# Laying the path: governance in early internet design

Sandra Braman

Sandra Braman is a Professor in the Department of Communication, University of Wisconsin-Milwaukee, Milwaukee, Wisconsin, USA.

**Abstract**

**Purpose** – *This article aims to present an analysis of ideas and practices regarding governance of and by the network design process by participants in the technical design process during the first decade (1969-1979) as recorded in the technical document series that provides both the medium for and the history of that design process, the Internet RFCs.*

**Design/methodology/approach** – *The research was conducted via a comprehensive inductive and adductive reading of all of the publicly available documents in the series from its launch in October of 1969 through the close of 1979.*

**Findings** – *The findings show that internet designers were well aware that the infrastructure they were building was social as well as technical in nature. They were concerned about both governmental constraints on the design process (governance of) and about how protocol compliance could be achieved (governance by the network design process). As do informational states, network designers developed governance tools that affected the identity, structure, borders, and change in social, informational, and technological systems. The dual faces of network governance reveal tensions between the network political and the geopolitical.*

**Originality/value** – *This work contributes to our understanding of the interactions between the social and the technical in the course of the internet design process as it was expressed in concerns about governance by others and of others brought up in the course of resolving technical design problems. Methodologically, the research provides a model of one approach to analyzing the development of governance mechanisms and specific policies along sociotechnical boundaries.*

**Keywords** *Internet, Design, Contracts, Digital communication systems, Legal systems, Protocols*

**Paper type** *Research paper*

Vint Cerf, writing in ''The current flow-control scheme for IMPSYS'' in 1973, claimed his ideas would ''secure the rights of life, liberty, and the pursuit of happiness for ourselves and our posterity . . .'' (RFC 442, p. 1)[1]. Though what came after the ellipsis, and concluded a paragraph otherwise concerned with retransmissions, was ''oops'' (RFC 442, p. 1), what Cerf presented as a joke did become the subject of ongoing discussion about legal and policy matters as goals of and constraints upon the process of designing what we now refer to as the internet. Particularly during the early years, before the discursive and decision-making processes conducted through the Internet Requests for Comments (RFCs) technical document series became formalized[2], such issues appeared regularly during debate over how to build a new type of telecommunications network. The technical matters that so concerned Cerf in the document above – retransmission time and congestion caused by unnecessary retransmissions – do affect free speech.

Cerf and his colleagues were among those who had come to realize that the problem of building the network would not stop with reaching agreement on technical standards (protocols). They had learned, by the early 1970s, that even once consensus had been achieved, compliance with decisions regarding just how the network should be designed and run would not necessarily be either immediate or automatic. Also, although it was

This material is based on work supported by the National Science Foundation under Grant No. 0823265, and by the University of Wisconsin-Milwaukee Office of Undergraduate Research. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author.

Received 16 July 2013
Revised 16 July 2013
Accepted 17 July 2013

understood that commercialization was a number of years off, there was a need to account for usage and consider cost. There was even more extensive discussion of governance within the first decade of the RFCs from the perspective of the law-like functions of the network design process itself than there was of the formal requirements of government(s).

Internet designers thus encountered two faces of governance. They saw that government laws, regulations, and policies would affect the nature of the network in ways so fundamental that they would, or should, affect how the network itself should be designed – governance of the network. They were also conscious that protocol design decisions achieved via the RFCs needed to be effectively and meaningfully authoritative for the network to run – governance by the network. It is the intertwining of the two types of governance, each simultaneously undergoing transformation, that is at the crux of debates over governing the internet in the twenty-first century. Study of both as each unraveled during the first decade of the design process, the ''framing years'' (Braman, 2011), can deepen our understanding of the tensions and battles taking place today. Analysis of the network designer discussions of governance while the development of the network was still directly under US government control (Abbate, 1999; Mueller, 2004), presented here, should be worthy of our attention because through that discourse the paths were laid for the development of governance mechanisms that followed. The subject matter should also be of interest to those focused on the evolution of new forms of transnational governance.

Sociolegal scholars who study the legalization of organizations may find this research useful as an example of the utility of exploring the legalization of sociotechnical, network, and other exploratory, ephemeral, and/or emergent communities as well. The community of those involved in the design process increasingly found themselves ''legalized'' in a manner different from but related to the types of legalization processes that have been the subject of such fascinating work by sociologists of organizations and scholars of law and society in recent years. Although there is a strong and valuable literature on the legalization of organizations, including attention to the ways in which organizations use such processes as a means of influencing law and policy[3], the same cannot yet be said for the legalization of sociotechnical communities.

The method used for this study was a comprehensive inductive and adductive reading of the texts. This study is one among several that reports on findings from a comprehensive reading of every publicly available document in the RFCs during the first decade, itself a subset of a larger project examining the RFCs as a discursive corpus for the first 40 years of the process, 1969-2009. Every RFC was read in its entirety and coded for over 70 variables ranging from the presence of particular concepts through treatment of specific legal and policy issues, decision-making problems and processes, cultural features, implicit or explicit social theory, and on. The subset of texts analyzed for the study reported upon here included those coded for governance with subcodes that included ''government'', ''governing bodies'', ''compliance'', ''legality'', and ''political analysis'' as well as the general question of ''who governs''. Among documents coded for law, subcodes included ''contract'', ''legal uncertainty'', ''pertinent law'', ''regulation'', and ''law-like RFC features''.

Not all RFCs are equivalent in terms of relative influence either within or outside of that discourse, but most of the authors involved in the governance discussions during the first decade were and are individuals who have had a great deal of impact on the development of the internet. Discourse analysis has been a common approach in communication policy analysis since the discursive turn swept across the social sciences in the 1990s[4], under the influence of the work of Michel Foucault (1972) and historians such as, importantly, Robert Wuthnow (1989), who examined relationships among knowledge formation, communication, and power. This study is atypical, however, in the technical nature of the discourse studied, and in its inclusion of standard-setting practices within the realm of governance deserving of such attention.

The ''by the way'' nature of the discussion about political and policy matters – the fact that in most cases these thoughts were offered as side comments in the course of a technical argument – made it necessary to read through every single sentence of each document, irrespective of the target subject matter or how technically detailed the content looked or the

target subject matter. It was impossible to know from title, abstract, or opening material whether or not there would be, perhaps buried in the midst of descriptions of commands or in defense of a particular technical choice, a comment about a policy issue such as privacy or concern over the likelihood of compliance. The value of such side comments in long-lived public and published discussions among experts on constitutive and constitutional subjects has long been recognized in US law, where they are known as ''dicta''. Dicta (plural of ''dictum'') in any court opinion include all statements beyond those that assert the point of law that is the crux of the decision. They are considered authoritative, though the reach and weight of that authority differ with jurisdiction. Dicta in US Supreme Court opinions are extremely important, often providing arguments that become decisive in later cases whether they initially appeared as dicta in the opinion of the Court, or in a concurrence or a dissent. (In the USA, justices of the Supreme Court are free to publish their disagreements with the official opinion of the Court [itself reached by vote among the nine justices], clarifying analytical differences and consequent departures in judgment, whether those ultimately support the decision of the Court or not, either in whole or in part. These concurring and dissenting opinions are also a part of the official and publicly available record.)

The comments mined for analyses of the ways in which the electrical engineers and computer scientists involved in internet design are the dicta of constitutive decision-making for the information and communication infrastructure through which most of our social and other processes now take place. Some background on the RFCs is therefore useful before turning to the treatment of both faces of governance in this sociotechnical design discourse. As is the case with states, the type of large-scale sociotechnical infrastructure being designed appears at the conjuncture of social, technological, and informational systems. Looking across the types of governance issues, tools, and regulatory approaches – again as is the case with states – allows the researcher to identify issues affecting the identity, structure, borders, and change of such systems.

