Protocol Politics

The Globalization of Internet Governance

Laura DeNardis

The MIT Press
Cambridge, Massachusetts
London, England

For information about special quantity discounts, please email special_sales@mitpress.mit.edu.

This book was set in Stone Sans and Stone Serif by SNP Best-set Typesetter Ltd., Hong Kong. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

DeNardis, Laura, 1966–
Protocol politics : the globalization of Internet governance / Laura DeNardis.
p. cm.—(Information revolution and global politics)
Includes bibliographical references and index.
ISBN 978-0-262-04257-4 (hardcover : alk. paper) 1. Internet governance. 2. Telecommunication—International cooperation. I. Title.
TK5105.8854.D46 2009
384.3'3–dc22

2008044249

10 9 8 7 6 5 4 3 2 1

1 Scarcity and Internet Governance

Will we shoot virtually at each other over the Internet? Probably not. On the other hand, there may be wars fought about the Internet.[1]
—Vinton Cerf

The Internet is approaching a critical point. The world is running out of Internet addresses. A tacit assumption of the twenty-first century is that sustained Internet growth will accompany the contemporary forces of economic and technological globalization. The ongoing global spread of culture and ideas on the Internet is expected to promote economic opportunity, human flourishing, and the ongoing decentralization of innovation and information production. This possibility is not preordained. It requires the ongoing availability of a technology commons in which the resources necessary for exchanging knowledge are openly and abundantly available. It depends on the availability of open technical protocols on which technological universality and the pace of innovation and access is predicated. It also requires Internet governance frameworks reflecting principles of openness and equal participation.

Scarcity

At the level of technical architecture, the success and growth of the global Internet is straining critical Internet resources, protocol arrangements, and Internet governance structures. Internet Protocol (IP) addresses are one of the resources necessary for the Internet's ongoing global expansion. Each device that exchanges information over the Internet possesses a unique numerical

1. Quote from TCP/IP creator Vinton Cerf in "What I've Learned: Vint Cerf," in *Esquire,* April 2008. Accessed at http://www.esquire.com/features/what-ive-learned/vint-cerf-0508.

address identifying its virtual location, somewhat analogous to a unique postal address identifying a home's physical location. This number is assigned either permanently to a computing device or temporarily for an Internet session. Information is broken into small units, called packets, before routed to its destination over the Internet. Each packet contains the Internet address for both the transmitting device and the receiving device and routers use these addresses to forward packets to their appropriate destinations.

Internet addresses are not an infinite resource. Approximately 4.3 billion available addresses serve the Internet's prevailing technical architecture. These finite resources are not material or natural resources like oil reserves, clean air, or the food supply; they exist at a much more invisible and deeper level of abstraction. They are the critical resources necessary for fueling the global knowledge economy. The traditional technical standard for Internet addresses, called IPv4 or Internet Protocol version 4, originated in the early 1980s and specifies a unique 32-bit number—a series of 32 0s and 1s such as 01101001001010100101100011111010—for each Internet address.[2] This binary number is read by computers, but humans usually express Internet addresses using a shorthand notation called "dotted decimal format" expressed as four octets such as 20.235.0.54.

The address length of 32 bits provides a theoretical reserve of 2^{32}, or approximately 4.3 billion unique Internet addresses. Internet engineers determined the size of the pool of Internet addresses, usually called the Internet address space, in an era prior to the widespread proliferation of home computers and a decade before the development of the World Wide Web. Establishing a reserve of billions of Internet addresses in this context seemed almost profligate and, in retrospect, demonstrated enormous foresight and optimism about the Internet's future.

But in the twenty-first century, 4.3 billion seems insufficient to meet the demands of projected Internet growth and emerging applications. In 2008 an estimated 1.5 billion individuals used the Internet, a usage rate of, at most, 25 percent of the world's six to seven billion inhabitants. At that same time only 17 percent of the 4.3 billion Internet addresses were still available,[3] with an assignment rate of approximately 160 million per

2. Jon Postel, "DOD Standard Internet Protocol," RFC 760, January 1980. This RFC documents the original Internet Protocol specification. See also Jon Postel, "Internet Protocol, DARPA Internet Program Protocol Specification Prepared for the Defense Advanced Research Projects Agency," RFC 791, September 1981.

3. The allocation of the IPv4 address space is consistently documented on the website of the Internet Assigned Numbers Authority (IANA), the institution

year.[4] Newer Internet applications such as Voice over Internet Protocol (VoIP), Internet television, networked appliances, and mobile Internet devices have only begun to place demands on Internet addresses. Internet engineers forecasted that this pace of innovation and growth would completely exhaust the remaining Internet addresses sometime between 2011 and 2015.

