of infrastructure.

Some of the early US legal writing about Internet policy, such as Lawrence Lessig's influential book *Code and Other Laws of Cyberspace* (1999), conceptually followed STS themes, especially highlighting the ways in which technical architecture (as well as law, norms, and markets) shapes and constrains society. As the Internet became commercialized and globalized, legal scholars have continued to produce important Internet governance work on every imaginable subtopic of Internet governance, whether trademark concerns in the DNS, intellectual property rights protection

online, or privacy laws. One of the challenges inherent in legal studies of Internet governance is that Internet technologies and institutions do not neatly reside within national borders. In chapter 5, "A Legal Lens into Internet Governance," legal scholar Rolf H. Weber helps explain the challenges and the ensuing considerations of legal harmonization, legitimacy, and multistakeholder legitimacy in spheres of Internet governance.

The perspectives of computer scientists have contributed greatly to understandings of how the Internet is controlled and what is at stake. This book includes a chapter from a prominent team of computer science researchers from the Web Science Institute at the University of Southampton: Wendy Hall, Aastha Madaan, and Kieron O'Hara. In chapter 6, "Web Observatories: Gathering Data for Internet Governance," they take up the question of the study of governance over the flow of data and content in the web ecosystem. They discuss the challenges of developing and re-creating methods for ethical and secure data gathering and sharing, and they propose an architecture for doing so.

Policy makers rely (or should rely) on analysis of empirical data in all areas of Internet policy, including cybersecurity, but sometimes these data (and analyses) can be inadequate to reliably inform policy-making decisions. Quantitative political science research sheds light on Internet governance trends and problems. One challenge in this arena is that the thing being studied continually expands and changes, making examinations intrinsically multivariable and also difficult to replicate as data change. The political science professor Eric Jardine takes up these challenges in chapter 7, "Taking the Growth of the Internet Seriously When Measuring Cybersecurity." Jardine addresses the lack of statistical normalization and other challenges such as the failure to control for "lurking confounders."

Another question in Internet governance research is how to study the private sector, which owns and operates the majority of cyber infrastructure and establishes policies through design of systems, terms of service, and institutional decisions that, in effect, govern. These private intermediaries include social media platforms, Internet service providers, content distribution networks, cloud computing providers, private DNS resolution providers, and many other categories of industry. An entire generation of doctoral student researchers across various disciplines is interested in studying this privatization of Internet governance instantiated in the decisions of intermediaries. Carrying out research projects about the privatization of governance

is challenging because it requires access to often closed and possibly even trade-secrecy-protected data.

The methods for studying the surface area of content are well established, but there is much more research fluidity and difficulty in studying what is beneath content, the hidden mechanisms and sinews of power controlling the flow of content and establishing conditions for human rights and innovation. For example, interviews with leading thinkers from the private sector sometimes are governed by nondisclosure agreements, underlying algorithms and other control mechanisms are protected by trade secrecy laws, and infrastructures are increasingly shrouded in proprietary enclosure. The Danish human rights researcher Rikke Frank Jørgensen takes up the question of studying Internet governance by private intermediaries in chapter 8, "Researching Technology Elites: Lessons Learned from Data Collection at Google and Facebook."

Studying content itself, however, is a critical area of Internet governance research and one that involves enormous data stores: media coverage of Internet governance topics, terms of service, deliberations about Internet governance, and so on. There are enormous quantities of text that can help elucidate Internet governance problems, understandings and misunderstandings, and solutions. Thus, research that uses text mining contributes greatly to examining the Internet governance ecosystem. Derrick Cogburn addresses this topic in chapter 9, "Big Data Analytics and Text Mining in Internet Governance Research." He studied 12 years of transcripts of the UN Internet Governance Forum to illuminate core themes and issues over time and determine the utility of text mining and big data analytics in Internet governance research on all topics, from censorship to cybersecurity.

The sheer volume of deliberations and discussions that feed into decisions about the design and administration of Internet architecture is massive. Because of the traditions of openness, transparency, and participation in Internet design communities, much (but not all) of this deliberation happens in the open and is archived in mailing lists, meeting minutes, and other online repositories. The Internet governance scholars Niels ten Oever, Stefania Milan, and Davide Beraldo address the topic of mailing-list research in chapter 10, "Studying Discourse in Internet Governance through Mailing-List Analysis." The authors explain the utility of and opportunity for interrogating mailing-list archives and propose a mixed-methods approach, a hybrid of computational and interpretive tasks.

Arguably the most societally consequential area of inquiry around governance of the Internet is cybersecurity. The global economy is completely digitally mediated and therefore dependent on the security and stability of networks. Privacy requires strong encryption. Consumer safety now depends on security of the IoT. Democracy requires not only secure voting systems but secure voter rolls and email. Free speech requires circumvention tools that provide freedom from filtering and censorship. Web queries require public key encryption. Online transactions require strong authentication. The study of cybersecurity governance is possibly the most critical area of Internet governance research because every other area depends on the security and stability of networks. The leading Internet governance researcher in this area is probably Citizen Lab director Ron Deibert, whose work has been groundbreaking because it has required the development of new technical tools as part of researching Internet governance. In chapter 11, "The Biases of Information Security Research," Deibert raises a critical point: even a highly technical area such as cybersecurity is politically contested and shaped by a constellation of economic and social factors that construct what research gets done. Chapter 11 raises questions of epistemology as much as methodology.