## The internet RFCs as a policy discourse

It was Brian Kahin, beginning early in the 1990s, who first started publicly discussing the need to treat the RFCs as policy documents. He did this in the course of his three-pronged program, which should be given more credit for its role in conceptualizing and shaping the field of internet policy. This program included organizing a series of conference series for many years, from his base at Harvard's Kennedy School of Government; editing book collections that published the best of the work presented at each conference, providing a first roadmap of each of the policy issue areas; and building an archive of all policy documents related to the internet. This archive is now housed at the Babbage Institute at the University of Minnesota and is available for scholarly use. Kahin explicitly discussed RFCs as policy documents in print in one of the books that were among the many work products of those conferences (Kahin and Keller, 1997). By 2013, the homepage of the RFC Editor, the site hosting the RFCs and metadata about them supported by the Internet Engineering Task Force (IETF), itself describes the RFCs as policy documents: the RFC Series ''Contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force'' (see www.rfc-editor.org).

This study uses inductive and deductive approaches to read the RFCs as a bounded discourse comprised of a clearly identifiable and publicly available set of documents in an organized set of technical documents that have authoritative status in the management of the internet because they are the official source of technical standards. Processes begun within the RFCs and/or dealing with problems and issues identified in the course of technical discussions, have had additional lives beyond this discourse with outcomes that include the Internet Corporation for Assigned Names and Numbers (ICANN). Here, these documents serve as historical evidence of the ways in which the computer scientists and electrical engineers involved in design of what we now call the internet during its early years thought about governance matters as broadly defined. An introduction to the history of the document series itself provides a background for thinking through the nature of such a history *vis-à-vis* the three different types of histories the document series itself provides.

*History of the RFCs*

The conversation about how to design a new type of telecommunications network took place not only, but in significantly influential part, within the technical document series known as the Requests for Comments. The RFCs were launched by then graduate student David Crocker, who presented them as an opportunity to document informally design discussions and decisions among those in a project community that was officially distributed across five institutions from the start, i.e. BBN, the consulting firm that served as the contractor with the US federal government's Advanced Research Projects Agency (the ''ARPA'' of ARPAnet), and the four universities with which BBN contracted in turn to do the network design work itself. Participation in the conversation was open to all who were interested, and from the start came from many more institutions than those under direct contract with BBN. Contributions of all kinds, however informal and however speculative, were actively welcomed. The RFC conversation continues today, at the time of writing including 6,975 documents, freely accessible on the website still hosted by the IETF (see www.ietf.org/rfc.html).

The purpose of the RFCs was and is to identify and explore technical issues upon which a consensus needs to be reached in order for a working network to function in a manner that supports a wide range of uses and users. It was not until discussion about commercialization of the internet began in earnest in the early 1990s that documents explicitly focusing on political matters began to appear. While discussions about just what a commercialized network would look like were underway, for example, Mitch Kapor of the Electronic Frontier Foundation published an argument for open access (RFC 1259). However, many legal and policy issues received attention from the start (Braman, 2010). In a few cases, designers of the internet identified as policy issues matters that were not addressed by the US government until much later. For example, beginning in 1971 there were 30 RFCs discussing matters of data integrity, a concept that the *Oxford English Dictionary* reports did not show up in print in a legal context until 1986 (over 30 years after its first appearance in a computing context) and that did not receive statutory treatment in the USA until the Federal Data Quality Act of 2001. In other areas, though – notably privacy – the concerns of network designers and policy-makers in the legal arena resonated strongly; about 17 percent of the documents during the first decade of the design process dealt with privacy, which received significantly more attention than any other single social issue other than generalized fears of bad actors and rogue processes (Braman, 2012b).

*RFC histories of the network design process*

The RFCs offer at least three histories:

1. that which was and is intended;
2. that which appears self-reflexively within the process; and
3. that which becomes available when the corpus is analyzed through theoretical lenses.

As intended, the RFCs document the history of the design process by serving as a repository of the conversation as it was enacted in print; in this sense the document series is a medium. Because the RFCs were not the only medium, and because of the nature of the document series itself, this history is neither comprehensive nor systematic beyond inclusion of all of the official internet protocols.

There is a second history of the design process presented within the series itself that is self-reflexive. Beginning with RFC 3 and continuing on in 62 of the documents produced by the close of 1979, RFCs marked stages in the history of the design process. RFC 33, for example, described the moment when the initial network of four sites actually came into use, and RFC 89 reported on ''Some historic moments in networking'' achieved as firsts during completion of a network control program at MIT. It was Vint Cerf again, in May 1974, who opened a theoretical and pragmatic justification for the redesign of basic ARPANET protocols by noting that ''The history of the Advanced Research Project Agency resource sharing computer network (ARPANET) is in many ways a history of the study, development, and implementation of protocols'' (RFC 635, p. 1) – that is, the history of the network is the history of the protocol development process recorded in the RFCs.

This self-reflexivity provided part of the experiential foundation for the gradual formalization of decision-making; this took place first for the design process with proceduralization of the submission, approval, and publishing of RFCs, and then for governance of the network itself. There was a call for behavioral and administrative as well as technical standards as early as 1971, when two authors employed by the Rand Corporation argued that social norms were a necessity for the user community. The desire for behavioral standards also led them back to technical standards; after describing the dependence of researchers at Rand and elsewhere on programmer members of the user community who served to ''buffer'' them from network detail, they wrote: ''Standardization of services is certainly a great value in expanding the community of users and eliminating the buffer'' (RFC 231, p. 1).

A third type of history becomes discernible only via an inductive and adductive reading of the RFCs as policy documents analyzable through diverse social theoretical lenses. It is in search of this history that the study discussed in this article examined texts for ways in which network designers thought about governance in the course of resolving technical design problems. It is notable that both the social and the technical sides of the governance of this large-scale sociotechnical network were introduced into the conversation during the same period. Because governance is the frame, the next section explores how governance was perceived as a design problem during the first decade of the process; those following address, in turn, the types of governance issues and policy tools were discussed during this period.

## Governance as a design problem

Within the first couple of years of the launch of the ARPAnet project, uncertainty about the future legal status of the network and ambiguity regarding the current legal status of sites linked to the network but not contractually bound to ARPA became design problems. Two documents in 1971 identified the big questions. Both started from a tension between the public and private sector created by the disjoint nature of the design context compared to the broader regulatory and legal environment. They differed in whether the lens used was that of geopolitical citizenship, with primary allegiance to the state and an emphasis on the social in sociotechnical analysis; or that of network political citizenship, with primary allegiance to the network and an emphasis on the technical in sociotechnical analysis. They also differed in seeming preference regarding the common carriage status of the ultimate network service provider.

The project involved using government funds to build an experimental network serving a variety of government purposes (including research on how to build such a network). The work was being conducted, however, within the context of a telecommunications environment that was, uniquely, private sector rather than public and the expectation that the network would ultimately be made available for commercial and other private sector purposes. The government was key to negotiations with private sector network providers – notably, during the period of this study, AT&T, functionally although not technically a monopoly – because all such entities were regulated by the US Federal Communications Commission (FCC) as under common carriers. Designating a network provider as a common carrier was important, in turn, because of the nature of the obligations such categorization carried with it; historically, these included the requirement to provider service to all comers (universal access), and not to affect the content being carried in any way (no editorial intervention) (Pool, 1983). In the USA, as elsewhere, common carriage is subject to rules and regulations quite different from those applied to broadcasting, even when the separate administrative units responsible for both fall under the same overall organizational umbrella of a single regulatory agency.

The texts of these two foundational governance documents in the RFCs thus revolved around two questions:

1. whether or not AT&T would be running the network in the future; and
2. if so, whether it would be doing so as a common carrier.

Authors of the two documents agreed that in future the network would be provided by one or more private sector entities; they disagreed on the question of whether or not such network service provision would be offered as a common carrier. From the perspective of those making key design and architecture decisions in the early 1970s, the long-term regulatory question was of importance because its outcome was believed to affect significantly the extent to which commercial network-based service providers would need to be taken into account (and the transactions that those businesses would generate). The likely presence of certain types of service providers, and services, in turn would influence the types of functions designers needed to take into account as parameters requiring protocol-based support.