The Internet standards community identified the potential depletion of these 4.3 billion addresses as a crucial technical design concern in 1990. At the time the Internet was primarily an American endeavor and US institutions had already received substantial IP address assignments. As the Internet began to expand internationally, Internet engineers expressed concern that the remaining address reserve would not meet mounting access demands or sufficiently accommodate new technologies such as wireless Internet access and Internet telephony. Even though fewer than 15 million individuals used the Internet in the pre-web technical context of 1990, the Internet standards community anticipated an eventual shortage and began crafting conservation strategies and technological measures to address resource constraints related to IP addresses. Short-term measures such as network address translation (NAT) and classless interdomain routing (CIDR pronounced "cider") have helped postpone somewhat the depletion of the IPv4 address place.

Against the backdrop of competing international protocols and a mixture of political and economic questions, the Internet Engineering Task Force (IETF), the standards-setting institution historically responsible for core Internet protocols, recommended a new protocol, Internet Protocol version 6 (IPv6), to expand the Internet address space. Originally designated the *next generation Internet protocol* (IPng), the IPv6 standard expanded the length of each address from 32 to 128 bits, supplying 2^{128}, or 340 undecillion unique addresses. The easiest way to describe the multiplier undecillion, at least in the American system, is a 1 followed by 36 zeros.

---

responsible for global coordination of Internet addresses and other number resources. See, for example, "IPv4 Global Unicast Address Assignments." Accessed at http://www.iana.org/assignments/ipv4-address-space.

4. See Internet engineer Geoff Huston's account "IPv6 Deployment: Just Where Are We?" on *Circle ID*, March 2008. Accessed at http://www.circleid.com/posts/ipv6_deployment_where_are_we.

The protocol selected to become the next generation Internet protocol was not the only option and projected address scarcity was not the only concern. The selection was not straightforward. It involved complex technical choices, controversial decisions, competition among information technology companies, resistance from large American companies to the introduction of any new protocols, and an institutional choice between a protocol developed within the prevailing Internet governance institutions and one promoted by a more international institution. Those institutionally involved in Internet standards governance also recognized, in the context of a globally expanding Internet, international concerns about Americans controlling Internet governance functions such as the assignment of IP addresses and the development of core Internet protocols.

Despite the availability of formal IPv6 specifications and its widespread availability in products, and despite the looming depletion of the (IPv4) Internet address space, the upgrade to IPv6 has *barely begun*. The press, technical communities, and IPv6 advocates have forecasted an imminent conversion to IPv6 for more than a decade. Beginning in 2000, governments in Japan, Korea, China, India, and the European Union established national strategies to upgrade to IPv6. These governments have designated the new protocol as a solution to projected address shortages and also as an economic opportunity to develop new products and expertise in an American dominated Internet industry. In contrast to international address scarcity concerns, US corporations, universities, and government agencies have historically possessed ample IP addresses. The United States, with abundant Internet addresses and a large installed base of IPv4 infrastructure, remained relatively dispassionate about IPv6 until discussions commenced in the area of cybersecurity and the war on terrorism after the terrorist attacks of September 11, 2001. The US Department of Defense formally established a directive mandating a transition to IPv6 by 2008, citing a requirement for greater security and demand for more addresses for military combat applications.[5] IPv6 advocacy groups have cited international imbalances in address allocation statistics as indicative of the standard's significance and have described IPv6 as a mechanism for spreading democratic freedoms, promoting economic development, and improving Internet security.

5. US Department of Defense Memorandum issued by DoD chief information officer, John P. Stenbit for Secretaries of the Military Departments, Subject: "Internet Protocol Version 6 (IPv6)," June 9, 2003. Accessed at http://www.dod.gov/news/Jun2003/d20030609nii.pdf.

These government directives and global IPv6 advocacy efforts have not helped spur significant adoption of IPv6. The success of the protocol depends on critical mass of IPv6 deployment, even among those who do not need it. Many market factors have constrained IPv6 adoption, but technical circumstances have also complicated the upgrade. The distributed and decentralized nature of the Internet's technical architecture precludes the possibility of a coordinated and rapid transition. Areas of centralized coordination exist in the development and administration of technical protocols, but decisions about protocol adoption are decentralized and involve the coordinated action of Internet operators and service providers, governments, and individuals overseeing countless network components and segments that comprise the global Internet. The transition, assuming it happens, can only happen incrementally.

