2 The Irony of Internet Governance Research: Metagovernance as Context

Sandra Braman

Even though reality
may not exist,
we have a right to it.[1]

Information policy—laws and regulations pertaining to any aspect of information creation, processing, flows, and use or, more colloquially, law and policy for information, communication, and culture—matters because it creates the context within which all other decision-making takes place. Internet governance, a form of information policy, matters in particular: it provides the context for much of that context, as the Internet is a "pan-medium" (Theall 1999), infrastructure for all forms of communication previously mediated by distinct technologies for which, historically, laws and regulations were differentially developed, interpreted, and applied. Critically, "all other decision-making" includes the processes of governance themselves.

At the close of the second decade of the 21st century, when profound challenges to rule of law are underway around the world, Internet governance researchers must grapple with the effects of the uses of this sociotechnical system—and of decisions about what those uses might be, how they might proceed, and what the consequences are likely to be—on governance itself. This chapter situates Internet governance research relative to the nature of governance and metagovernance more broadly, taking steps toward a research agenda by identifying questions raised by these developments. Additional theoretical and conceptual work is needed to provide a foundation for analysis of dimensions not historically considered but fundamental to arguments and operations in a world of algorithmic agency and digital structure.

The chapter concludes with a few thoughts on humility, which brings us to irony; in Samuel Beckett's (1953/2012) words, "I can't go on, I'll go on." Bob Jessop (2016) uses the term "irony" to refer to analyzing, making, and implementing policy in the face of knowledge that, ultimately, all governance efforts will fail. For those who study network policy, his use of the concept appropriately resonates with Robert Britt Horwitz's *The Irony of Regulatory Reform* (1989), a model of network policy analysis that is fully imbued with the role of networks as agents as well as subjects of power, deeply involved in transformations of the state.

The Internet and Governance

Relationships between the Internet and governance go both ways. As DeNardis and Musiani (2016) succinctly put it, there is governance *of* the Internet, and there is governance *by* the network. The latter includes structurational and constitutive effects of Internet design and policy, whether direct and evident or indirect and needing analysis to become visible, as well as uses of the Internet as policy tools. The same elements can serve both "governance of" and "governance by" functions (Merrill 2016).

Many of the questions those involved in Internet governance engage are not new. Some are. It can take deep knowledge of history to know which questions are which; neither legal nor discursive silos help. In one example of their cost: the first edition of the *Tallinn Manual* (Schmitt 2013), the NATO-sponsored effort by international legal experts to determine whether and how existing international law pertains to cybersecurity and cyberwarfare, ignored network-specific treaties altogether. By the time of the second volume, *Tallinn Manual 2.0* (Schmitt 2017), the experts involved had apparently been exposed to Anthony Rutkowski's (2011) history of the treatment of what we now call cybersecurity issues beginning with the first international telecommunications treaties in the mid-19th century. Including this domain of international law in the *Tallinn 2.0* analysis affected a number of conclusions reached, but that came several years after the first volume had been released to inform other national and international decision-making.

Whether the questions Internet governance researchers face are new and unique to the context or not, the conditions of the world for which decisions are being made are qualitatively new in many ways, some of which we are only now beginning to discover and others of which are yet to come

or may remain indiscernible. Even before the turn toward political extremisms of the first decades of the 21st century, the conditions under which we operate, and how we operate, had been changing in often radical ways and becoming increasingly turbulent—so much so that political scientists feel driven to add the prefix "meta-" to the words they are using as they think about what is going on. Whether the conversation starts with what is happening to the state (government), or whether it starts from what governs in a particular area of social life (governance), it leads to metagovernance. Indeed, as Meuleman (2008) demonstrates, quite different intellectual traditions wind up in essentially the same place in this regard. Metagovernance involves establishing system parameters and determining what can happen within and between systems. Information policy, including Internet governance, is inherently parametric policy, a matter that Lawrence Tribe (1985) notes makes it constitutional in nature within US law and that Jessop (2011) identifies as so important that engagement with parametric issues is itself one of the five types of metagovernance in his handbook chapter on that concept. It includes material as well as normative structures, making Internet governance infrastructure in this additional way for all other forms of metagovernance and governance, too.

The keystone works on the state and governance of recent years referred to in this chapter were published before the 21st century ruptures in countries around the world. That does not lessen our responsibilities as Internet governance researchers. This section looks briefly at some of the theoretical literatures that have been or could be useful for thinking about Internet governance within the larger context of the evolution of forms of governance and metagovernance before turning to the regime theory that is important to several other chapters of this book—and at its limits.

Theoretical Context

This is a world in which theoretical pluralism is not only preferred but a necessity. Jessop (2016) presents several theoretical approaches to study of the state, all of which he argues have validity and importance. We should not expect the directions in which things evolve to be singular. At their extremes, as Marshall McLuhan notes, the effects of the use of information and communication technologies can simultaneously be opposite in nature (McLuhan and McLuhan 1992). Where there are singularities, rationalities can bifurcate (DeLanda 1991). The causal processes that get us from here to

there are not necessarily linear, despite either desire or perception (Martine 1992). Where positivists would look for determinism, matters may well be stochastic. Policy concepts that have been useful in the social environment may not be so on the technical side, or may yield quite different outcomes (Edwards and Veale 2017).

The characteristics that make informational metatechnologies such as digital technologies qualitatively distinct from modern technologies and premodern tools (Braman 2002) have transformed the nature of the matériel through which system transformations take place (Archer 1982, 1984; Giddens 1984) to such an extent that whether something is agent or structure can often now be a matter of choice. This identifies an Internet governance research agenda of its own. We have long been aware of the agency/structure choice when it comes to intellectual property rights, a domain in which manufacturers can often put the same capacities into either software or hardware, respectively relying on either copyright or patent for protection. David D. Clark (2018) identifies and explains other significant areas in which the option is available in ways that have governance implications as we work on the "future Internet."

McKelvey's (2018) work on daemons, a concept important in technical design of what we now call the Internet from the earliest years of that process (Braman 2011), draws our attention to network potentialities that are unseen and unknown for most users, latent until they become active. This gives us a user-, rather than network-, oriented approach to thinking about the technical environment and what it is like to live as a human within a world of algorithms. The development of positive policy recommendations for a daemon-filled world of the type described by McKelvey leads in the direction of capabilities, so persuasively introduced to information policy by Julie Cohen (2012). There is work to be done here.

Regime Theory

The regime theory relied upon by a number of authors in this book was developed by political scientists as a way of thinking about international relations in issue areas where things were generally working but for which there was no existing international law—and, when it came to digital network matters, often no existing national law, either. The rising salience of such issues was reflected by policy analysts, many of whom shifted their attention from government to governance during the 1990s (Bache et al.

2015). Working with the framework as classically presented by Krasner (1983), Cowhey (1990) was the first to explicitly use regime theory in analysis of telecommunications policy. Mueller's (2004) work comparing the Internet and satellite governance mechanisms provides another example in network policy terrain. It is useful in analysis of a number of specific information policy issues raised within the context of the Internet as well (Braman 2004a, 2004b). Drezner (2009) and Nye (2014) are frequently referred to by those who explicitly apply this approach to Internet governance. Although regime theory was initially conceived of in regard to international relations, it has been taken up for use at other levels of social and governance structures, all the way down to the municipal level (Coletta and Kitchin 2017)—also matters of Internet governance because, as we know from Star and Ruhleder (1996), it is in its local manifestations that infrastructure comes into existence. It would be valuable to have a mapping of the multiple levels at which regime formation and transformation are now taking place in ways that are pertinent to—or comprise—Internet governance across all these levels.

A corollary of regime theory is that private sector agents are explicitly and openly—rather than begrudgingly, critically, and/or with hesitation—included within policy analysis. International law firms, hired to craft contracts for network-reliant and globally active clients, were already playing significant roles in thinking about legal arrangements for transnational digital information flows in the 1980s (see, e.g., Bruce, Cunard, and Director 1986), influencing public law affecting the Internet in inevitably path-dependent, if not precedential, ways. A related set of processes was underway in the network-intertwined industry of finance (Dezalay and Garth 1996). What would the kind of analysis undertaken by Dezalay and Garth on finance yield if undertaken on the role of such players in Internet governance?

As regime experience accumulates, working rules can become formal law, and norms can become foundational or operational principles. The kinds of learning Levinson talks about in her concluding chapter 13 of this book are among those involved. How do formal processes of Internet-specific institutions impede or encourage such learning? How useful is regime theory under conditions in which learning does not apply, whether because it is in a postlaw rather than prelaw context, or because rule of law has collapsed?