The two documents that broached the overarching governance issues early on differed in a second way that emphasizes their complementarity. The first was presented from the perspective of the technical nature of the sociotechnical infrastructure being built, as manifested in the network. The second, published just a month later, started from the perspective of the social nature of the sociotechnical infrastructure being, as manifested in the law. Taken together, these two documents are interesting examples of policy analysis because they provide an early example of the trend towards ''anticipatory'' policy-making, and they demonstrate that those with technical expertise were clearly understanding the network they were building as a sociotechnical project.

Going more deeply into the detail of discussion of governance within the RFCs brings to light distinctions among perspectives that approach governance from the network political side (what the network community prefers) and those that do so from the geopolitical side (governmental laws). It became clear that designers of the internet understood what they were doing as the building of a sociotechnical – not just technical – system. The question of compliance loomed large, which quickly led to the jurisdictional problem: when was something a matter of network governance, and when was it not?

### *Governance from the network side*

In April of 1971, Robert Kahn of BBN introduced key network governance issues as they were stimulated by the need to consider, as the document was titled ''Host accounting and administrative procedures'' (RFC 136). He would have had an interest in such matters because it was his employer, consulting firm Bolt, Beranek & Newman (BBN), which had received the contract from the Advanced Research Project Agency (ARPA) of the US Department of Defense (DoD) and, in turn, issued subcontracts to the sites where the actual design work was being done. In this text seemingly simple pragmatic questions such as how to bill for network-based services lead immediately into the most fundamental of questions about the nature of the network being built, providing a vivid example of the drama inherent in any debate over accounting schemes (e.g. Goldberg and Moye, 1985; Hopwood and Miller, 1994).

Kahn introduced what he saw as the key network governance issues by asking ten questions. He took care to emphasize that these were intended only to stimulate discussion and should not be taken as statements of his own positions on any of these matters:

1. What regulations, if any, apply to the connection of non-ARPA sites?
2. Who or what operates the Network?
3. What is [*sic*] the criteria upon which new sites should be incorporated into the Network?
4. What is the relation, if any, between the ARPA Network and common carrier services?
5. What procedures are required to bring new sites on board and up to speed?
6. What is the most effective way to characterize their resources?
7. What usage of other Network resources do they anticipate?
8. What procedures will be required for a typical user to obtain access to that host?
9. What is their charging policy and for what items?
10. Are their rates in accordance with government standards? (RFC 136, p. 1).

These questions are cast at varying levels of abstraction. Closest to the ground, and reflecting the fact that at the time the network was a government project, Kahn draws attention to the need to keep rates charged for services in line with government standards. At the most abstract end of the spectrum, he asks an almost theological question: ''Who or what operates the Network?'' (RFC 136, p. 1). In between come questions that can have two answers because of the dual faces of the regulation of sociotechnical systems, the legal and the technical; Question 1 does this markedly. Question 6 may seem opaque to contemporary eyes but refers to the fact that the most fundamental of concepts – such as what is a byte, or a record – needed to be explicitly thought through and consensually defined in order for the design work to go on.

Key operating assumptions and the expectations they engender are laid out, including the likelihood that, at least for a while following the exploratory design period, a private sector entity would provide services to ARPA- and non ARPA-supported contractors who would reimburse the entity for its services. In Kahn's view, this entity would not operate as a common carrier. This position underpinned his argument that all hosts should be required to take on governance responsibilities, with particular attention to access, security, and authentication procedures. Along with such responsibilities comes liability: ''What accounting mechanisms, if any, are needed to deal with events, from which recovery or continuation is not possible . . . '' (RFC 136, p. 4). The possibility of distinguishing among classes of users or working conditions was identified as an issue from the perspective of whether or not a single log-in procedure would be sufficient for all requirements.

Kahn's assumption that ultimately major stakeholders in the development of the network will be profit-oriented private sector entities did not bar him from appreciating the need to incorporate other goals in the design process as well. This led to the question of whether or not any network services ought to be subsidized for the greater good. Following the suggestion that it might be useful to develop a classification system for network resources so that their uses could accounted for separately, and preceding the suggestion that standardized rates for each class of activity be considered, Kahn asks: ''Should some classes of Host activity be exempted from accounting?'' (RFC 136, p. 1).

### *Governance from the legal side*

About a month after publication of Kahn's RFC 136, J. Heafner, of the Rand Corporation, published his ''Minutes of Network Working Group Meeting, 5/16 through 5/19/71'' (RFC 164). Heafner's role recording the conversation was not surprising, given the history: The Rand Corporation had been involved in the development of what we now refer to as the internet since a proposal to build a packet-switched network characterized by redundancy and the use of digital technologies was put forward by its employee Paul Baran in the early 1960s. Rand's location in Santa Monica was the seventh node to come onto the network and took part in the first test of ''distributed'' networked communication in 1969. The Rand Corporation receives contracts from many of the government entities interested in a successful networked computing project.

In this report on discussion of expectations regarding future network management, Heafner presented the governance question as it would appear to a government regulator rather a network administrator. Heafner, too, assumed that a private sector organization would ultimately operate the service under ''Government sponsorship''. However, in direct contrast to Kahn's view, Heafner suggests that, if allowed to do so, AT&T would be very interested in offering the service as a common carrier (RFC 164, p. 28). This RFC offers insight into why the question of private as opposed to public sector control of the network was significant for the network's future, and thus for its design, highlighting the role of entities in a class that would now include the third party intermediaries so important to internet governance: ''The question of profit making time-sharing companies on the Net depends on whether or not AT&T takes over Net operations'' (RFC 164, p. 28).

From a document that, the author assures us, was not edited to ensure comprehensibility for anyone not at the meeting, we learn that while SRI was working on theorem-proving mechanisms over the network, Rand was thinking about ''man/machine synergism'', and IBM was trying to develop a new networking concept. Reports were issued for each single

connection to the network, with Carnegie Mellon reporting two – one fast and one slow. Two Air Force sites were linking up in order to have the experience in preparation for development of a wholly autonomous network. This was the meeting during which the Canadian government emphasized the importance of ensuring that everyone, even in geographically vast and sparsely populated areas, would be able to get online. The UK shared the information that it was thinking it might put up three computers that would become network nodes. MERIT, at the University of Michigan, reported that most of the bugs were out of its hardware. EDUCOM, a nonprofit association serving educational institutions, described a membership of 100 universities of which 60 or 70 had already expressed interest in joining the network and 14 of which had the money in hand and were immediately ready to go. Raytheon, somewhat mysteriously, let those at the meeting know that it was ''indexing behavioral data to allow one to search an index to see if the body of data of interest is within the Network'' (RFC 164, p. 16).

The central design debate during the meeting revolved around the question of the best conceptual analogue for the structure of the network they were trying to build. A professor from Stonybrook offered a ''flexible operating system'' tree-like model that was severely critiqued by Bob Metcalfe, who presented the ARPANet point-of-view that the network is not a tree but a directed graph. (Differences between the two include the degrees of freedom of directionality as well as the fact that directionality is a key dimension of the latter.) What Metcalfe went on to identify as the important governance questions for such a structure are all very familiar to policy analysts half a century later: transparency, autonomy, resource allocation, and, notably, resilience. Metcalfe's comments were followed by discussion of the need for a committee on ''theory'' (RFC 164, p. 23). (Analysis of these documents is beyond the scope of this article, but communication theory and political theory were coded during the inductive reading of the RFCs.)

*The sociotechnical nature of the problem*

Designer appreciation of the fact that they were involved in a sociotechnical – not solely technical – enterprise was evident in RFCs during the first decade dealing with the conceptualization of the network itself. The necessity of interactions between the human and the machinic comes up over and over again. Other work introduces the distinction between the human and the ''daemon'', or machinic, user of the network (Braman, 2011). In the documents on governance, the sociotechnical duality appears in multiple embodiments.