More significant, the new protocol is not directly backward compatible with the prevailing protocol in that a computing device exclusively using IPv6 protocols cannot directly exchange information with a computing device exclusively using IPv4. In other words, an individual using an IPv6-only computing device cannot, without some transition mechanism, directly access the majority of web servers that exclusively use IPv4. The transition usually involves the incremental step of deploying both IPv4 and IPv6 protocol suites or implanting one of several technical translation intermediaries. Most upgrades to IPv6 involve dual protocol stack implementations using both IPv4 and IPv6. Projected scarcity in the IPv4 address space was the original incentive for introducing the new protocol, so IPv6 upgrade strategies that also require IPv4 addresses defeat this purpose. The incentive structure for upgrading to IPv6 is paradoxical. Those wanting (or needing) to implement IPv6 have an incentive to do so but are somewhat dependent on IPv4 users adding IPv6 functionality. The incentive for IPv4 users to add IPv6 functionality is for "the common good" rather than for immediate gain.

The Internet Protocol is only one of thousands of information technology standards, but it is the central protocol required in nearly every instance of Internet use. Computing devices that use IP are on the "Net." IPv6 is a critical issue because it was designed to address the problem of projected Internet address scarcity in the context of globalization. It also serves as a useful case study for how protocols, while often established primarily by private actors, are intertwined with socioeconomic and political order. *Protocol Politics* examines what is at stake politically, economically, and technically in the development and adoption of Internet protocols and the scarce resources they create. It explores the implications

of looming Internet address scarcity and of the slow deployment of the new protocol designed to address this problem.

Protocols

A central thesis of this book is that protocols are political. They control the global flow of information and make decisions that influence access to knowledge, civil liberties online, innovation policy, national economic competitiveness, national security, and which technology companies will succeed. From a technical standpoint, protocols can be difficult to grasp because they are intangible and often invisible to Internet users. They are not software code nor material products but are language—textual and numerical language. They are the blueprints that enable technical interoperability among heterogeneous technology products. Technical protocols are functionally similar to real-world protocols. Cultural protocols are not necessarily enshrined in law, but they nevertheless regulate human behavior. In various cultures, protocols dictate how humans greet each other, whether shaking hands, bowing, or kissing. Protocols provide rules for communicating through language with a shared alphabet and grammatical approach, and conventions for mailing a letter. The information content on an envelope bears the recipient's name and address in a predetermined format. There is nothing preordained about these communications norms. They are socially constructed protocols that vary from culture to culture. Instead of providing order to real-world language and human interaction, technical protocols provide order to the binary streams (0s and 1s) that represent information and that digital computing devices use to specify common data formats, interfaces, networking conventions, and procedures for enabling interoperability among devices that adhere to these protocols, regardless of geographical location or manufacturer.

As a note on terminology, this book will use the term "protocol" synonymously with the term "technical standard," although protocol is often a subset of technical standards referring primarily to networking standards that control and enable the flow of information between computing devices on a network as opposed to other types of technical standards such as data file formats or application-level standards.

Understanding the social implications of Internet protocols requires some understanding of which standards fall within this "Internet protocols" taxonomy as well as the Internet governance processes that control these protocols. Most Internet users are familiar with well-known standards

such as Bluetooth wireless, Wi-Fi,[6] the MP3[7] format for encoding and compressing audio files, and HTTP,[8] which enables the standard exchange of information between web browsers and web servers. These are only a few examples of thousands of standards enabling the production, exchange, and use of information.

The Internet is based on a common protocological language. The fundamental collection of protocols on which the Internet operates is TCP/IP. By its strict nomenclature, TCP/IP is actually two protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). In Internet vernacular, however, the term TCP/IP has a more taxonomical function of encompassing a large family of protocols, historically including protocols for electronic mail such as Simple Mail Transport Protocol (SMTP); for file transfer including File Transfer Protocol (FTP); an assortment of routing protocols; and protocols for information exchange between a web client and web server such as HTTP. IPv4 and IPv6 are two fundamental Internet protocols considered components of TCP/IP.

The TCP/IP suite traditionally groups protocols into four functional layers: the Link layer, the Internet layer, the Transport layer, and the Application layer. The Link layer refers to protocols defining the interfaces between a computing device and a transmission medium and is closely associated with local area network (LAN) standards such as Ethernet. The Internet layer includes standards for network-layer addressing and for how packets are routed and switched through a network. The most prominent example of a standard operating conceptually at this level is the Internet Protocol, including both IPv4 and IPv6. Two important examples of Transport-layer protocols are TCP and User Datagram Protocol (UDP), standards responsible for ensuring that information has successfully been exchanged between two network nodes. Finally, the Application-layer protocols interact with actual applications running on a computer and include critical Internet protocols such as HTTP for web communications and FTP for exchanging files. Figure 1.1 depicts a handful of representative protocols traditionally considered part of the TCP/IP family of protocols.