Regime theory involves governance under conditions of invention, evolution, or transition that can reify, whether as laws and regulations of

geopolitically recognized states or through other means. Regime theorists typically assume incremental change in political and legal conditions, and that what are perceived to be very rare possibilities need not be taken into account. We now know, though, that change can be radical rather than incremental, sudden rather than slow, and that the outlier possibility may be the one we have to live with. Those doing Internet governance research need to be thinking about what happens under conditions of exception, of crisis, of turbulence, and of chaos. What role does Internet governance play in abuses of human rights and civil liberties? What roles might it play in preventing or mitigating such abuses? The burgeoning global community of researchers focused on resilience should be an important venue, and set of collaborators, for Internet governance researchers. The UN Sustainable Development Goals are now commonly being taken into account across issue areas; how might that be done with Internet governance research, following in the footsteps of Rajnish et al. (2017)?

Implications for Internet Governance Research

These elements of the theoretical context for Internet governance research make the terrain for this book's authors a set of "meta" questions. What kind of research do we need to help design infrastructure for imagining, desiring, and creating governance systems for the world that we irrevocably, and together, now inhabit? How can we understand effects of policy decisions that are stochastic and iterative in nature, much like financial derivatives, with declining degrees of confidence in predictability? How should we govern governing? The next section provides some foundational definitions for addressing such questions.

Definitional Basics

The concepts of the Internet and of Internet governance are addressed here. Discussion of the intervening concept of governance includes attention to metagovernance as well.

Internet

I join Abbate (2017) and Russell (2017) in the analysis that we are nearing the end of the period during which the concept of the Internet is the dominant frame for policy and/or many other purposes. (Because there are

those who perceive themselves not to be on the Internet but on Facebook or some other platform, the extent to which this already affects perceptions of Internet governance matters among users. The ways in which they become involved in governance would be an interesting research question.) But I also agree with Hofmann, in chapter 12, and with Jessop (2016), in his work on the semantics of governance, that there are political power and policy efficacy in rhetorical frames and narratives. Thus I also take the position that thinking in terms of Internet governance will continue to have utility even as the actual network merges with material, biological, and social environments. That leaves us with two definitional problems—which legal history pertains, and how do we know when what is being regulated is communication and therefore fundamentally a matter of human rights and civil liberties?

The editors of this volume, like those of the journal *Internet Histories* (Brügger et al. 2017), are to be lauded for not only acknowledging but also actively encouraging appreciation of the multiplicities of the technological realities and experiences of the Internet. There are times, though, when which history is being privileged matters. It is this that is the foundational question in the network neutrality battle being played out in the United States. Ithiel de Sola Pool's seminal book *Technologies of Freedom* (1983)—which argues that, as different legal systems converge to cope with the convergence of computing and communication technologies, it is likely that the most repressive features of each would dominate in the new system that will emerge—explains how the trifold technological history (print, telecommunications, and broadcasting) yielded three different regulatory systems in the US by the time that government began to deal with digitization. Two of them, systems with very different regulatory approaches, have both been discussed as providing the history of the Internet for the purposes of network neutrality and other regulation. Additional legal histories are available when the Internet is approached from perspectives that are not oriented around communication. It would be the separate histories of currency, finance, and capital that apply to what has been described as "the internet of money" (Libra Association Members, n.d.), a suite of offerings that includes cryptocurrency and the associated financial services Facebook and a group of corporations that at launch included Mastercard, Visa, Spotify, Uber, and Lyft have been promoting. Starting from finance rather than communication frames Internet governance histories in ways

that preference values oriented around capital rather than human rights or citizenship. Similar stories can be told for every other government around the world.

As Abbate (2017) points out, how Internet governance is defined is itself a political question precisely because it determines which histories pertain, "ideology in practice" (Gurumurthy and Chami 2016, 1). This is not just inherent in the design process, but is also a matter of deliberate effort: "Internet governance technologies not only embed political values in their design and operations but are increasingly being co-opted for political purposes irrelevant to their primary Internet governance function" (DeNardis 2012, 721). Which histories should provide the frame for Internet governance? Should different histories serve as foundations for diverse dimensions of the problem? Is it useful to incorporate historical pluralism as well as theoretical pluralism in Internet governance research?

Policy analyses in any specific area can often be greatly enriched by looking across diverse regulatory systems for the various ways in which the same type of problem has been addressed. One example: the issue of who controls the interface between private and public environments has arisen for both material and electronic networks, but the policy discussions for each have taken place within different legal silos and have not cross-referenced each other despite the shared features of the problem. On the material side, in the United States, treatment of mailboxes was a matter of constitutional law; on the electronic side, attachments to customer premises equipment are matters of administrative law, regulated by the Federal Communications Commission (FCC). Debates over the latter, which launched the liberalization of telecommunications regulation in the United States in the 1970s, were intense but never referred to the constitutional issues, although arguments made and principles used in constitutional law would have been pertinent in ways that have become ever more obvious.

The Internet border gateway protocol (BGP), critical to relations within and between the autonomous systems of which the Internet is made and thus key to human rights issues such as efforts to censor or shut down national networks altogether (Vargas-Leon 2016), is different in many ways from either the physical or electronic predecessor issues, but the discussions on these matters went on for a long time, arguments were presented from a wide range of perspectives, and there is a great deal that could be learned for the toolbox of concepts and possibilities to consider for Internet

governance. Not every argument will transfer, but it is also likely that many will, as adapted or reoperationalized for the context. The point is not specific to the border gateway protocol.

Crawford (2007) prescriptively suggests that the Internet governance conversation should meld with the general domain of communication law and policy. If that is so, there is still the difficulty of deciding when Internet governance issues should be decided in light of fundamental constitutional principles and human rights law, justified when the network is understood to be about communication, arguably balanced differently against other needs when what is at stake is a transaction or a weapon. We are a couple of decades now into struggles over treating software as speech (see, e.g., Burk 1997; Coleman 2009) and are beginning to see the literature using speech-related arguments in analyses of autonomous entities such as robots (see, e.g., Bambauer 2017; Calo, Froomkin, and Kerr 2016). Quite aside from what speech rights would inhere to autonomous digital agents should they be granted any form of citizenship status, there is no obvious limit to the range of types of digital information collection, processing, and flow issues to which free speech analyses might be applied.

A look at the many and diverse ways in which US lawmakers and regulators have historically tried to bound the field of communication, published not long after the beginning of the 21st century, concluded that the most useful means of doing so for this technological era would be to treat media policy as those matters that mediate the nature of the public itself—who and what it is, the conditions under which members of the public can discuss together shared matters of public concern, and to which information members of the public have access upon which to base their discussions (Braman 2004c). That would not be a bad place to begin to think about how to draw boundaries regarding what should be considered to be communication for the purposes of Internet governance research, with the important caveat that it is now clear that several additional dimensions of analysis, discussed below, would need to be added to evaluate whether any given design decision, regulation, or content policy is now required.

Governance

A handbook by political scientists on governance opens by defining the concept in very general terms: "Theories and issues of social coordination and the nature of all patterns of rule" (Bevir 2011, 1). This is the broadest

of possible approaches, including theories and practices that increasingly involve governance as hybrid and multijurisdictional, populated by a plurality of stakeholders who engage with each other via networks. A synthesis of the governance literature as it has developed to include metagovernance refers to it as the coordination of structures and practices that themselves are involved in coordinating social relations marked by complex, reciprocal interdependence (Jessop 2011). Metagovernance can be unbundled into first-order efforts involving one form of metagovernance, and second-order activities that involve multiple forms of metagovernance.