A sociotechnical model of the communication process, one author points out, was embedded in practice. Presaging later French approaches to the economics of telecommunications based on incorporating all activities conducted through and reliant upon the network as part of the *filière electronique*, one author includes the human in the network affected by proposed changes to the Telnet protocol:

> In the design of this protocol, it was apparently assumed that the majority of terminals attached to a TIP would be interactive, be normally used in a character-by-character mode both for transmission to and from the terminal, and normally support a human user who would in effect be in the communication loop. The human user would thus be in a position to detect any significant telecommunication-induced errors both by direct observation of the character stream and, more importantly, by examining the computer output in the context of his ongoing interaction (RFC 230, p. 1).

Just as there was a sociotechnical sense of the nature of the network, so there was a sociotechnical sense of the nature of community formation and maintenance. Authors of a ''Logger Protocol Proposal'', devoted to an interface problem, pointed out that there were benefits to achieving a consensus on technical standards for the network irrespective of what those standards were because ''agreement on a common protocol would tend to foster a sense of Network 'community', which would tend to be fragmented by the local option route'' (RFC 98, p. 2).

The two faces of internet governance were quite evident in RFCs dealing with legality *per se*. There was concern about what might be described as ''internal'' legality, meaning the conformity of code or actions with existing technical standards. Examples of such uses of

the concept include its use in discussion of code syntax (e.g. ''The legal ways of concatenating fields are indicated'', RFC 31, p. 4) and of the acceptability of new code or actions relative to existing protocols (e.g. ''The Init was legal and the socket FS is being activated'', RFC 48, p. 13). There was also concern about what might be described as ''external'' legality that may need to be taken into account when considering code or actions that are technically feasible but may run counter to social standards (e.g. ''The protocol requirements for the user interface to an NCP are that it provided all network functions and no illegal privileges'', RFC 46, p. 9).

Some prohibitions against particular technical functions based in social concerns read very much like those of government-based legal systems:

> The idea of allowing a process to masquerade within the network as another process (even with the best of intentions) by using its socket user code introduces a potentially dangerous security breach. [. . .] it should be a basic protocol law that NO PROCESS WHATSOEVER may request or accept connections or transmit or receive data over a socket having a user code not its own (RFC 49, p. 4).

*Compliance*

The enduring problem of compliance received attention during the first decade of the internet design process via references to its necessity, justifications for insisting upon it, and discussion of possible techniques for achieving it. The first step, what would in the geopolitical context be referred to as the ''rule of law'', had been achieved by the late 1970s even though there were, so to speak, critical legal vacua. As Pogran and his colleagues put it, the network community was characterized by a culture of technical standards in an environment in which in fact there often were none (RFC 724). This characteristic of the network community – an inherent acceptance of rule of law as a logical necessity in more senses than one – would make it much easier to achieve compliance with internet protocols than would otherwise have been the case. This is not to say that there was not resistance. Indeed, as late as 1975, the notion that there might be ''official'' protocols was still being described with some skepticism:

> FTP-2 was established by a duly constituted ARPAnet committee and we are duty-bound to implement it. I don't suppose anyone would actually put it that baldly, but I've heard things which amounted to that. It's silly (RFC 686, p. 2).

As time went on, the urgency of the need for compliance went up. BBN's monthly surveys of the use of the new Telnet protocol made it possible to keep track of the extent to which compliance had been achieved. In September of 1974, for example, BBN reported that 62 percent of sites were not yet using the new protocol and it was noted that ''There is still a long way to go to 100 percent new-protocol implementation'' (RFC 702, p. 1). Perhaps in frustration at the slowness with which compliance was being achieved, in another year BBN announced that compliance with the protocol, its implementation ''had become the top priority item'' (RFC 688, p. 1).

*Conceptualizing the domain*

A key analytical challenge for those studying the law is understanding commonalities across, and interactions among, developments, disputes, and divergences across typical subject matter siloes. In ''ordinary'' times, there is often a choice to be made as to which among a number of different ways of characterizing a wrong for which legal redress is being sought is used to frame the suit, with implications for available courts and other matters as well. At a more abstract, and/or historical level, it is only in this way that it becomes possible to see larger social trends of importance. In extraordinary times, whether of extreme transitions or of exceptional conditions that justify lifting otherwise fundamental constitutional constraints, such cross-issue analysis – internal comparative law, if you will – can help map flows of diverse energies in interactions across the system of systems undergoing change.

The same type of cross-issue analysis will be of value when studying governance of and within sociotechnical communities; some explorations of this type will be found below. In an interesting way, though, there is an additional problem when studying the emergence of

governance within a community not initially, or otherwise, thinking of it. Here the question must begin with identifying the governance issues themselves. This is a translational activity, involving the secondary reading of technical texts for their importance, whether implicit or explicit, to governance. The texts are written to the network political community, the world of those involved in the design, building, and use of the important new type of telecommunications network that has become essential to almost all human activity today. As becomes clear below, there are times when the interests of those in the network political community align with those of the geopolitical community of the state, but there are also times when network political and geopolitical interests diverge. To facilitate comparative analysis of governance within network political and governance within geopolitical communities, the following discussion is organized along the lines used to think through over 30 legal and regulatory issues involving geopolitical governments in earlier work (Braman, 2009). Quite disparate types of policy issues can be grouped together in heuristically valuable ways by thinking of their roles *vis-à-vis* the complex adaptive social, informational, and technological systems that come together in the conjuncture of the internet: by thinking in terms of their impact on identity, structure, borders, and change.

## Identity

For geopolitical states, information policy issues affecting identity arise in quite different ways, including the identity of the individual, the identity of the state, and interactions between the two levels of analysis via identities such as that of the citizen. Issues of authentication are of course key to the network environment and core to the individual identity issues of concern from a governance perspective. Given the enormity of the subject and the significant literature that already exists on authentication issues, they will not be addressed in this article. Instead, the focus will be on the identity of the network, so to speak, involving questions such as where authority over network activity lies, information collection about the network, and formal identification of users as such for purposes of self-regulation.

### *Network subsidiarity*

The question of the appropriate extent of centralization introduced in Kahn's 1971 overview of governance issues discussed above continued as a major theme throughout the first decade of the network design process, as it does at the time of writing in 2013 on a global scale. Though the network supports non-hierarchical systems, it is of course also possible to use the network to run hierarchical systems; being non-hierarchical is a potential, not a necessity. It was believed by those involved in the network design process early on that some centralized management of the network would be necessary; experience reinforced that idea. However, it was also understood that the network would not function well if all decision-making came solely from the top.

Motivations for protecting or wanting local control included the desire for autonomy, efficacy, and the importance of local knowledge. With power located at two levels – in the network and in users' hands – the question of how those two levels of governance relate to each other inevitably arose. The sheer diversity of the nature of governance practices by users raised its own coordination issues. In the USA, the word ''federalism'' is used to refer to the complex ways in which power is shared between the national government and the governments of the states. In the Europe, ''subsidiarity'' is used. In both cases, there have been differences in interpretation and implementation over time and across perspectives. As the more international of the two terms, subsidiarity will be the concept used here to refer to the same problem as it arises in the context of internet governance. These discussions about network subsidiarity and the regulatory roles of ''hosts'' at individual networked computing sites provide background, among other things, on the history of the development of the role of what we now call third-party intermediaries, such as internet service providers (ISPs), as agents of the state.

Kahn introduced the subsidiarity principle in general terms as a requirement for effective network governance: ''Understanding the relationship between service, improvement, reliability and cost will be the responsibility of the Network operator, but [. . .] feedback from the Host sites in this area is absolutely essential'' (RFC 136, p. 2). Specifically, each site was

expected to have its own standards for programming and operational procedures. Presaging an issue that was soon to become serious for those in business and for international relations, Kahn addressed the question of how much information a site or user would have to share with those who manage the network head on. He took the position that each site would be required to share only information about matters that affect external performance with the network operator ''primarily required operations and documentation of procedures'' (RFC 231, p. 2).