The Internet's core TCP/IP protocols represent only a portion of the standards required for end-to-end interoperability over the Internet. The Internet's routine support of audio, images, and video has expanded the number of embedded standards necessary for any exchange of information over the Internet. Efficient and universal Internet use requires file format and compression

6. The IEEE 802.11 wireless LAN standards are collectively referred to as "Wi-Fi."
7. MPEG Audio Layer 3.
8. HyperText Transfer Protocol.

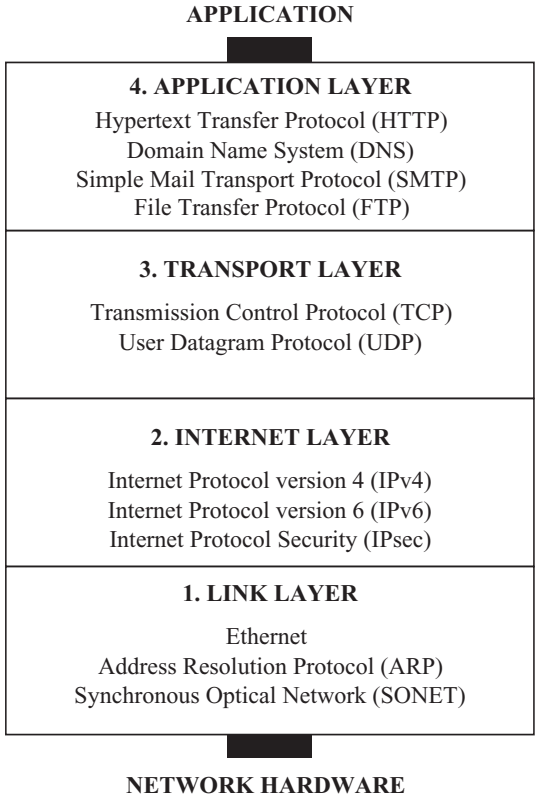

Figure 1.1
Traditional TCP/IP protocol suite

standards such as MP3 for audio files, JPEG for image files, and MPEG for video. VoIP is another critical area of standardization including prominent protocols such as H.323, Real-time Transport Protocol (RTP), and Session Initiation Protocol (SIP). The types of devices accessing the Internet are equally heterogeneous and include cell phones and other handheld devices, household appliances, and laptops. Internet access standards such as the Wi-Fi family of protocols for wireless laptop connectivity, Bluetooth, or GSM for cell phone connectivity are protocols required for routine Internet use.

Private, non–state institutions and some public–private institutions are responsible for the bulk of Internet standards development. The IETF has developed the majority of Internet standards. As an institution it is unincorporated, has no formal membership or membership requirements, and makes decisions based on rough consensus. The IETF, as the developer of the original Internet Protocol and IPv6, will figure prominently in this

book. The World Wide Web Consortium (W3C) is an important, non–state entity that sets Application-layer standards for the web. The International Telecommunications Union's Telecommunications Sector (ITU-T) sets Internet-related standards in areas such as voice over the Internet and security. ITU-T recommendations require consensus and approval of member states. The IEEE (the Institute of Electrical and Electronics Engineers) is a nonprofit professional organization that has contributed many key networking standards ranging from various incarnations of the Ethernet LAN standard to the Wi-Fi family of standards. These are only a few of many institutions involved in Internet standards governance.

This book focuses most heavily on the Internet Protocol. IP has several characteristics that place it at the center of a number of social, economic, and institutional concerns. The first quality is *universality*—IP is a necessary precondition to being on the Internet. Nearly every information exchange over the Internet uses IP. Referring back to Figure 1.1, it is notable that at three of the four protocol levels, there are protocol alternatives. The Transport-layer function can easily include UDP or TCP; any number of LAN technologies can achieve Link-layer functionality; the protocol used at the Application layer is dependent on the application in question (e.g., email, web, voice). At the Internet layer, the primary protocol is IP. Whether IPv4 or IPv6 is being used, IP is the defining protocol for network level functionality. If IP is the least common denominator for communicating over the Internet and the one protocol used in every instance of Internet connectivity, one can envision that this protocol would be relevant to a number of concerns and of interest to those seeking greater control of the Internet.