Law (1992, 382) memorably describes governance as "an effect generated by heterogeneous means." The comment is not just accurate and witty but also has an implication that is profound: *Governance is always emergent*, in the specific sense in which that concept is understood within complex adaptive systems theory—an emergent system is one that cannot be explained at any other than the system level, rather than by the operations of any of its parts. Epstein, Katzenbach, and Musiani (2016) go further, arguing that by definition all the specifics of governance can *not* be identified; that is, *governance is fully recognizable only post hoc*—by the time you see it, it is in place. (Josephine Wolff [2018] titled her book on the cybersecurity dimensions of Internet governance *You'll See This Message When It Is Too Late*.) This post hoc feature of visibility makes preemption, as understood theoretically by Brian Massumi (2007), particularly important. From this perspective, the comment from Karl Rove, aide to President George W. Bush, regarding the "reality-based community" may be not a cynical throwaway but an empirical description of importance to researchers, courts, physicians, and others oriented around the facts. As it was first published in *The New Yorker* by the reporter to whom the statement was given:

> The aide [Rove] said that guys like me [the reporter] were "in what we call the reality-based community," which he defined as people who "believe that solutions emerge from your judicious study of discernible reality." … "That's not the way the world really works anymore," he continued. "We're an empire now, and when we act, we create our own reality. And while you're studying that reality—judiciously, as you will—we'll act again, creating other new realities, which you can study too, and that's how things will sort out. We're history's actors … [ellipsis in original] and you, all of you, will be left to just study what we do." (Suskind 2004)

Jessop (2011) argues that governance inevitably fails, appearing to be successful only when dilemmas are framed so that negative, sometimes

catastrophic, consequences are beyond the spatiotemporal horizons of visibility. Each of these categories of dilemma frames suggests a research program for those studying Internet governance. Corporation Schlumberger intentionally designed instruments and information collection practices for oil and gas exploration to be deceptive to governments, customers, and the public with respect to just which information was actually being collected, playing with such horizons of visibility for persuasive and operational purposes (Bowker 1994). What would such social technologies and practices look like in the domain of Internet governance? Over time, government structure and departmental or agency design can function as spandrels, analogous to architectural features that were once structurally necessary but that are now available for aesthetic, rhetorical, or other purposes (Braman 2006). Which features of Internet governance might be in use as spandrels, making it appear as if something presented is offered because it is considered desirable by users, the public, or policy makers when in reality it is something else, as well as or instead, that may for producers or others be the real point? In what ways can or does Internet governance make use of the spandrels of national, regional, and other governments? Are there equivalents to these questions regarding spandrels as they would apply to the corporate decision-making so important to Internet governance?

There has been so much scholarly discussion about changes in the nature of the state since the 1970s that it is actually identifiable as a distinct literature, on changing states. Three streams in this literature have arisen over time (Bevir and Rhodes 2011). The first engages the networked state as it has been practiced and understood by the late 1980s (see Antonelli 1988), a form in which the multiplicity of networked relations at every level of the governance structure creates an environment in which the state can no longer exercise power unilaterally. The second involves work on metagovernance, theories about ways in which the state continues to exert control in the networked environment by managing the multiple processes in play. The third loosened the sense of state control even further, focusing on "decentered governance," abandoning both governance and government in favor of attention to how individuals and elites exercise power in an environment framed more in terms of ethnically based nationalisms than the bureaucratic dimensions that typically characterize analyses of states. This sense of the decline in the effectiveness of governments has been expressed in various ways. Jessop (2004) discusses governance in the

shadow of government. For Bovaird (2005), it is governance without government. For Bevir and Rhodes (2011), the stateless state. Arguments can be made that there are areas of Internet-based activity that may be beyond our ability to govern at all (Braman 2015).

Under these conditions, it is reasonable to ask whether continuing to engage in policy making and analysis is meaningful. Jessop suggests the concept of "collibration" to refer to a variety of techniques that governments use in situations in which there would otherwise be regulatory failure. He likes that concept because it works across types of policy tools and processes, but this is an area in which there has been a lot of creativity. The Organization for Economic Cooperation and Development (OECD 2018) offers a variant in its report on science, technology, and innovation, another area of information policy that Antonelli (2017) argues falls within the domain of Internet governance because of the network's importance to knowledge production and knowledge production's importance to society, the economy, and governance writ large. The OECD report uses the term "concertation" to similarly refer to efforts to hold things together that are so various in kind, so multiple in number, and so distributed across levels of the social structure, levels of the governmental hierarchy, and geography that effective management would in reality, most experienced practitioners and observers believe, be a rank impossibility. The performative value of theoretical work is being emphasized throughout this essay, but it has its limits. Asserting new concepts in any area is no guarantee it will make things happen. It is this recognition of the limits of one's efficacy in the face of expected failure that leads Jessop (2011) to insist that one principle for successful metagovernance should be "requisite irony," to which this chapter returns in its conclusion.

There is a substantial literature further articulating governance conceptually and analyzing it in various contexts to which references here and in other chapters in this book will point the reader. One takeaway from this work for those doing Internet governance research would be to abandon the sense of exceptionalism that continues to hover, even if more faintly than before, over the research community. Continuing to learn about other domains in the manner modeled by Raymond and DeNardis (2015) is not only valuable for analysis of these matters as they pertain to the Internet, but is the only way to fully understand the role that Internet governance plays in larger governance and metagovernance processes.

A second takeaway is the importance of acknowledging developments in the systems with which those involved in Internet governance are engaging. Easy assumptions cannot necessarily be made about which countries fall into which category when it comes to characterizing their political nature, for example. Jessop's authoritative work on theories of the state published in 2016 still refers to the United States as a liberal democracy, even though earlier work of his describes exactly the steps through which the political affairs of 2020 are unfolding with prescient clarity. There are extreme developments in many other countries around the world. Longstanding assumptions underlying political, legal, and policy analyses need to be unearthed and questioned or the analyses of Internet governance researchers, too, will be limited to historical matters.

Internet Governance

Musiani (2015) provides a valuable review of the literature on conceptualizations of Internet governance. This chapter is placed within a simplified typology of types of definitions that has a core shared across all types of definitions, the most *narrow* approach, applying only to management of the network itself. From this perspective, exemplified by Mueller and Badiei in chapter 3, Internet governance is the responsibility of those global institutions explicitly created for that policy purpose and devoted to it—ICANN, the Internet Engineering Task Force, the Internet Architecture Board, and related entities. An *intermediate* definition of Internet governance would add "uses" to the subjects of governance and the national institutions responsible for the Internet in their countries, such as the Russian Runet as imagined in the "Internet isolation" (*Moscow Times* 2019)—or "reliable Internet" (Tass 2019)—bill of 2019. The approach offered by DeNardis in chapter 1, building on her earlier work with Musiani, in my view relies on an intermediate definition. I use a *broad* definition of Internet governance that includes 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).

There are two different ways of seeking the literature in a given policy area. One is to bound the domain through the lens of a specific term

or set of terms (focusing on words used). Mueller and Badiei in chapter 3 use this approach to analyze the history of the Internet governance literature. Browne's (1997) approach to defining "information policy" does the same with that related and pertinent concept. At the opposite end of the spectrum, the domain can be bounded conceptually and theoretically, irrespective of the terminology used by various authors to refer to elements of the domain. My approach to defining information policy represents this end of the spectrum for that concept (Braman 2006), and a similarly broad approach to bounding the domain of Internet governance is used here.

Searching on the phrase "Internet governance" to locate literature on the subject will be most successful with the narrowest definition, though that still will not yield a comprehensive view of the pertinent literature because other terms continue to be used to refer to the same sets of institutions, functions, and activities. It will have some but less utility with an intermediate definition. Searching on that phrase will be least successful with the broadest definitional approach, missing a great deal in the pertinent literatures. Use of the narrowest approach is most valuable within academia (where resource battles begin by bounding turf, with its genuine implications for things such as faculty positions and budgets) and, of course, operationally for those involved in Internet-specific decision-making processes. Intermediate approaches can have enormous utility for analytical purposes. General public discourse about Internet-policy-related matters and the experience of individuals, communities, and organizations typically use the broadest approach, so in my view that can be particularly valuable for outward-facing communications of academics in addition to its heuristic and analytical value.

Thus, here "Internet governance" includes uses (and users), decision-making by general-purpose policy-making entities (e.g., geopolitical governments) and by those specific to the Internet (e.g., ICANN), and decision-making and structurational actions by private and public sector entities, daemons and humans, through informal and formal, transient and fixed, means. This is the same approach taken in a mid-1990s bibliographic essay on the streams of literature in areas of the law that were coming together into an identifiable field of Internet policy (Braman 1995), much as happened with the microeconomics of information and the macroeconomics of the information economy (Braman 2005), with two differences: today Internet-specific entities loom much larger, both in the pertinent literatures and

in my thinking, and we are now using the frame of algorithms to address issues in this space as well.

What we think of as Internet governance issues will remain of central importance even when the term "Internet" itself has become a limited referent for the intelligent network environment within which we govern and are governed, and even when we are talking about metagovernance in all its versions rather than only governance. It has value because it keeps our attention on the range of existing decision-making venues from the global to the local, is a constant reminder to think about interactions among the effects of different decisions and policies, offers a singular lens onto complex interactions among many policy issues, and provides a valid umbrella for the range of types of decision-making venues, processes, stakeholders, and effects involved. Finally and importantly, thinking in terms of Internet governance justifies reliance on constitutional principles and international human rights law. It is not coincidental that David Kaye, the UN special rapporteur for freedom of expression, titled his 2019 book *Speech Police: The Global Struggle to Govern the Internet*. Rebecca MacKinnon used her 2012 book title to emphasize the importance of including Internet users in the network's governance if there is to be adequate concern for human rights and civil liberties: *Consent of the Networked: The Worldwide Struggle for Internet Freedom*.