Access issues received particular attention as the responsibility of those managing each individual computing site. Although there was concern that a site's printer could accidentally or deliberately be flooded with garbage, for example, network designers decided that safeguards should be site- rather than network-based. From the perspective of a user writing over 40 years later, long after we have become accustomed to denial of service (DNS) attacks as part of our shared experience, some of the discussion about the extent to which this might be a problem appears appealingly innocent: ''I would recommend initial implementations without standard special safeguards in this area. Safeguards would be a site-dependent option. Standard safeguards for the above problem can be easily added later if they really prove necessary and satisfactory ones can be agreed on'' (RFC 221, p. 2).

Some respect for local decision-making grew out of appreciation of the importance of what was literally local knowledge for understanding what could and could not be done via, or with, the network connection. The detailed description of the range of types of information held by local connections to the network, and of their possible uses of or responses to that information, provided in RFC 689's discussion of the ARPANet's host-to-host protocol as it stood in 1975, vividly demonstrated the importance of and appreciation for such local knowledge to network designers. Reliance on site-level practices for identity authentication of their local users also falls in this category. Bob Thomas of BBN argued that it was reasonable to rely on the judgment of users in charge at each site because ''for any host, the host either regards the problem as important and has a mechanism for guaranteeing signatures on local mail or that the host does not regard the problem as important and does not guarantee signature authentication'' (RFC 644, p. 1).

One approach to assuring users of the network of their autonomy was to draw a distinction between standardizing the functions and the ''look and feel'' of services to be offered via the network and standardization of the services themselves. Rand Corporation authors of a document with recommendations for intra-network service centers introduced their thoughts by noting:

> Some areas are identified for consideration in intra-network standardization. We do not describe a methodology for analyzing computer systems; however, such analysis may be appropriate for solving the problems. We also do not enumerate the spectrum of services that may be required. We merely enumerate areas where commonality of appearance and function can be of immediate value to a network user (RFC 231, p. 1).

### *Information collection*

As is classically, and always, the case for those with power, information collection quickly became an important management, or regulatory, tool for the network. In both geopolitical and network political environments, observation of network activity can be both about the self (the act of proprioception) and about the other (targets of surveillance other than oneself).

Beginning with a 1971 ''Status Report'', BBN used the RFCs to publish details about the status of most hosts. The tone provided by the use of quotation marks around the word ''data'' might have been suggestive of the author's sense of the reliability and validity of the information being acquired:

> The information for these reports will be gained from talking to people at each site, and from experimental ''data''. These data will be the results of daily attempts to log into each of the Hosts which might be accessible to a Network user; the attempts will have been made from the BBN prototype Terminal IMP at a random time each weekday (RFC 235, p. 1).

Complaints about inadequate documentation of network equipment began to appear by 1972 (see, for example, RFC 369). Though there was discussion relatively early on of the fact that both the number of messages buffered and the number of bits of encoded data involved were needed for accurate measurement of the capacity of any given channel (RFC 150), it took quite a while for the recording of such data to become systematic. The amount of data believed needed for network management purposes kept increasing, expanding to include such details as the functions and numbers of each socket (RFC 322).

A factor that significantly affected measurement efforts was the constantly changing nature of general network conditions and of the state of any given link. In a 1973 document devoted to the levels of transmission bit rates and delays that the network would have to achieve in order to support audio and video teleconferencing, it was noted that a test that failed in one instance might be repeated successfully within 15 seconds (RFC 508, p. 6). Another ''experiment'', using the Xerox PARC node in 1973, uncovered a second technical barrier to the acquisition of detailed quantitative data about network performance. Before launching into details of incoming and outgoing traffic, the author offered a caveat: ''The statistics will be presented in a rather qualitative fashion, since they were reset each time the system came up'', (RFC 550, p. 1). Noting that it had only taken half an hour to set up the system to gather the data, the author goes on to chide members of the network community: ''I find it regrettable that even those of us presumably engaged in 'computer science' have not found it necessary to confirm our hypotheses about network operation by experiment and to improve our theories on the basis of evidence'' (RFC 550, p. 2).

By 1973, much of the data collection function had been taken over by MIT, and the testing was being undertaken every 20 minutes (RFC 523). The use of both geographic and logical maps of the network, including the hosts connected to it (RFC 597), made visible interactions between the geopolitical and the network political. BBN began tracking rates of compliance by new sites joining the network (RFC 702; RFC 703) and asserted the quid pro quo that became so important among the arguments for compliance discussed further below:

> A host which directly connects into the network must assume the responsibility for implementing this set of protocols. That is the ''price of admission'' to become a network host (RFC 705, p. 2).

If a site did not want to achieve compliance by using BBN's equipment, the company recommended ''front-ending'' with an additional machine between its computer and the network (RFC 705, p. 2).

### *Self-regulation*

Users were encouraged to be systematic in their self-regulation of areas for which individual sites have responsibility. Two user groups were established to help support such efforts. The ''Charter for Arpanet Users Interest Working Group'' opens with a description of the functions these groups were intended to serve:

> The ARPANET Users Interest Working Group (NIC Ident = USING) was formed at a meeting of 15 network people on May 23, 1973 in an attempt to improve the Network user's working environment. USING will attempt to represent the interests and needs of users in the Network community, so as to increase awareness of user requirements and encourage better provision of the need services. The group believes that the network is moving beyond a concentration of resources in self-perpetuating research and development; the Network is becoming a service and its viability as such is dependent on user satisfaction.
>
> A second group, the ARPANET Users Group (NIC Ident = USERS) is organized as a forum for users to express their desires and complaints. Acting as a steering committee and lobby for this group, USING will forward their ideas to the appropriate centers (RFC 584, p. 1).

The charter goes on to make clear that some technical knowledge and commitment would be required for participation in the first of the two groups, while anyone interested was welcome as a member of the second. The scope, defined as ''those facets of Network activity that affect the provision of services to users'' (RFC 584, p. 1), included reliability, resources, and usability matters.

Achieving standing relative to any specific decision-making process, the legal right to have one's voice heard and to issue complaints with which the system must deal, is fundamental among one's always several legal identities. While users had always been welcomed, in general, from the start, it is with the establishment of these user groups that those responsible for design of the network grant standing to those outside of the design community who are using the network. At the point that this is happening, there are still so few users that they can form a group after having established their identities as network users. There may be parallels between these users' groups and the twenty-first century Internet Governance Forum (IGF) that are worth exploring.

## Structure

System structures can be comprised in a multitude of formal and informal ways. The most important structural elements during discussions about governance were formal contracts and informal but powerful community norms.

### *Contracts*

The most immediate, and most used, response to the ambiguity regarding what regulations should apply to non-ARPA sites when they wanted to join the network was the contract. The legal contracts that have become so central to internet governance via ICANN's flow-down contract system (Mueller, 2004) first facilitated the network with ARPA's contract to BBN. It was natural that they were recommended as a means of governing relationships among hosts in the network and between hosts and users (RFC 164).

With contracts come obligations. When it comes to the design and building of large-scale sociotechnical infrastructure, especially during exploratory phases, it may be difficult to specify adequately what form those obligations might or should take. It may be that such specification is considered unnecessary among the few launch individuals on a large project, likely to have been drawn from a relatively small community and pre-existing relationships. Whatever the cause, the expectation that those involved in the network design process should be providing services to government agencies was resented by some. Indeed, pressure to cooperate turned that resentment, in some cases, into active resistance against efforts at network governance. L. Peter Deutsch of SRI succinctly described the problem:

> . . . what obligations does the network community have to act as a service and information resource to the outside world (government agencies in particular) as opposed to its presumed major function of learning about how to build and use computer networks and its actual major function of research in many areas of computing which have nothing to do with networks at all[?]
>
> I feel that the confusion between the ARPANET as a service network and the ARPANET as an experiment in the line of network research, and the frustrations and communication failures resulting from superimposing network responsibilities on top of existing research projects, have not received adequate contemplation by the network community (RFC 446, p. 1).