A second characteristic of IP is *identification*—IP creates a globally unique identifier. As the Internet architecture is currently constituted, no two computing devices can simultaneously use the same address. Regardless of whether an IP address is permanently assigned to a computing device or assigned temporarily for a session, the IP address, along with other information, can potentially provide information about what computing device conducted a specific activity on the Internet at a specific moment in time.

A third characteristic of IP is *exposure*—IP addresses are not encrypted. An important design consideration that potentially factors into concerns about privacy, censorship, and access is that IP addresses are usually "out in the open" on the Internet. Even when information is encrypted for transmission over the Internet, the packet header appended to this information is not necessarily encrypted. IP addresses are included in this header. Given that IP addresses are not encrypted, it is always conceivable to determine the IP address attached to content, even if the content itself is cryptographically protected.

A fourth characteristic is *disinterestedness*—IP locates intelligence at end points. Although this principle is not exclusive to IP, a traditional design feature underlying Internet protocols is to locate intelligence at network end points. Applying this principle to IP, this protocol would not be concerned with the content of packets transmitted over the Internet, or whether the content was viewed, but only with the efficient routing and addressing necessary for the packet to reach its end point.

Examining Internet standardization and the Internet Protocol is an inherently interdisciplinary exercise involving technology, culture, politics, institutional economics, and law. To confront this inherent interdisciplinarity, *Protocol Politics* is heavily influenced by the field of Science and Technology Studies (STS); accounts of standards as political from Janet Abbate and other historians of technology; the work of legal scholars such as Jack Balkin, Yochai Benkler, Larry Lessig, Anupam Chander, and Madhavi Sunder; and the field of institutional economics, particularly as applied by Internet governance scholar, Milton Mueller.

Politics are not external to technical architecture. As sites of control over technology, the decisions embedded within protocols embed values and reflect the socioeconomic and political interests of protocol developers. In a discussion about debates over Open Systems Interconnection (OSI) versus TCP/IP in *Inventing the Internet*, Janet Abbate notes that technical standards are often construed as neutral and therefore not historically interesting. Perceptions of neutrality derive in part from the esoteric and concealed nature of network protocols within the broader realm of information technology. As Abbate demonstrates, "The debate over network protocols illustrates how standards can be politics by other means. . . . Efforts to create formal standards bring system builders' private technical decisions into the public realm; in this way, standards battles can bring to light unspoken assumptions and conflicts of interest. The very passion with which stakeholders contest standards decisions should alert us to the deeper meanings beneath the nuts and bolts."[9] Many of the research questions *Protocol Politics* examines emanate from Abbate's view about debates over protocols bringing to light unspoken conflicts of interest.[10]

9. Janet Abbate, *Inventing the Internet*, Cambridge: MIT Press, 1999, p. 179.

10. Like Abbate's account, other historical works similarly reinforce this political dimension of technical standardization. For example, Ken Alder's account of the development of the metric standard during the French Revolution, *The Measure of All Things: The Seven-Year Odyssey and Hidden Error That Transformed the World* (New York: Free Press, 2002), examines how seemingly neutral and objective standards are historically contingent and embody both political and economic interests.

Protocol Politics also asks questions about how protocols, once developed, have political meanings that can be adapted for various purposes.[11] The decisions made during protocol design can have significant public policy consequences. From an advocacy standpoint, the Internet Standards, Technology and Policy Project at the Center for Democracy and Technology (CDT) in Washington, DC, has raised awareness about the public policy consequences of Internet standards. Increasingly, policy decisions about whether to advance or restrict online freedoms occur in the technical standardization process invisible to the public and established primarily by private industry rather than legislatures. When Internet engineers designed the Internet address structure for the new IPv6 standard, they decided to build some privacy protections into the protocol. The CDT's project sought to increase public awareness and to inject a public voice into this technology-embedded form of public policy.[12]

Standards are not software code but language. If code is "law"[13] regulating conduct similar to legal code, or even if software is its own modality of regulation unlike law or physical architecture,[14] then the underlying protocols to which software and hardware design conforms represent a more embedded and more invisible form of legal architecture able to constrain behavior, establish public policy, or restrict or expand online liberty. In this sense, protocols have political agency—not a disembodied agency but one derived from protocol designers and implementers. There is no remote corner of the Internet not dependent on protocols. They are control points, in some cases, areas of centralized control, and sometimes distributed control, mediating tensions between order and freedom.

11. See, for example, Paul Edwards's critical integration of political and technical histories in *The Closed World, Computers and the Politics of Discourse in Cold War America* (Cambridge: MIT Press, 1996), examining how cold war "politics became embedded in the machines—even, at times, in their technical design—while the machines helped make possible its politics." (p. ix).