Internet Governance and the State

Of the five trends in Internet governance Laura DeNardis discusses in chapter 1, two involve challenges to the state. The first, one of the most important arguments in that chapter, starts from the perspective of the state: Internet security and national security are diverging as well as converging. The second starts from the side of Internet governance: turning on their head usual analyses of legal globalization that start with the state, DeNardis describes laws and regulations of geopolitically recognized states as "bordered policy," with borders that are not always and in all ways contiguous with those of the networks being governed.

There are myriad types of states and theories about them (Held 1989), with social science interest in them rising and falling. As Jessop (2016, 1) notes, "here as in other fields, it seems that social scientists do not so much solve problems as get bored with them." The theories matter, though,

because they not only reflect but also effect transformations in the nature of the state—so much so that Jessop insists conceptualizations of the state are among the core elements of the modern state, along with territory, state bureaucracy and resources, and the population. The same can be said for the ideas of governance and metagovernance. Jessop explores what he calls the historical semantics of the modern state, including the vocabulary used by theorists to describe and discuss the state and the roles of those conceptual frames in shaping the nature of the state and its practices. Using different language, Hofmann's chapter 12, on rhetorical functions that are served by decision-making structures and organizational forms, makes related arguments, as do ten Oever (2019) and Milan and ten Oever (2017) in their analyses of what activists and advocates do on the ground.

This section looks at two among the ways in which Internet governance is inextricably implicated in challenges to the state—treatment of borders, and the development of alternative governance forms. There is insufficient room here to explore additional important dimensions of these relationships and tensions as they pertain to rule of law and citizenship. Conceptual and methodological limits raised by such issues are discussed in the next section.

Borders of the State

Social and technical discussions of Internet governance have long been absorbed in the particular issues raised by borders, often but not only as they present in the form of jurisdictional dilemmas. On the social side, there has been work by legal scholars (classics include Burk 1997; Froomkin 1997; Johnson and Post 1996; and Zittrain 2005), many of whom felt the importance of the topic could not be overestimated; in Reidenberg's (2005) view, it would be on such issues that rule of law in Internet governance would rise or fall. The border-defining Internet governance issues that are the most familiar involve the domain name system (DNS) (Bradshaw and DeNardis 2018).

On the technical side, the first reference in the technical document series that is both medium for and documentation of the design process, the Requests for Comments (RFCs), to jurisdictional issues was when those responsible for design of what we now call the Internet were making the first international connection, to Norway, in 1972 (NORSAR n.d.). A decade later, it was argued that no technical restrictions on transborder email should be allowed that are any different in kind from those used with physical mail

(the question involved encryption), and it was suggested that, when Internet design and architecture come into conflict with the law, governments should change their laws to solve the problem (RFC 828 [Owen 1982]). Other border issues that came up in the first decades, each launching ongoing design debates and efforts, included identity certification procedures (e.g., RFC 1114 [Kent and Linn 1989]), addressing (e.g., RFC 1218 [North American Directory Forum 1991]), and network security (e.g., RFC 1244 [Holbrook and Reynolds 1991]). By the close of the 1980s, discussion in RFCs included references to comparative legal scholarship (e.g., RFC 1135 [Reynolds 1989]).

The question of how to think about the boundaries of the geopolitical state in network terms has always been a challenge. Rutkowski (2011) provides an invaluable history of what we think of as cybersecurity principles, beginning with how they were first used in treaties dealing with postal systems and semaphore networks long before the digital era. Provisions included such things as exchanging network architecture and addressing information, data retention, authentication of messages of governments, and filtering of harmful messages. Among the principles to which almost every country in the world was a signatory at the time of his analysis are not only the proactive requirement to ensure communications security (a contemporary concern in the international legal community because of the question of how much a government needs to know regarding what flows through networks that cross its geographic territory), but also the rights to cut off all state connections with the international network and to cut off all private communications deemed dangerous "to the security of the state or contrary to its laws, to public order or to decency" (Rutkowski 2011, 15). Today we popularly refer to "rights to cut off" as the Internet kill switch (Vargas-Leon 2016).

Importantly, Rutkowski (2011) included a detailed description of what it took for him to collect all the pertinent documents from multiple institutional sources and to transfer the data from print and digital formats into a common digital format for analysis, processes that clearly took significant amounts of time and resources. By publicizing his data collection method and making the materials publicly available for use by others, Rutkowski urges us to do the same with other historical materials we need to study. In what other areas of Internet governance research would this kind of recuperation and sharing of primary research materials be of value? Should an institution take leadership in hosting such materials on behalf of the global community of Internet governance researchers?

International telecommunications network border issues have always been complex. Negotiations over international telecommunications networks in the late 19th and early 20th centuries revolved around such fundamental matters as the nature of corporations and what it means to be "foreign" (Zajácz 2019). For a long time, the US Federal Communications Commission operationally treated Canada and Mexico as domestic for regulatory purposes, and Alaska and Hawaii as foreign, because the agency found it more convenient to determine the boundaries by those of the specific network technology involved (land technologies to get to Canada and Mexico, underwater technologies to get to Alaska and Hawaii) than by geopolitics. Decisions about where to put the "border" between countries linked by a telecommunications circuit, necessary for the purposes of determining who paid whom for what when it comes to network flows in the world of telecommunications regulation as it had long been, were conceptual and negotiated (Frieden 1993), lending particular importance to national categorical decisions made regarding how to regulate the "converged" technological environment once digitization was at hand (Frieden 1984, 2004) from the international network perspective.

What is required to carry through on commitments made in the international treaties about electronic networks analyzed by Rutkowski (2011) is, of course, qualitatively and quantitatively more complex and thus difficult to understand and to successfully engage with in the contemporary environment. *Tallinn Manual 2.0* (Schmitt 2017) essentially suggests a new policy principle—the right of a state *not* to know what is going through networks that cross its territory or for which it has any other kind of responsibility, as a protection against needing to act on it in ways that could be self-destructive and/or politically unacceptable (Braman 2017). There are other areas in which developments provide limits to states, most notably with cybersecurity—something cannot be considered an action of national or homeland security concern unless it is an action against the state or the state, or an agent of the state, is involved. Ongoing questions for Internet governance researchers include asking how we can tell if something or someone is "of the state" in any given context or process or agent, and whether that is so by fiat, de jure or de facto. The problems are conceptual, empirical, and—perhaps, apparently, and/or potentially—contextual. How do ICANN processes affect perceptions of effective boundaries and expectations that governance must come from geopolitically recognized states in accord with rule of law? What

are the effects of the DNS structure on regional, national, and local identities and community functions? What are the effective borders in cyberspace that ordinary users experience when engaging in activities of particular types, when they exhibit certain characteristics and/or when there are tensions between activities as bounded by geopolitical, network, or institutional (third-party intermediary) "jurisdictions"? How do users know when they are crossing each of these types of borders, and what matters to them when they do? To what extent are users aware when they cross borders on the Internet, and when does that matter to them?

Another path of Internet governance research involving borders became visible when the US government began surveilling information held on travelers' electronic devices at border crossings (for a period, irrespective of citizenship status) and related developments. At the beginning of the 21st century, a draft "PATRIOT Act 2" named the Domestic Security Enhancement Act was proposed that included reducing or eliminating some US citizenship rights for those who publicly expressed concern about the civil liberties and human rights dimensions of post-9/11 security and surveillance practices. It seems possible that a continuation of the Trump administration in the United States could result in dilution of citizenship rights on the basis of relationships with foreign nationals conducted through or facilitated by the Internet, providing a model that might well then be followed by other countries. What kinds of political and legal proposals are being put forward regarding treatment of information and communication that crosses borders, the relationship networks of which they are a part, and the identities of those who engage in cross-border flows and relationships in countries around the world, whether those are directed at the border gateway protocol within the network, censorship of certain types of content, or other control points?

Alternative Governance Forms

It was during the second of the stages in the history of the literature on changing states that we saw the rise of governance forms that are alternative to the state and in competition with it (Bevir and Rhodes 2011). The Internet and its governance have provided the affordances through which to develop multinational and transnational organizational forms of even greater scale, scope, flexibility, and power relative to states. The network makes it possible for such organizations to engage in "regulatory arbitrage,"

maximizing organizational ability to take advantage of resources and opportunities offered by geopolitically recognized entities (Froomkin 1999). The work by Raymond and DeNardis (2015) on the varieties of multistakeholderism and Kulesza's (2018) analysis of its limits are foundational on this subject for those studying Internet governance. Musiani (2016) points out that the DNS itself can simultaneously be considered a technology and an alternative governance institution.