Dominant Internet governance discourses, as they have been constructed by those with a stake in the outcome of many tangible policy debates, have ideologies. For example, China and Russia have increasingly espoused an ideology of cyber sovereignty that advocates for strong nation-state control of the Internet in the name of order and as a reflection of authoritarian tendencies toward information and communication technologies. In the West, the collective coordinating tasks that keep the Internet operational have been cast, with some descriptive accuracy, as private-sector-led, multistakeholder Internet governance. But in the same way that cyber sovereignty embeds an ideology and privileges an approach, multistakeholder governance advocacy has been adopted as a way, for some, to oversimplify Internet governance as a monolithic practice or to preserve hegemonic power for dominant institutions.

In chapter 12, "The Multistakeholder Concept as Narrative: A Discourse Analytical Approach," a leading Internet governance scholar, Jeanette Hofmann, examines how narratives and imaginaries, including those emanating from academic research, are significant constructors of policy discourses. As Hofmann suggests, there is often a disconnect between expectations of

multistakeholderism and how this model performs in practice. She explains how discursive representations of such concepts in Internet governance, including those coconstructed by the academic community, take on various utilities. The chapter addresses a critical subject but also helps emphasize the place of discourse analysis in Internet governance scholarship.

The book concludes with chapter 13, "Toward Future Internet Governance Research and Methods: Internet Governance Learning," in which Nanette Levinson draws from related research arenas to elucidate what foundations can inform the future of Internet governance research and methods.

Both "Internet" and "governance" are malleable terms whose meanings are in flux, especially as it becomes more and more difficult to define what the Internet is, whether based on underlying technical architecture, user communities, or underlying values. More "users" are bots and things than people. More networks increasingly depend on proprietary protocols, especially in cyber-physical systems, rather than open protocols such as TCP/IP (transmission-control protocol/Internet protocol). The Internet in China bears no resemblance to the Internet in Sweden. Acknowledging the spectrum of technologies, the conflicts between values, and the fragmentation of the Internet that already exists does not negate the descriptive reality of the present moment. The constellation of governance and control issues around the Internet now determines conditions of privacy, speech, innovation, and the security and stability of the digital economy. Internet governance researchers seek to shed light on these critical decision points that will shape society for an entire generation.

References

Bradshaw, S., & DeNardis, L. (2016). The politicization of the Internet's domain name system: Implications for Internet security, universality, and freedom. *New Media & Society, 20*(1), 332–350.

Braman, S. (2011). The framing years: Policy fundamentals in the Internet design process, 1969–1979. *The Information Society, 27*, 295–310.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: MIT Press.

DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society, 15*(5), 720–738.

DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance*. New York, NY: Palgrave MacMillan.

Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. Boczkowski, & K. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society* (pp. 167–194). Cambridge, MA: MIT Press.

Global Commission on Internet Governance. (2016, December 7). *A universal Internet in a bordered world: Research on fragmentation, openness and interoperability* (Research Vol. 1). Retrieved from https://www.cigionline.org/publications/universal-internet-bordered-world-research-fragmentation-openness-and-interoperability

Global Commission on Internet Governance. (2017, January 7). *Who runs the Internet? The global multi-stakeholder model of Internet governance* (Research Vol. 2). Retrieved from https://www.cigionline.org/publications/who-runs-internet-global-multi-stakeholder-model-internet-governance

Global Commission on Internet Governance. (2017, May 8). *Mapping the digital frontiers of trade and intellectual property* (Research Vol. 3). Retrieved from https://www.cigionline.org/publications/mapping-digital-frontiers-trade-and-intellectual-property

Global Commission on Internet Governance. (2017, June 23). *Designing digital freedom: A human rights agenda for Internet governance* (Research Vol. 4). Retrieved from https://www.cigionline.org/publications/designing-digital-freedom-human-rights-agenda-internet-governance

Global Commission on Internet Governance. (2017, July 26). *Cybersecurity in a volatile world* (Research Vol. 5). Retrieved from https://www.cigionline.org/publications/cyber-security-volatile-world

Global Commission on Internet Governance. (2017, July 26). *The shifting geopolitics of Internet access: From broadband and net neutrality to zero-rating* (Research Vol. 6). Retrieved from https://www.cigionline.org/publications/shifting-geopolitics-internet-access-broadband-and-net-neutrality-zero-rating

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, UK: Oxford University Press.

Klein, H. (2002). ICANN and Internet governance: Leveraging technical coordination to realize global public policy. *The Information Society, 18*(3), 193–207.

Kleinwächter, W. (2000). ICANN between technical mandate and political challenges. *Telecommunications Policy, 24*(6–7), 553–563.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.

Levinson, N. S., & Marzouki, M. (2015). IOs and global Internet governance interorganizational architecture. In F. Musiani, D. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 47–72). New York, NY: Palgrave MacMillan.

MacKinnon, R. (2011). *Consent of the networked: The world-wide struggle for Internet freedom*. New York, NY: Basic Books.

Markham, A., & Baym, N. (Eds.) (2008). *Internet inquiry: Conversations about method*. Thousand Oaks, CA: Sage.

Mathiason, J. (2008). *Internet governance: The new frontier of global institutions*. New York, NY: Routledge.

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.

Musiani, F., Cogburn, D., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in Internet governance*. New York, NY: Palgrave MacMillan.

Nye, J. S. 2014. *The regime complex for managing global cyber activities*. Global Commission on Internet Governance Paper Series (Paper no. 1). Centre for International Governance Innovation/Chatham House.

Paré, D. (2003). *Internet governance in transition*. Lanham, MD: Rowman & Littlefield.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory, 7*(3), 572–616.

Weber, R. H. (2010). *Shaping Internet governance: Regulatory challenges*. Berlin, Germany: Springer.