12. See, for example, Standards Bulletin 2.01, "ENUM and Voice over Internet Technology," April 28, 2003; Standards Bulletin 1.03, "Patents on Internet Technology Standards," December 13, 2002; John Morris and Alan Davidson, "Policy Impact Assessments: Considering the Public Interest in Internet Standards Development," 2003; and Alan Davidson, John Morris, and Robert Courtney, "Strangers in a Strange Land: Public Interest Advocacy and Internet Standards," 2002. Papers accessed at http://www.cdt.org/standards.

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

14. James Grimmelmann, "Regulation by Software," 114 *Yale Law Journal* 1719 (2005).

Internet protocols are an example of what Yochai Benkler calls *knowledge-embedded tools*, similar to enabling technologies for medical and agricultural resources.[15] Knowledge-embedded tools, such as open (vs. proprietary) standards, are necessary for enhancing welfare and enabling innovation itself. Internet standards such as TCP/IP and HyperText Markup Language (HTML) have historically been openly available, enabling citizens and entrepreneurs to contribute to Internet innovation, culture, and electronic discursive spheres. Other widely used technical standards do not exhibit this same degree of openness. From an economic standpoint, standards have significant effects such as enabling or restricting global trade and enabling competition and innovation in product areas based on common standards. [16] As David Grewal suggests in *Network Power*, the "creation and diffusion of standards underlying new technologies is a driving element of contemporary globalization."[17]

A striking feature of this type of social force is that it is established by institutions, often private institutions, rather than by elected representatives. Following Milton Mueller's approach in *Ruling the Root: Internet Governance and the Taming of Cyberspace*, this book draws from institutional economics—the intersection of law, economics, and politics. Much work has been done on the critical role of institutions in creating the world around us.[18] *Protocol Politics* examines institutional dynamics but also highlights the critical contributions of key individuals in the evolution of Internet governance and their contributions to the rise of new production models embraced by Internet governance institutions. These models transcend national boundaries, bypass intergovernmental organizations, and challenge traditional beliefs about economic behavior. One objective of this book is to examine the institutional

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

16. See Rishab Ghosh, *An Economic Basis for Open Standards*, December 2005. Accessed at http://flosspols.org/deliverables/FLOSSPOLS-D04-openstandards-v6.pdf.

17. David Grewal, *Network Power: The Social Dynamics of Globalization*, New Haven: Yale University Press, 2008, p. 194.

18. For example, Arturo Escobar suggests, "The work of institutions is one of the most powerful forces in the creation of the world in which we live," in *Encountering Development, The Making and Unmaking of the Third World*, Princeton: Princeton University Press, 1995, p. 107. See also Yochai Benkler, "Coase's Penguin, or, Linux and the Nature of the Firm," 112 *Yale Law Journal* 369 (2002), for an exploration of new "commons-based peer-production" models of large-scale collaboration motivated by a variety of incentives distinct from managerial hierarchy or market prices.

characteristics and principles necessary to maximize the legitimacy of private institutions to establish global knowledge policy.

An Internet Governance Framework

Questions about Internet standardization and the IP address space are questions about Internet governance. While the distributed architecture and ubiquity of the Internet can convey the impression that no one controls the Internet, coordination—sometimes centralized coordination—occurs in several technical and administrative areas necessary to keep the Internet operational. John Perry Barlow, in *A Declaration of the Independence of Cyberspace* written to traditional world governments, wrote that "We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different."[19] But there have always been some centralized governance functions in cyberspace, although not governance by sovereign governments or even intergovernmental organizations.

The term "Internet governance" has many definitions and is a highly contested term.[20] Internet governance functions have been around for far longer than the term Internet governance. Even the term "governance" in this context requires qualification because Internet governance actors have not primarily been governments. As Milton Mueller explains, there are sometimes two extreme views about who controls the Internet: the view that the Internet is inherently uncontrollable and therefore not controlled; and the antithetical view that a small cabal of individuals and corporations has authoritative hegemony over the Internet. As Mueller suggests, "For any complex sociotechnical system, especially one that touches as many people as the Internet, control takes the form of *institutions*, not commands."[21] The functions these institutions control can be quite expansive, depending on how one defines Internet governance.

19. John Perry Barlow, "A Declaration of the Independence of Cyberspace," 1996. Accessed at http://homes.eff.org/~barlow/Declaration-Final.html.
20. See Jeanette Hoffman, "Internet Governance: A Regulatory Idea in Flux," 2005. English translation accessed at http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf.
21. Milton Mueller, *Ruling the Root*, Cambridge: MIT Press, 2002, p. 11.