It should not be surprising that as geopolitical governments privatize formerly public functions and corporations simultaneously become increasingly governmental, the public and private sector entities as social technologies converge, yielding new organizational and decision-making forms. Two literatures studying these developments have been particularly influential. Scholars in the law and society tradition study the ways in which internal practices, programs, and rules serve governance functions (beyond the more traditionally acknowledged and publicly aggressive approaches of lobbying and revolving doors) (Mather 2013). In an example of such work relevant to Internet governance research as defined here, Bamberger and Mulligan (2015) studied corporate implementation of privacy law in several countries. The second literature of importance is that on governmentality as theorized by Michel Foucault (1980, 1982, 1984). Cerny (2008) provides one example of this type of analysis as applied to the looseness, ambiguities, flexibility, uncertainties, and multiplicities of the Internet governance environment, but Foucauldian ideas have influenced many, including thinkers in mainstream political science (e.g., Jessop 2011). The two approaches—law and society, and governmentality—are not in conflict with each other, but whichever is used, these trends can make it more difficult for those studying Internet governance to pursue many types of questions because access to information becomes more difficult when it can be claimed that data and its processing are proprietary, when the data are lost altogether because what had been considered a government function is abandoned, or when the data are unavailable for other reasons. Jørgensen in chapter 13 provides important experience-based advice in this regard, but here the most pressing challenges that Internet governance researchers face are conceptual and methodological.

There are recurring aspirations to use the Internet to operate completely outside the reach of national and international law, whether that is attempted physically, as in the Sealand experiment, or through some other

means. The current locus of such aspirations is the blockchain, though as Werbach (2018) informatively and persuasively argues, the blockchain will be most useful and is most likely to succeed if it is fully articulated within the law. That point is not limited to the blockchain, though how such efforts relate to the law will vary. In her analysis of internal attempts by Silk Road to prevent illegal online activity in pursuit of the anonymous networking entity's long-term success, Zajácz (2017) illustrates one reason this is so—the very protections for anonymity that allowed that network's illegal activities to continue as long as they did out of view of the state in turn undermined efforts by those who managed Silk Road to guarantee that participants in the marketplace would meet their obligations in the manner required for the trust needed to sustain the market. Across types of cybersecurity incidents, Wolff (2018) has found that it is much harder for those who engage in cyberattacks to use what they get once they bring it out of a database or network than it is for them to get in.

A seriously understudied type of Internet governance is that taking place within the autonomous systems the Internet, "a system of interconnected autonomous systems" (Tozal 2016), comprises. They are important control points (DeNardis 2012, 2014), can be categorized by the types of peering relationships they preferentially engage in (Tozal 2016), and can be mapped geographically as well as topologically, providing insight into additional ways in which such systems may be subject to political control (Yacobi-Keller et al. 2018). Some argue that the multiplicity of these systems justify describing the Internet as distributed rather than decentralized (Mathew 2016). When there are cyberattacks, they are leveled at autonomous systems, so Nur and Tozal (2018) suggest a method for measuring centrality that is based on how relatively critical a given autonomous system is to the network, or to society, as a whole. And that is about as far as the literature goes. Will we start thinking in terms of citizenship in autonomous systems, as the network unit of particular importance to user operations? Would going this route make it easier to think about governance tools that can be used in common irrespective of whether the autonomous system involved is public or private, or are different sets of governance tools still needed for the two types of subjects? With whom does thinking about autonomous systems from a governance perspective put ICANN in relation?

These trends come together with the increasing governmentalization of social media. Reversing the trend of what has been happening with

citizenship, which has been becoming thinner and thinner, platforms are building from thin to thick: first currency is offered, then a means of engaging in transactions, then dispute resolution, and on. The announcement of Libra and its associated app that provides infrastructure for transactions and other financial matters from Facebook and collaborator corporations has gone the furthest in this regard by the time of writing. Geopolitical governance entities are insisting that the offerings undergo government review and approval before proceeding. What are the further concerns, if any, from the Internet governance perspective? To what extent, and how, are Internet governance decisions responsible should such offerings draw significant resources away from the state and toward the corporation that hosts the social media platform that will serve as the governance infrastructure, in turn contributing to the weakening of rule of law from the perspective of geopolitically recognized states?

Conceptual and Methodological Limits

Although, as discussed above, the general socio-technical point has by now been beautifully made, illustrated, and practiced, today's Internet governance research questions require attention to analytical dimensions not historically addressed. This in turn requires us to go further theoretically, conceptually, and methodologically in many areas for which this this chapter does not have space, such as level and type of complexity and liability issues. Following, though, are some of the conceptual, theoretical, and methodological challenges.

Stages of Information Processing

We are most accustomed to thinking about speech issues in terms of single speech acts that involve identifiable and quantifiable (unitizable) expressions, flows of information, or sets of interactions. The sensemaking literature, and that which focuses on meaning making by an active audience, looks at how multiple flows come together at specific human conjunctures but still typically involve single steps. The problem of what it would take to effectively and meaningfully evaluate algorithmic decision-making, however, reminds us that in most, if not almost all, cases, it will actually be a stream of steps of information processing that yields the effect of any given one. How many steps back need to be known to be confident of the

provenance of informational or communicative content or of an action, whether by a human or daemon agent? Each information processing step can involve interactions with others that may themselves be complex systems involving diverse types of liability and levels of responsibility. Under what conditions is a specific agent to be held accountable for an act or communication resulting from interactions among many agents? We are beginning to hear calls for provenance of data regarding its information processing history from those seeking accountability and transparency of algorithms. How is such provenance most accurately and usefully determined? Who is to hold the records?

Conceptual and historical kernels of what it would take to achieve operationalizable answers to these questions for the purposes of current use within geopolitical legal systems and within the network exist. Treatment of the right to receive information as a necessary element of the right to communicate in the United States (and thus something that is also protected by the First Amendment) is one important example of an inherently multistep approach to thinking about the stages of information processing that need protection in order to achieve the constitutional goal. What new rights might be recognized as a result of further developing our ability to analyze algorithms for governance purposes? How might we come to articulate existing rights in new ways in order to map validly onto the digital environment in comprehensible ways? In what forms might such developments appear across the diverse institutions involved in Internet governance? What methods might be developed to identify when rights are being supported or being curtailed?

Analysis of information policy in US Supreme Court decisions of the 1980s (Braman 1988) found that essentially all involved some sort of reference to a model of an information production chain on which distinctions deemed to be of constitutional importance relied, whether implicitly or explicitly. A highly systematic effort to conceptualize information policy provisions across stages of the information production chain is underway by Rebecca MacKinnon's Ranking Digital Rights nonprofit organization (https://rankingdigitalrights.org). How can these and other extant models available for distinguishing among stages of information production chains be used in Internet governance research? Do we need to conceptualize additional stages of such chains, or conceptualize known stages differently, in order to adequately understand what is happening online for Internet

governance purposes? What methodological tools can we develop to distinguish among stages?

Types of Information Processing

Reliance on information production chain models in the course of legal analysis means that distinctions among types of information processing are being made for governance purposes. When struggles over specific types of information processing ensue, often what is at stake is whether the kind of processing involved is speech or not, with the answer determining whether fundamental protections for human rights and civil liberties, such as those protecting free speech, apply. Legal debates over this as they specifically arise in the digital environment go back at least to the 1990s (Burk 2000). Battles over treating code as speech should be expected to continue (Coleman 2009; Petersen 2015). In the world of what is now called cyber operations, the question of how to distinguish cybercrime (matters of national law) from cyberwar (matters of international law) has proven so difficult that this new terminology was developed to refer to the two jointly for analytical purposes (Schmitt 2017).

Just how to draw distinctions among types of information processing in the online environment is at the heart of debates over governance of and by algorithms. Most of the literature in this terrain to date has started by identifying undesirable effects of the use of particular algorithms, such as bias or incitement. The work on information policy in constitutional law mentioned above distinguished between only two types of information processing—human and machinic, what we now refer to as algorithmic. Already in the 1980s it was clear both that that was far from adequate, and that going further would require significant intellectual effort. Now that the algorithmic moment is before us, it is time to invest in that effort. For each issue examined by an Internet governance researcher, what are the types of information processing involved, and what are the distinct governance problems attached to each? Is there a distinction between general-purpose and single-purpose information production chains that is useful for governance purposes? How do the policy tools used to address the same issue as it may arise across different stages of the information production chain vary? Under conditions in which it can be assumed that technological innovation will continue at a significant pace and highly competitively, is it possible to group types of processes together for evaluative and

governance purposes with confidence that the range of types of information processing of concern, and their uses, are actually being taken into account? What methods can be developed to evaluate the efficacy of such policy tools?