Another issue that arose as questions about the implications of contractual conditions was the question of whether or not it was legal to publish data about the network given that, at the time, network experimentation was essentially a matter of internal government operations. This question became a problem when BBN considered distributing information it had collected about quantities of information flows from each site; this was resolved in favor of publication of the data within the RFCs (RFC 378).

Informal contracts, too, had effective power. The most effective of these may have been the quid pro quo. As was noted in a description of a piece of equipment that could front-end new computers to link them to the network, ''A host which directly connects into the network must assume the responsibility for implementing this set of protocols. That is the 'price of admission' to become a network host'' (RFC 705, p. 2).

*Community norms*

The emphasis on being a part of the network community, and achieving community-level consensus on decisions made, generated a powerful normative environment (Braman, 2011; Turner, 2008). The costs of not adhering to community norms regarding group discussion and achievement of a community consensus around design decisions were made clear:

> For all its shortcomings, RFC 680 has performed a needed service, just as did RFC 561 before it. It defined additional message header items at a time when this needed to be done. Unfortunately, since the group had not sought ideas and input from others, the specification did not adequately respond to a sufficient set of community needs. In addition, the manner in which the document was promulgated – or not promulgated – left a great deal to be desired. Implementators of message-processing subsystems who had not received RFC 680 proceeded to go their own ways, feeling justified in doing so, while those who accepted RFC 680 as a standard felt justified in complaining to – and about – those whom they considered to be maverick implementors of idiosyncratic message service subsystems (RFC 724, p. 2).

Failure to get sufficient community input when devising new approaches, the authors of this RFC go on to warn, would encourage others to ignore any requests for compliance (RFC 724, p. 4).

The community pressure went so far as to include the suggestion that one must become a community insider in order to understand how to comply. During a discussion of the logistics of front-ending systems newly joining the network that also included scathing critiques of the competence of those who had been linking up new systems to the network, it was asserted that ''it is of the utmost importance that whoever performs the task already have ARPANET expertise, for we know of no case where 'outsiders' have successfully come aboard without becoming 'insiders' in the process'' (RFC 647, p. 5).

## Borders

Borders for three types of systems interact in the design, governance, and use of the internet: those of social systems, informational systems, and technological systems. Elsewhere, interactions between social and technological systems when it comes to defining the ''other'' are discussed (users of technologies other than one's own are ''foreign'') (Braman, 2012a). In the RFCs dealing with governance during the first decade of the design process, two issues involving network borders from the perspective of informational systems were discussed:

1. language affordances at the level of character sets; and
2. the destruction of information that arrives in a manner outside of protocol.

*Language and network borders*

Concern over the very real cultural, political, and economic consequences of a network that was for a long time dominated by English does not always take into account either the very real commitment to internationalizing all aspects of the network from the start of the design process or the equally real technical and organizational problems that had to be resolved before multiple languages would come into use. Early explorations into one of the most fundamental of issues, i.e. the character set to be used to express communications in whatever language, appeared during the first decade of the Internet RFCs. Decisions about which language or languages to allow, prefer, and/or insist upon effectively put in place a type of content regulation that in turn creates a boundary for the network that has cultural and social dimensions as well as technical.

This issue appeared during design of the Telnet protocol. Some were concerned about what they believed would be an ''irreversible'' loss of network control that would follow if sites were allowed to use character sets other than ASCII in their communications. The suggestion was that once network content had been translated into or become intermingled with content using any character set other than the network standard ASCII, the communications were in

essence lost to the network and would never return. The fix recommended in the RFC that most directly confronted this issue was technical, but in a way that would resolve the social and cultural issues; this proposal would require those designing and using other codes to make sure that all of them included a return to ASCII – back into the network linguistically (RFC 340). This was, effectively, a form of content regulation levelled at the code rather than content level, since for the latter it could be argued the proposed restriction would be content neutral. Under conditions in which the network under design and experimentation participated in a global ''network of networks'' (Braden, RFC 1122), treating use of a specific character set as a defining feature effectively establishes one type of network boundary.

### *Information destruction*

The information collection discussed above in the section on identity has powerful structural effects, of course, as well. Issues of information architecture are also matters of state, and of network, governance, although they are beyond the scope of this article. By reference, though, when thinking about the structural tools available for network governance, it should be recalled that the procedures by which information is collected, held, processed, and used are all architectural – structural – features of the societies about whom the information is generated and upon whom decisions based upon it are exercised.

The specific stage in the lifecycle of information that did receive specific attention in the Internet RFCs during discussions of governance in the first decade of the design process was, in essence, the destruction of information. The practice of discarding information has the effects of preventing its receipt, rendering it unusable, and perhaps corrupting or destroying it irreversibly. Discarding information was recognized as a tool in the effort to elicit compliance in a discussion about what to do with data that arrived that was not sent in compliance with protocol but did arrive in a form that was receivable and comprehensible. In their ''Response to RFC 607, 'Comments on the File Transfer Protocol''', Pogran and Neigus took the position that compliance was more important than receivability and comprehensibility; they recommended discarding data that was sent out of compliance. Speaking about the single instance that had triggered the conversation, they justified the practice of destroying information in this way with the argument that: ''The sender of the data has clearly violated the protocol, and the receiver cannot divine the sender's original intent'' (RFC 614, p. 3).

This can also be understood as a form of content regulation, this time translating technical protocol into, in essence, social protocol. One is reminded of the legal struggles over whether or not a prison system has to consider a handwritten plea for life by someone scheduled for execution if that letter was written in a form that was illiterate.

## Change

All of the types of systems that interact in the course of designing, making, and using the internet – social, informational, and technological – undergo change. Change can be incremental or abrupt, random or directed. There are legal and policy challenges in this area when there is a desire to prevent, instigate, or channel certain types of system change. During the first decade of the internet design process, such issues appeared in the form of efforts to reduce certain types of change to the technological system, prevent error as a form of change in the informational system, and used humor as a change management tool in the social system.

### *Reducing change*

Several issues that would now be described as usability problems were mentioned implicitly in a RFC arguing that compliance with protocols was to everyone's advantage because doing so would so simplify their use of the network. Those with online experience were likely to understand the value of simplification in an environment that was currently filled with the need to respond to many different ways of handling each connection, flow, or process:

> During the early phases of specifying this standard, a great deal of concern was expressed over the problems which may be experienced during the transition from the current standard to this new one. We feel that the true problem is the lack of realization that THERE IS NO CURRENT OFFICIAL STANDARD. Enough systems have enough overlapping behaviors to allow the current mail environment to function, but this in no way constitutes a standard.
>
> In fact, we strongly believe that the new requirements imposed by the proposed standard involve less complexity than the ambiguities resulting from the current variations in system behaviors (RFC 724, p. 7).

There was so much variability of the type referred to in this passage that one author, in the course of another document discussing a ''message archiving & retrieval service'', recommended relying on an intermediary software program to do the formatting until network-wide standards for such had been accepted (RFC 744, p. 3).

Usability issues folded together in this statement include the need to deal with so many different ways of setting up and using connections and types of network behavior that intended meaning is often ambiguous. Complexity was identified as an important intervening variable. As a shadow behind all of these, there may be the programming and cultural inclination towards Occam's Razor, the notion that the simplest explanation must be the best.

The analog for this type of argument in the world of geopolitical governance is the ''traffic cop'' argument used to justify the licensing of broadcasting and telecommunications in a legal environment in which it is constitutionally unacceptable to license print. (The crux of the argument is that because a license given is a license that can be taken away, any licensing arrangement for a communication medium is a constraint on free speech). In the electronic context, it is argued, the regulator is needed as a traffic cop in order to ensure that everyone licensed can be heard, since otherwise the communications of one could drown out or interfere with those of others (Pool, 1983).