Internet governance refers generally to policy and technical coordination issues related to the exchange of information over the Internet. Many conceptions of Internet governance, especially those emanating from technical communities, are quite bounded in scope, describing Internet governance as having three distinct functions: "(1) technical standardization, (2) resource allocation and assignment, and (3) policy formulation, policy enforcement, and dispute resolution."[22] Many Internet governance examinations inquire within a closed sphere of institutional interactions and their internal technical decision-making processes. This type of inquiry does not necessarily reflect the contextual milieu that shapes decisions or the broader social implications of these decisions. The underlying framework of *Protocol Politics* rests on a broader view of Internet governance to create openings for examining how values shape Internet governance decisions and for assessing the economic, legal, and political externalities of these decisions.

In addition to Internet standardization there are four additional areas of Internet governance, with Internet governance broadly conceived: critical Internet resources, intellectual property rights, security, and communication rights.

Critical Internet Resources

In regard to critical Internet resources, the topic that receives the most press and scholarly attention is the role of ICANN as a global governance institution and its associated policies about the management and assignment of Internet domain names and numbers. Most of this concern addresses domain names. The domain name system (DNS) serves a critical function necessary for the successful operation of the Internet, translating between alphanumeric domain names and their associated numerical IP addresses necessary for routing information across the Internet. The DNS performs this address resolution process and resolves billions of queries each day. The DNS is really an enormous database management system distributed globally across numerous servers and operating like a hierarchical tree. The component (.gov, .edu, .com, etc.) on the far right of any domain name is called the top-level domain (TLD). Other top-level domains are country codes, or ccTLDs, such as .br for

22. Internet Governance Project White Paper, "Internet Governance: The State of Play," September 2004. Accessed at http://www.internetgovernance.org/pdf/ig-sop-final.pdf. The Internet Governance Project is a partnership of scholars at Syracuse University, Georgia Institute of Technology, and Wissenschaftszentrum Berlin für Sozialforschung.

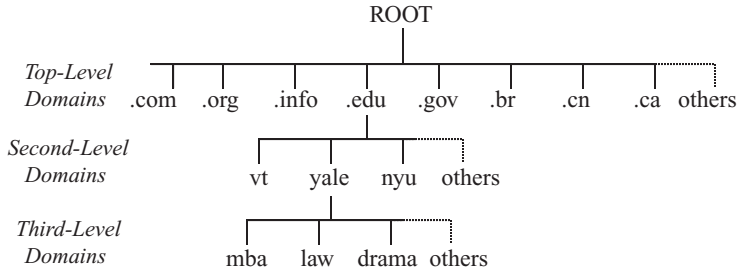

Figure 1.2
Domain name space

Brazil, .ca for Canada, and .cn for China. In domain name semantics, the word to the left of the top-level domain is called the second-level domain, such as the "yale" in "yale.edu." Figure 1.2 conceptually depicts a small portion of the domain name space. The Internet's root name servers contain a master file known as the root zone file itemizing the IP addresses and associated names of the official DNS servers for all top-level domains.

The domain name system establishes the domain name space in the same way that the Internet Protocol establishes the Internet address space. As critical resources necessary for Internet connectivity and use, the management of the Internet address space and the domain name space are central tasks of Internet governance. This function includes the actual allocation and global coordination of Internet domain names and numbers. Within ICANN, the Internet Assigned Numbers Authority (IANA) is responsible for root zone management for the DNS, as well as globally coordinating the IP address space. Internet governance concerns about the DNS include controversies about the assignment of top-level domain names, conflict over authority and control over the root zone file and root name servers, issues of national and transnational jurisdiction, questions about institutional legitimacy, and a host of policy questions dealing with critical infrastructure protection, intellectual property issues related to domain names, dispute resolution, and institutional questions of legal and political responsibility.

One objective of *Protocol Politics* is to bring more attention to the IP address space in the Internet governance realm of critical Internet resource management. A major analytical theme will address how new technologies create new resources. This theme is not unique to Internet governance. Battles over technologically derived resources are a central issue of information and communication technology policy, whether

addressing electromagnetic spectrum or bandwidth in network neutrality debates. What may be unique about Internet addresses is that they are a completely global resource that has always been centrally coordinated by some Internet governance entity. The Internet Protocol (both IPv4 and IPv6) created Internet addresses. In the case of the prevailing IPv4 protocol, the resource pool contains a theoretical maximum of approximately 4.3 billion addresses. The IPv6 address space contains 340 undecillion addresses. Like electromagnetic spectrum and other technologically derived resources, Internet addresses carry significant network externalities and economic value. This value cannot be assessed within the traditional sphere of market economics because, as of yet, these finite resources have never been exchanged in free markets. Centralized control of IP addresses has historically existed to maintain the architectural principle of globally unique addresses. A single individual, Jon Postel, originally administered these finite technical resources but responsibility gradually shifted to geographically distributed, international registries known as regional Internet registries (RIRs). Despite this global dispersion of IP addresses and assignment responsibility, definitive oversight of the entire address reserve, including the allocation of address resources to international registries, has remained centralized, eventually becoming an IANA administrative function under ICANN.