Types of Speakers and Information Processors

Legal systems typically distinguish among types of communication speakers and receivers; examples include children versus adults, willing versus unwilling receiver, employee versus nonemployee, and spouse versus nonspouse. Analytical dimensions of long-standing interest include whether, and, if so, how, a speaker is anonymous; independent or autonomous (two related but distinct features); intelligent; and someone with whom there is a confidential relationship. In the digital environment, we have come additionally to think about whether the speaker is human or machinic, and we have come to think of speech as a distinct set of types of information processing. For those studying Internet governance in light of its importance vis-à-vis governance in general, it is particularly useful to approach the human versus machinic aspect through the lens of the question of who or what qualifies as a legal subject, and as a citizen.

Recognition of the distinction between human and machinic users—the latter referred to as daemons—was evident very early on in the history of Internet design (Braman 2011; McKelvey 2018). Each type of user required different things from the designers, some of whom communicated that they found the needs of daemons easier to understand than those of humans. It was acknowledged, however, that serving the needs of humans, odd as they might seem, led to solutions that were in many cases also significant improvements for the network. Artificial intelligence research focuses on how technologies can do things that humans do better than humans can do them. We are just beginning to see research on the separate question of how humans and daemons may differ when they engage in the same types of information processing. The story that deterrence games about nuclear war used computers rather than humans because it was found that humans would never launch nuclear warheads but computers would may be apocryphal, but it is telling even so. Vempaty et al. (2018) have found that humans and computers *do* differ when they engage in decision-making on at least some kinds of problems. This line of research is extremely important for those analyzing Internet governance processes. What kinds of differences

in how the two types of information processors work need to be taken into account? How do these differences affect the values that are embedded in technology design or network architecture? How could such differences be presented in public and policy-making conversations in such a manner that they would make sense and could reasonably be the subject of decision-making?

The question of whether or not an entity is a legal subject arises both for individuals and for groups of people. Regarding the former, there is now a field of "robot law" (see, e.g., Calo, Froomkin, and Kerr 2016) that begins with the issue of personhood. When it comes to the latter, autonomous networks like WikiLeaks—not to be mistaken with the autonomous systems discussed above—are already proving problematic, as the US government found when it attempted to pursue that entity in the course of the Bradley (now Chelsea) Manning trial (Braman 2014). As social technologies continue to converge, producing new social forms, this problem is likely to arise repeatedly. The question of whether nonhumans can become legal subjects first came to the fore in the 1970s in the United States, when the issue was the environment. The history begins with a student, an origin story of a type familiar to Internet governance researchers: a law school student, Christopher Stone—son of the highly independent and influential investigative journalist I. F. Stone—sent his argument, since published as the book *Should Trees Have Standing?* (Stone 1974), to US Supreme Court Justice William O. Douglas, who in turn convinced the court to recognize that forests have standing before the law and thus have rights that could be legally protected. The suggestion that entities with artificial intelligence should be granted personhood was put forward before the Internet was commercialized and made available for general use (Solum 1991). Resonances between discussions of legal personhood for biological and machinic nonhuman entities continue (see, e.g., Solaiman 2017; Teubner 2006). What would change in Internet governance should daemons (which can include things like operating systems and network layers) and algorithms be granted legal personhood? How should the governance implications of such a fundamentally important development be taken into account when considering the question? Should all daemons and algorithms be treated alike from this perspective and, if not, what methods can be developed for drawing lines?

The literatures on citizenship dimensions of the Internet are large and diverse, as most broadly conceptualized beginning with political

communication research on the impact of the Internet on political behaviors. John Perry Barlow (1996) famously issued a "Declaration of Independence" for those who see themselves first and foremost as citizens of cyberspace, and shortly afterward it became popular to think in terms of the network citizen (Hauben and Hauben 1997). A reading of the Internet RFCs from the perspective of what they say about legal, policy, and political matters over time shows the development of a sense of network citizenship that can conflict with geopolitical citizenship, creating problems for Internet governance (Braman 2013). This author's first exposure to the concept in the mass media was in a Singaporean newspaper in 2000, which used "network citizenship" as a term the readers were assumed to understand to refer to individuals who engaged in political activity online. Indeed, a quick search in summer of 2019 of the literature for "network citizenship" finds most of it is research on Asian countries. The development of China's social credit system (Liang et al. 2018) provides evidence of one direction in which network citizenship can evolve. MacKinnon (2012) argues for another, reviving the use of the concept in her call for development of a sense of global participation in decision-making for the Internet, done in a manner that effectively—not just rhetorically—protects human rights and civil liberties. How can tensions between geopolitical and network political citizenship be resolved? The history of the concept of citizenship is marked by the addition of dimensions considered to be inherent to the notion; do we need additional conceptual work to take into account the nature and implications of network citizenship? How does approaching Internet governance research through the lens of network citizenship affect the questions we ask and how we ask them? What does inclusion of both machinic and network citizenship require of the indicators we use to evaluate the nature and strength of democratic practices?

Governability and Irony

No one disputes that such matters as equity and fairness should be taken into account in technology design and network architecture. The challenge is that doing so may require more than we are now actually capable of in terms of fully understanding what is happening when highly complex systems multiply interact with each other across scales, geographies, uses, scopes, and contextual conditions. This is no apologia, nor a suggestion

that demands for incorporating attention to such matters within design processes in as accountable a manner as possible shouldn't continue to be fought for—but it *is* an expression of humility in the face of what might actually be humanly possible when it comes to the governability of this environment, irrespective of by whom or for what purposes.

In the face of what so many political scientists now acknowledge to be the inevitability of governance failures, Jessop (2011) identifies three ways in which governance entities manage to not fail, to appear not to fail, or to, in essence, redefine what is meant by failure. An entity can achieve the appearance of successful governance by making sure that any problems appear beyond the spatiotemporal horizons (or perceptions of horizons) of a given set of players or forces. It can survive through a continual *fuite en avant*, continually escaping from one crisis by turning to another mode of policy making that will also fail. Or policy makers could engage in self-reflexive irony, even when they know they are likely to fail.

For Internet governance researchers, the first two of these are not within reach, but the third is. There are many ways of thinking about the job of an intellectual, but Clifford Geertz reminds us that, among other things, it is a way of life, and so are the methods we use:

> The various disciplines…are more than just intellectual coigns of vantage but are ways of being in the world, to invoke a Heideggerian formula, forms of life, to use a Wittgensteinian, or varieties of noetic experience, to adapt a Jamesian. In the same way that Papuans or Amazonians inhabit the world they imagine, so do high energy physicists or historians of the Mediterranean in the age of Phillip II.… To set out to deconstruct Yeats's imagery, absorb oneself in black holes, or measure the effect of schooling on economic achievement is not just to take up a technical task but to take on a cultural frame that defines a great part of one's life. (Geertz 1982, 24)

The researcher *is* the methodological instrument irrespective of any other tools used (Lindlof and Taylor 2018). When we are talking about method, we are talking about who we are.

The irony of Internet governance research is that, as most broadly defined, Internet governance itself may not exist in any of a number of senses. Policies we do put in place may not be effective. What makes sense technically may not work politically, socially, or legally, and vice versa. It is becoming difficult to separate the Internet as the subject of governance of human communications from a wide variety of other types of processes and from the material environment itself. The subject (and subjects) may be too complex to be governable at all, or it may not even exist as a legal

subject. Political processes we thought were stable enough to support continued incremental social, economic, political, and cultural change are turning out not to be. Put together, all of these make Internet governance research a problem in metagovernance.

Whether or not Internet governance exists, we have a right to it—or may choose to go on as if we believe we do. Researchers are involved with lots of "ologies," from epistemology and methodology on. Deontology is among them.

Note

1. Sandra Braman, from *The One Verse City* (Eugene, OR: Wolf Run Books, 1974).

References

Abbate, J. (2017). What and where is the Internet? (Re)defining Internet histories. *Internet Histories, 1*(1–2), 8–14.

Antonelli, C. (1988). The emergence of the networked firm. In Cristiano Antonelli (Ed.), *New information technology and industrial change: The Italian case* (pp. 13–32). Dordrecht, Netherlands: Springer.

Antonelli, C. (2017). Digital knowledge generation and the appropriability trade-off. *Telecommunications Policy, 41*, 991–1002.

Archer, M. S. (1982). Morphogenesis versus structuration: On combining structure and action. *The British Journal of Sociology, 33*(4), 455–483.