### *Error prevention*

Errors at the local level, such as mistakes in routing messages, could be catastrophic for the network at large. The ability to reliably deliver error-free flows of information and communication is certainly key to network identity. It can be understood as an effort to prevent change in the informational system, as well. The use of what information scientists have long called ''metadata'' – information about information, as in Dewey Decimal system classification of books – can serve governance purposes in this area. Although a key point of internet design was flexibility in routing options, it became clear to those concerned about governance that there was a limit beyond which unpredictability by one site could be problematic for all. Discussion around a 1971 incident that alerted the community to the problem suggests a means of using mandated metadata (more information collection) as a means of increasing governance capacity for the informational system in service to the goal of reducing technological change and diversity in the technological system.

In a 1971 incident, an error in a machine at Harvard wound up routing all messages through Harvard irrespective of where they were going, with disastrous consequences (RFC 528, p. 2). Though not all local errors had such ubiquitous effects, they were always problematic and frequent enough to lead the BBN author of this document on network reliability issues to highlight that acknowledging such problems required a perceptual shift and an emphasis on compliance. From the perspective of 2013, the final sentence in this quote reads as an extreme example of deadpan humor:

> Initially, it was thought that the only components in the network design that were prone to errors were the communications circuits, and the modem interfaces [. . .] are equipped with a [. . .] checksum to detect 'almost all' such errors. The rest of the system, including Host interfaces, IMP processors, memories, and interfaces, were all considered to be error-free. We have had to reevaluate this position in the light of our experience (RFC 528, p. 1).

*Humor*

Among the many uses of humor in social settings is to smooth periods of transition, solicit complicity, and positively contribute to the formation of community. This was a not uncommon technique during the early years of the internet design process. It is well known that RFCs published on April 1 were likely to be jokes, but humor appears abundantly throughout the document series during that decade. At times it was used in what appears to have been an effort to encourage compliance. In one document, for example, Jon Postel and a colleague opened by announcing that ''The czar of socket numbers [Jon Postel] has established the following assignments . . . ''. Wryly noting that ''not everyone is conforming to their assignments'', they go on to say they ''hope we can resolve this problem with a minimum of disruption''" (RFC 433, p. 1).

Of course humor can also be the tool of the powerful individual exerting, among other things, Weberian charismatic power. This may have been behind Vint Cerf's description of a meeting as ''ridiculously long'', for example, when that same meeting resulted in allocation of 50 percent of the available links in a particular range to Cerf for his assignment as he wished while any communications on the other 50 percent were to be discarded (RFC 323, p. 1).

## Sociotechnical governance: of and by the internet

Edelman and her colleagues in sociolegal studies made an argument, in their article ''On law, organizations, and social movements'' (Edelman *et al.*, 2010), that could and should be extended to communities. As applied to social movements, their point is that interdisciplinary work tends to combine any pairing of two of the three intertwined subjects of concern – the law, organizations, and social movements – but rarely, if ever, all three. It is bringing all three together within a common analytical framework, they submit, that is required in order to understand the phenomena and processes of concern.

So, too, with the study of large-scale sociotechnical infrastructure. Two subjects have dominated the study of internet governance broadly writ:

1. interactions between network development and efforts by geopolitically recognized entities (states, regional governments, and international organizations) to regulate that network; and
2. development of the formal decision-making procedures and entities that comprise the constellations of governance via internet-specific organizations and efforts.

As is demonstrated in this and other analyses of the discourse among Internet designers presented by the RFCs, however, there is at least one more issue – i.e. the growth, maturation and, perhaps, politicization of a network-based community as it moves through the stages of legalization in general (acceptance of, in essence, the rule of law) and its specifics (compliance with technical protocols and community norms).

In the case of internet governance as discussed within the technical document series that records the network's design history, the RFCs, 1969-1979, it is worth highlighting that the computer scientists and electrical engineers involved in the design discussion were well aware that the infrastructure they were building was social as well as technical in nature. Although some of that awareness was begrudging inclusion of human needs in design decisions that would otherwise favor the ''daemon'', or nonhuman, network users (such as software), at other times there was genuine sensitivity to social concerns such as access, privacy, and fairness in the transmission of messages from network users both large and small.

Newcomers to the study of law are sometimes surprised to learn that legal systems are not internally coherent, even those that had undergone an effort to be systematic in a radical redesign situation to be completed in a relatively short period of time. It is inevitable, though, that any new attempts to regulate any type of speech or behavior will be layered over many other approaches to same, as well as individual experiences, current and past public representations of such matters and their manifestations in (or, indeed, as drivers of) popular

culture, and on. While in general not all pieces of a puzzle can be solved simultaneously and instantaneously, in the case of what we now call the internet the nature of the puzzle itself kept undergoing change as the design process that would become the subject of governance as well as a venue through which the tools of governance would be exercised.

From this perspective, it is certainly not surprising that not every element of what would become the governance structures for the internet were evident on the surface of the texts within the RFCs. Almost all of those that did receive attention within this technical document series from 1969-1979 mapped well only the same types of tools as they are used by geopolitically recognized states. In both cases – uses of information policy by a geopolitical entity of a national government and by a network political entity such as, in the early years, the network design community and, later on, ICANN – the same types of tools are used. In both cases, these tools are directed at the identity, structure, borders, and change of and in the social, informational, and technological systems that interact to create the environment for information, communication, and culture.

Once legalization of a community is accomplished, it may or may not take hold with success. Current debates over where the locus of internet governance should reside are among the types of evidence available that the internet governance system's survival in its current form is not guaranteed. It is hoped that the effects of research of this kind – that begin with the asking of the question long before getting to any findings – will contribute to the building of an epistemic, discursive, and pragmatic and effective place for public discussion and decision-making about the ways in which the design and regulation of the network and its uses are recognized as constitutive if not constitutional in nature, and in which participants are drawn from multiple communities of discipline and practice.

## Notes

1. FIt is common practice to refer to RFCs by document number rather than author and year, so that is the practice used here and in the ''RFCs cited'' list.
2. David Clark of MIT, a key figure in the history of the design of the internet and a lead player in efforts to rethink design of the network for the future, provided feedback on this larger project's proposal's initial plan to comprehensively read the complete set of documents for the first 40 years of the design process, through the close of 2009. As someone who has been a long-time contributor to the RFCs and is deeply familiar with their content, context, authors, and impact, his response to this project both early on as it was first conceptualized and several years in, after publication of several items reporting on the project's findings (Clark, 2011), was useful. Clark suggested that the type of comprehensive reading conducted for the first decade of the RFCs was unlikely to be worth the researcher's while beyond the second decade because, in Clark's words, the ore would be ''too low grade'' for the specific analytical purposes of this project. Other methods for identifying text and bounding analytical group boundaries have been and are being used to address some other types of more targeted questions, with the method used often being specific to the question.
3. Key works for the study of the legalization of organizations include Edelman and Suchman (1997), Scheppele (1994), and Sitkin and Bies (1994). For a good introduction to the application of these ideas specifically to analysis of internal decision-making as law-like in nature, see Coglianese and Lazer (2003).
4. For theoretical and methodological discussions associated with this development, see Fischer and Forester (1993), Johnstone (2005), and Wittrock and Wagner (1990). For relatively early examples as applied to communication policy, see Babbili (1990) and Stanley (1990).

## References

Abbate, J. (1999), *Inventing the Internet*, MIT Press, Cambridge, MA.

Babbili, A.S. (1990), ''Understanding international discourse: political realism and the non-aligned nations'', *Media, Culture & Society*, Vol. 12, pp. 309-324.

Braman, S. (2009), *Change of State: Information, Policy, and Power*, MIT Press, Cambridge, MA (first published 2006).