Archer, M. S. (1988). Towards theoretical unification: Structure, culture and morphogenesis. *Culture and agency: The place of culture in social theory* (pp. 247–307). Cambridge, UK: Cambridge University Press.

Bache, I., Bartle, I., Flinders, M., & Marsden, G. (2015). *Multilevel governance and climate change: Insights from transport policy*. Pickering & Chatto.

Bambauer, J. R. (2017). Dr. Robot. *UC Davis Law Review, 51*, 383–398.

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: Driving corporate behavior in the United States and Europe*. Cambridge, MA: MIT Press.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Duke Law & Technology Review, 18*(1), 5–7.

Beckett, S. (1953/2012). *The unnameable*. New York, NY: Grove Press.

Bevir, M. (2011). Governance as theory, practice, and dilemma. In M. Bevir (Ed.), *The Sage handbook of governance* (pp. 1–16). Thousand Oaks, CA: Sage.

Bevir, M., & Rhodes, R. A. W. (2011). The stateless state. In M. Bevir (Ed.), *The Sage handbook of governance* (pp. 203–217). London, UK: Sage Publications.

Bevir, M., & Rhodes, R. A. W. (2016). The "3Rs" in rethinking governance: Ruling, rationalities, and resistance. In M. Bevir & R. A. W Rhodes (Eds.), *Rethinking governance: Ruling, rationalities and resistance* (pp. 1–21). New York, NY: Routledge.

Bovaird, T. (2005). Public governance: Balancing stakeholder power in a network society. *International Review of Administrative Sciences, 71*(2), 217–228.

Bowker, G. (1994). *Science on the run: Information management and industrial geophysics at Schlumberger, 1920–1940*. Cambridge, MA: MIT Press.

Bradshaw, S., & DeNardis, L. (2018). 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. (1974). *The one verse city*. Eugene, OR: Wolf Run Books.

Braman, S. (1988). *Information policy and the United States Supreme Court* (Unpublished dissertation). University of Minnesota. Dissertation #8823521; Proquest document ID 303670545.

Braman, S. (1995). Policy for the net and the Internet. *Annual Review of Information Science and Technology (ARIST), 30*, 5–75.

Braman, S. (2002). Informational meta-technologies and international relations: The case of biotechnologies. In J. Rosenau & J. P. Singh (Eds.), *Information technologies and global politics: The changing scope of power and governance* (pp. 91–112). Albany: State University of New York Press.

Braman, S. (2004a). The processes of emergence. In *The emergent global information policy regime* (pp. 1–11). Houndsmills, UK: Palgrave Macmillan.

Braman, S. (2004b). The emergent global information policy regime. In *The emergent global information policy regime* (pp. 12–37). Houndsmills, UK: Palgrave Macmillan.

Braman, S. (2004c). Where has media policy gone? Defining the field in the twenty-first century. *Communication Law and Policy, 9*(2), 153–158.

Braman, S. (2005). The micro- and macroeconomics of information. *Annual Review of Information Science and Technology (ARIST), 40*, 3–52.

Braman, S. (2006). *Change of state: Information, policy, and power*. Cambridge, MA: MIT Press.

Braman, S. (2011). The framing years: Policy fundamentals in the Internet design process, 1969–1979. *The Information Society, 27*(5), 295–310.

Braman, S. (2013). The geopolitical vs. the network political: Internet designers and governance. *International Journal of Media & Cultural Politics, 9*(3), 277–296.

Braman, S. (2014). "We are Bradley Manning": Information policy, the legal subject, and the WikiLeaks complex. *International Journal of Communication, 8*, 2603–2618.

Braman, S. (2015). The state of cloud computing policy. In C. Yoo & J.-F. Blanchette (Eds.), *Regulating the cloud: Policy for computing infrastructure* (pp. 279–288). Cambridge, MA: MIT Press.

Braman, S. (2017). The medium as power: Information and its flows as acts of war. In C. George (Ed.), *Communicating with power* (pp. 3–22). Bern, Switzerland: Peter Lang, International Communication Association Theme Book Series.

Browne, M. (1997). The field of information policy, I: Fundamental concepts. *Journal of Information Science, 23*(4), 261–275.

Bruce, R. R., Cunard, J. P., & Director, M. D. (1986). *From telecommunications to electronic services: A global spectrum of definitions, boundary lines, and structures*. Boston, MA: Butterworth.

Brügger, N., Goggin, G., Milligan, I., & Schafer, V. (2017). Introduction: Internet histories. *Internet Histories, 11*(1–2), 1–7.

Burk, D. (1997). Jurisdiction in a world without borders. *Virginia Journal of Law and Technology, 1*(3), 1522–1687.

Burk, D. (2000). Patenting speech. *Texas Law Review, 79*, 99–162.

Calo, R., Froomkin, A. M., & Kerr, I. (Eds.). (2016). *Robot law*. Edward Elgar.

Cerny, P. G. (2008). The governmentalization of world politics. In E. Kofman & G. Youngs (Eds.), *Globalization: Theory and practice* (3rd ed., pp. 221–237). London, UK: Continuum.

Clark, D. D. (2018). *Designing an Internet*. Cambridge, MA: MIT Press.

Cohen, J. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven, CT: Yale University Press.

Coleman, G. (2009). Code is speech: Legal tinkering, expertise, and protest among free and open source software developers. *Cultural Anthropology, 24*(3), 420–454.

Coletta, C., & Kitchin, R. (2017, July–December). Algorhythmic governance: Regulating the "heartbeat" of a city using the Internet of Things. *Big Data & Society,* 1–17.

Cowhey, P. F. (1990). The international telecommunications regime: The political roots of regimes for high technology. *International Organization, 44*(2), 169–199.

Crawford, S. P. (2007). The Internet and the project of communication law. *UCLA Law Review, 55*, 359–407.

DeLanda, M. (1991). *War in the age of intelligent machines*. New York, NY: Zone Books.

DeNardis, L. (2012). Hidden levers of Internet control. *Information, Communication & Society, 15*(5), 720–738.

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

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 1–23). Houndsmills, UK: Palgrave Macmillan.

Dezalay, Y., & Garth, B. G. (1996). *Dealing in virtue: International commercial arbitration and the construction of a transnational legal order*. Chicago, IL: University of Chicago Press.

Drezner, D. W. (2009). The power and peril of international regime complexity. *Perspectives on Politics, 7*(1), 65–70.

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for. *Duke Law & Technology Review, 16*(1), 18–84.

Epstein, D., Katzenbach, C., & Musiani, F. (2016). Doing Internet governance: Practices, controversies, infrastructures, and institutions. *Internet Policy Review, 5*(3). doi:10.14763/2016.3.435

Foucault, M. (1980). *Power/knowledge* (C. Gordon, Ed.). New York: Pantheon Books.

Foucault, M. (1982). The subject and power. *Critical Inquiry, 8*(4), 777–795.

Foucault, M. (1984). Space, knowledge and power. In P. Rabinow (Ed.), *The Foucault reader* (pp. 239–256). New York, NY: Pantheon Books.

Frieden, R. M. (1984). The international application of the Second Computer Inquiry. *Michigan Yearbook of International Legal Studies, 5*, 189–218.

Frieden, R. (1993). International toll revenue division: Tackling the inequalities and inefficiencies. *Telecommunications Policy, 17*(3), 221–233.

Frieden, R. M. (2004). The FCC's name game: How shifting regulatory classifications affect competition. *Berkeley Technology Law Journal, 19*(4), 1275–1314.

Froomkin, M. A. (1997). The Internet as a source of regulatory arbitrage. In B. Kahin & C. Nesson (Eds.), *Borders in cyberspace* (pp. 129–163). Cambridge, MA: MIT Press.

Froomkin, M. A. (1999). Of governments and governance. *Berkeley Technology Law Journal, 14*, 617–633.

Geertz, C. (1982). The way we think now: Toward an ethnography of modern thought. *Bulletin of the American Academy of Arts and Sciences, 35*(5), 24.

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. Berkeley: University of California Press.

Gurumurthy, A., & Chami, N. (2016). Internet governance as "ideology in practice"—India's "Free Basics" controversy. *Internet Policy Review, 5*(3). doi:10.14763.2016.3.431

Hauben, M., & Hauben, R. (1997). *Netizens: On the history and impact of Usenet and the Internet*. Los Alamitos, CA: IEEE Computer Society Press.

Held, D. (1989). *Political theory and the modern state*. Cambridge, UK: Polity Press.

Holbrook, J., & Reynolds, J. (Eds.). (1991). *Site security handbook*. RFC 1244. Retrieved from the Internet Engineering Task Force website: https://tools.ietf.org/html/rfc1244

Horwitz, R. B. (1989). *The irony of regulatory reform: The deregulation of American telecommunications*. Oxford, UK: Oxford University Press.

Jessop, B. (2004). Multi-level governance and multi-level metagovernance. In I. Bache & M. Finders (Eds.), *Multi-level governance* (pp. 49–74). Oxford, UK: Oxford University Press.

Jessop, B. (2011). Metagovernance. In M. Bevir (Ed.), *The Sage handbook of governance* (pp. 106–123). Thousand Oaks, CA: Sage.

Jessop, B. (2016). *The state: Past, present, and future*. Cambridge, MA: Polity Press.

Johnson, D., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review, 48*(5), 1367–1402.

Kaye, D. (2019). *Speech police: The global struggle to govern the Internet*. New York, NY: Columbia Global Reports.

Kent, S., & Linn, J. (1989). *Privacy enhancement for Internet electronic mail: Part II—Certificate-based key management*. RFC 1114. Retrieved from the Internet Engineering Task Force website: https://tools.ietf.org/html/rfc1114

Krasner, S. D. (Ed.). (1983). *International regimes*. Ithaca, NY: Cornell University Press.

Kulesza, J. (2018). Balancing privacy and security in a multistakeholder environment: ICANN, WHOIS, and GDPR. *The Visio Journal, 3*, 48–58.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice, 5*(4), 379–393.

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet, 10*(4), 415–453.

Libra Association Members. (n.d.). *An introduction to Libra*. Libra White Paper. Retrieved from https://libra.org/en-US/white-paper/

Lindlof, T. R., & Taylor, B. (2018). *Qualitative communication research methods* (4th ed.). Thousand Oaks, CA: Sage Publications.

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books.

Martine, B. J. (1992). *Indeterminacy and intelligibility*. Albany: State University of New York Press.

Massumi, B. (2007). Potential politics and the primacy of preemption. *Theory & Event, 10*(2). doi:10.1353/tae.2007.0066

Mather, L. (2013). Law and society. In R. E. Goodin (Ed.), *The Oxford handbook of political science*. Oxford, UK: Oxford University Press. doi:10.1093/oxfordhb/9780199604456.013.0015

Mathew, A. J. (2016). The myth of the decentralised Internet. *Internet Policy Review, 5*(3). doi:10.14763/2016.3.425

McKelvey, F. (2018). *Internet daemons: Digital communications possessed*. Minneapolis: University of Minnesota Press.

McLuhan, E., & McLuhan, M. (1992). *Laws of media: The new science*. Toronto, Canada: University of Toronto Press.

Merrill, K. (2016). Domains of control: Governance of and by the domain name system. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 89–106). New York, NY: Palgrave Macmillan.

Meuleman, L. (2008). *Public management and the metagovernance of hierarchies, networks, and markets: The feasibility of designing and managing governance style combinations*. The Hague, Netherlands: Physica-Verlag.

Milan, S., & ten Oever, N. (2017). Coding and encoding rights in Internet infrastructure. *Internet Policy Review, 6*(1). doi:1.14763/2017.1442

The Moscow Times. (2019, February 12). Russia moves to grant government the power to shut down the Internet, explained. *The Moscow Times*. Retrieved from https://www.themoscowtimes.com/2019/02/12/russia-moves-grant-government-power-shut-down-internet-explained-a64470

Mueller, M. (2004). ICANN and INTELSAT: Global communication technologies and their incorporation into international regimes. In Sandra Braman (Ed.), *The emergent global information policy regime* (pp. 62–85). Houndsmills, UK: Palgrave Macmillan.

Musiani, F. (2015). Practice, plurality, performativity, and plumbing: Internet governance research meets science and technology studies. *Science, Technology, & Human Values, 40*(2), 272–286.

Musiani, F. (2016). Alternative technologies as alternative institutions: The case of the domain name system. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 73–87). New York, NY: Palgrave Macmillan.

NORSAR. (n.d.). NORSAR and the Internet. Retrieved May 22, 2010, from http://www.norsar.no/pc-5-30-NORSAR-and-the-Internet.aspx

North American Directory Forum, The. (1991). *A naming scheme for c=US*. RFC 1218. Retrieved from the Internet Engineering Task Force website: https://tools.ietf.org/html/rfc1218

Nur, A. Y., & Tozal, M. E. (2018). Identifying critical autonomous systems in the Internet. *The Journal of Supercomputing, 74*(10), 4965–4985.

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. Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

OECD. (2018). *OECD science, technology and innovation outlook 2018: Adapting to technological and societal disruption*. Paris, France: Author.

Owen, K. (1982). *Data communications: IFIP's international "network" of experts*. RFC 828. Retrieved from the Internet Engineering Task Force website: https://tools.ietf.org/html/rfc828

Petersen, J. (2015). Is code speech? Law and the expressivity of machinic language. *New Media & Society, 17*(3), 415–431.

Pool, I. de Sola. (1983). *Technologies of freedom*. Cambridge, MA: Belknap Press.

Rajnish, P., Ranjan, B. S., Mridula, P., Shrutilka, B., Neha, A., & Divya, S. (2017). Role of Internet governance in achievement of Sustainable Development Goals. *International Journal of Research in Social Sciences, 7*(9), 574–577.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory, 7*(3), 571–616.

Reidenberg, J. (2005). Technology and Internet jurisdiction. *University of Pennsylvania Law Review, 153*, 1951–1974.

Reynolds, J. (1989). *The helminthiasis of the Internet*. RFC 1135. Retrieved from the Internet Engineering Task Force website: https://tools.ietf.org/html/rfc1135

Russell, A. L. (2017). Hagiography, revisionism & blasphemy in Internet histories. *Internet Histories, 1*(1–2), 15–25.

Rutkowski, A. (2011). Public international law of the international telecommunication instruments: Cyber security treaty provisions since 1850. *Info, 13*(1), 13–31.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual*. Cambridge, UK: Cambridge University Press.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0*. Cambridge, UK: Cambridge University Press.

Solaiman, S. M. (2017). Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law, 25*(2), 155–179.

Solum, L. B. (1991). Legal personhood for artificial intelligences. *North Carolina Law Review, 70*, 1231.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111–134.

Stone, C. D. (1974). *Should trees have standing?* Palo Alto, CA: William Kaufmann.

Suskind, R. (2004, October 17). Faith, certainty and the presidency of George W. Bush. *The New York Times Magazine*. Retrieved from www.nytimes.com/2004/10/17/magazine/17BUSH.html

Tass. (2019, May 1). Putin signs law on reliable Russian Internet. *Tass*. Retrieved from http://tass.com/politics/1056750

ten Oever, N. (2019). Productive contestation, civil society, and global governance: Human rights as a boundary object in ICANN. *Policy & Internet, 11*(1), 37–60.

Teubner, G. (2006). Rights of non-humans? Electronic agents and animals as new actors in politics and law. *Journal of Law and Society, 33*(4), 497–521.

Theall, D. F. (1999). *James Joyce's techno-poetics*. Toronto, Ontario: University of Toronto Press.

Tozal, M. E. (2016). The Internet: A system of interconnected autonomous systems. In *2016 Annual IEEE Systems Conference (SysCon)* (pp. 1–8). IEEE.

Tribe, L. H. (1985). Constitutional calculus: Equal justice or economic efficiency? *Harvard Law Review, 98*(3), 592–621.

Vargas-Leon, P. (2016). Tracking Internet shutdown practices: Democracies and hybrid regimes. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance* (pp. 167–188). Houndsmills, UK: Palgrave Macmillan.

Vempaty, A., Varshney, L. R., Koop, G. J., Criss, A. H., & Varshney, P. K. (2018). Experiments and models for decision fusion by humans in inference networks. *IEEE Transactions on Signal Processing, 66*(11), 2960–2971.

Werbach, K. (2018). *The blockchain and the new architecture of trust*. Cambridge, MA: MIT Press.

Wolff, J. (2018). *You'll see this message when it is too late: The legal and economic aftermath of cybersecurity breaches*. Cambridge, MA: MIT Press.

Yacobi-Keller, U., Savin, E., Fabian, B., & Ermakova, T. (2018). Towards geographical analysis of the autonomous system network. *International Journal of Networking and Virtual Organizations, 21*(3), 379–397.

Zajácz, R. (2017). Silk Road: The market beyond the reach of the state, *The Information Society, 33*(1), 1–12.

Zajácz, R. (2019). *Reluctant power: Networks, corporations, and the struggle for global governance in the early 20th century*. Cambridge, MA: MIT Press.

Zittrain, J. L. (2005). *Jurisdiction*. St. Paul, MN: Foundation Press.