Braman, S. (2010), ''The interpenetration of technical and legal decision-making for the internet'', *Information, Communication & Society*, Vol. 13 No. 3, pp. 309-324.

Braman, S. (2011), ''The framing years: policy fundamentals in the internet design process, 1969-1979'', *The Information Society*, Vol. 27 No. 5, pp. 295-310.

Braman, S. (2012a), ''Internationalization of the internet by design: the first decade'', *Global Media and Communication*, Vol. 8 No. 1, pp. 27-45.

Braman, S. (2012b), ''Privacy by design: networked computing, 1969-1979'', *New Media & Society*, Vol. 14 No. 5, pp. 798-814.

Clark, D. (2011), personal conversation, October.

Coglianese, C. and Lazer, D. (2003), ''Management-based regulation: prescribing private management to achieve public goals'', *Law and Society Review*, Vol. 37 No. 4, pp. 691-730.

Edelman, L.B. and Suchman, M.C. (1997), ''The legal environments of organizations'', *Annual Review of Sociology*, Vol. 23, pp. 479-515.

Edelman, L.B., Leachman, G. and McAdam, D. (2010), ''On law, organizations, and social movements'', *Annual Review of Law and Social Science*, Vol. 6, pp. 653-685.

Fischer, F. and Forester, J. (Eds) (1993), *The Argumentative Turn in Policy Analysis and Planning*, Duke University Press, Durham, NC.

Foucault, M. (1972), *The Archaeology of Knowledge & the Discourse on Language*, (trans. by Sheridan Smith, A.M.), Pantheon Books, New York, NY.

Goldberg, J.P. and Moye, W.T. (1985), *The First Hundred Years of the Bureau of Labor Statistics*, US Department of Labor, Washington, DC.

Hopwood, A.G. and Miller, P. (Eds) (1994), *Accounting as Social and Institutional Practice*, Cambridge University Press, Cambridge.

Johnstone, I. (2005), ''The power of interpretive communities'', in Barnett, M. and Duvall, R. (Eds), *Power in Global Governance*, Cambridge University Press, Cambridge, pp. 185-2004.

Kahin, B. and Keller, J. (Eds) (1997), *Public Access to the Internet*, MIT Press, Cambridge, MA.

Mueller, M. (2004), *Ruling the Root: Internet Governance and the Taming of Cyberspace*, MIT Press, Cambridge, MA.

Pool, I. de S. (1983), *Technologies of Freedom: On Free Speech in an Electronic Age*, Belknap Press, Cambridge, MA.

Scheppele, K.L. (1994), ''Legal theory and social theory'', *Annual Review of Sociology*, Vol. 20, pp. 383-406.

Sitkin, S.B. and Bies, R.J. (1994), ''The legalization of organizations: a multi-theoretical perspective'', *The Legalistic Organization,* Sage Publications, Thousand Oaks, CA, pp. 19-49.

Stanley, M. (1990), ''The rhetoric of the commons: forum discourse in politics and society'', in Simon, H.W. (Ed.), *The Rhetorical Turn: Invention and Persuasion in the Conduct of Inquiry*, University of Chicago Press, Chicago, IL, pp. 238-257.

Turner, F. (2008), *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, University of Chicago Press, Chicago, IL.

Wittrock, B. and Wagner, P. (1990), ''Social science and state developments: the structuration of discourse in the social sciences'', in Brooks, A. and Gagnon, A. (Eds), *Social Scientists, Policy, and the State*, Praeger, New York, NY, pp. 113-138.

Wuthnow, R. (1989), *Communities of Discourse: Ideology and Social Structure in the Reformation, the Enlightenment, and European Socialism*, Harvard University Press, Cambridge, MA.

## Appendix. RFCs cited


- RFC 31, ''Binary message forms in computer'', D. Bobrow, W.R. Sutherland, February 1968.
- RFC 46, ''ARPA network protocol notes'', E. Meyer, April 1970.
- RFC 48, ''Possible protocol plateau'', J. Postel, S.D. Crocker, April 1970.
- RFC 49, ''Conversations with S. Crocker (UCLA)'', E. Meyer, April 1970.
- RFC 98, ''Logger protocol proposal'', E. Meyer, T. Skinner, February 1971.
- RFC 136, ''Host accounting and administrative procedures'', R.E. Kahn, April 1971.
- RFC 150, ''Use of IPC facilities: a working paper'', R.B. Kalin, May 1971.
- RFC 164, ''Minutes of Network Working Group meeting, 5/16 through 5/19/71'', J.F. Heafner, May 1971.
- RFC 221, ''Mail box protocol: Version 2'', R.W. Watson, August 1971.
- RFC 230, ''Toward reliable operation of minicomputer-based terminals on a TIP'', T. Pyke, September 1971.
- RFC 231, ''Service center standards for remote usage: a user's view'', J. F. Heafner, E. Harslem, September 1971.
- RFC 235, ''Site status'', E. Westheimer, September 1971.
- RFC 322, ''Well known socket numbers'', V. Cerf, J. Postel, March 1971.
- RFC 323, ''Formation of Network Measurement Group (NMG)'', V. Cerf, March 1972.
- RFC 340, ''Proposed Telnet changes'', T.C. O'Sullivan, May 1972.
- RFC 369, ''Evaluation of ARPANET services January-March, 1972'', J.R. Pickens, July 1972.
- RFC 378, ''Traffic statistics (July 1972)'', A.M. McKenzie, August 1972.
- RFC 433, ''Socket number list'', J. Postel, December 1972.
- RFC 442, ''Current flow-control scheme for IMPSYS'', V. Cerf, January 1973.
- RFC 446, ''Proposal to consider a network program resource notebook'', L.P. Deutsch, January 1973.
- RFC 508, ''Real-time data transmission on the ARPANET'', L. Pfeifer, J. McAfee, May 1973.
- RFC 523, ''SURVEY is in operation again'', A.K. Bhushan, June 1973.
- RFC 528, ''Software checksumming in the IMP and network reliability'', J.M. McQuillan, June 1973.
- RFC 550, ''NIC NCP experiment'', L.P. Deutsch, August 1973.
- RFC 584, ''Charter for ARPANET Users Interest Working Group'', J. Iseli, D. Crocker, N. Neigus, November 1973.
- RFC 597, ''Host status'', N. Neigus, E.J. Feinler, December 1973.
- RFC 614, ''Response to RFC 607: 'Comments on the File Transfer Protocol''', K.T. Pogran, N. Neigus, January 1974.
- RFC 635, ''Assessment of ARPANET protocols'', V. Cerf, April 1974.
- RFC 644, ''On the problem of signature authentication for network mail'', R. Thomas, July 1974.
- RFC 647, ''Proposed protocol for connecting host computers to ARPA-like networks via front end processors'', M.A. Padlipsky, November 1974.
- RFC 686, ''Leaving well enough alone'', B. Harvey, May 1975.
- RFC 688, ''Tentative schedule for the new Telnet implementation for the TIP'', D.C. Walden, June 1975.

- RFC 689, ''Tenex NCP finite state machine for connections'', R. Clements, May 1975.
- RFC 702, ''September, 1974, survey of New-Protocol Telnet servers'', D.W. Dodds, September 1974.
- RFC 703, ''July, 1975, survey of New-Protocol Telnet servers'', D.W. Dodds, July 1975.
- RFC 705, ''Front-end protocol B6700 version'', R.F. Bryan, November 1975.
- RFC 724, ''Proposed official standard for the format of ARPA network messages'', D. Crocker, K.T. Pogran, J. Vittal, D.A. Henderson, May 1977.
- RFC 744, ''MARS – a message archiving and retrieval service'', J. Sattley, January 1978.
- RFC 1122, ''Requirements for Internet hosts – communication layers'', R. Braden, October 1989.
- RFC 1259, ''Building the open road: the NREN as test-bed for the national public network'', M. Kapor, September 1991.



## Corresponding author

Sandra Braman can be contacted at: braman@uwm.edu