The extent to which Internet addresses have critical technical, economic, and political implications raises governance questions about how access to resources and power over these resources are distributed or should be distributed among institutions, nation-states, cultures, regions, and among entities with a vested economic interest in the possession or control of these resources. This book examines IP address creation and distribution not only from the standpoint of institutional economics and efficiency, but from normative and overarching questions of distributive justice.[23]

Intellectual Property Rights

In addition to critical resource management, intellectual property rights are a significant Internet governance concern. Decisions related to intellectual property rights order the flow of information, creativity, and compensation over the Internet. This area encompasses issues such as trademarks, patents, and copyright, and the balance between intellectual

23. Anupam Chander explains that, in cyberlaw scholarship generally, concerns about human values such as distributive justice and equality are greatly neglected. See Anupam Chander, "The New, New Property," 81 *Texas Law Review* 715 (2003).

property protection and the Internet's tradition of free and open access to knowledge. One objection to including intellectual property as an Internet governance concern is the argument that Internet governance should only address technical architecture and critical resources, not content. This argument quickly breaks down because intellectual property rights enforcement is often implemented within technical architecture, such as copyright filtering or digital rights management (DRM) technologies and because some of the greatest intellectual property concerns address technical architecture itself rather than content. Copyright and patents in technical standardization are particularly complex areas intersecting with innovation policy, antitrust concerns, economic competition, and the openness of the Internet. Intellectual property scholar Mark Lemley describes the problem of patent owner holdup, particularly in the technical standardization context, as "the central public policy problem in intellectual property law today."[24]

Intellectual property questions are also at the heart of many domain name controversies, such as trademark disputes over domain name registrations. Traditional legal remedies for Internet trademark disputes have not always been helpful because of uncertainty about which country's laws have jurisdiction in any given dispute and because traditional legal intervention is a lengthy process relative to the pace of Internet developments. ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) has served as a mechanism for trademark protection in the sphere of domain names but, like most of ICANN's activities, has been controversial.

Intellectual property rights for content itself can also be a purview of Internet governance institutions, particularly if one views intellectual property issues as more about social relations and the ability of humans to engage in cultural production and meaning and free expression.[25] A central question is how to view "fair use" in online environments and how to balance the goal of protecting artists' and authors' rights with a separate set of public interest questions such as improving access to knowledge in the developing world, encouraging digital education, and facilitating the creation of culture and the ability to dissent. Online copyright protection not only places restrictions on copying a work similar to restrictions in the offline world, it can mean additional

24. Mark Lemley, "Ten Things to Do about Patent Holdup of Standards (and One Not To)," 48 *Boston College Law* 149 (2007).

25. See, generally, Madhavi Sunder, "IP3," 59 *Stanford Law Review* 257–332 (2006). "Intellectual property is about social relations and should serve human values."

restrictions in access through technological and legal measures for copyright protection.

Internet governance questions addressing intellectual property occur at many levels. For companies providing Internet services based on common technical standards, one concern is whether they are liable if they host copyright-infringing content. Institutionally, standards-setting organizations sometimes have intellectual property policies such as requiring ex ante disclosure of intellectual property rights among member companies involved in standardization or requiring agreements that any standards-based intellectual property rights be made available on a so-called reasonable and nondiscriminatory basis. As mentioned, ICANN has procedures to deal with trademark protection. Other intellectual property related Internet governance takes place at the national level, such as through the Digital Millennium Copyright Act (DMCA) passed in the United States in 1998, and at the international level through the World Intellectual Property Organization (WIPO) or the World Trade Organization's (WTO's) TRIPS agreement, short for Trade-Related Aspects of Intellectual Property Rights.

Security

Internet security is perhaps the most critical area of Internet governance. When a worm or denial of service attack compromises the Internet's reliability and availability, all other areas of Internet governance seem irrelevant. This Internet governance is particularly complex because security problems involve a wide variety of concerns ranging from critical infrastructure protection to user authentication and because responsibility for Internet security is distributed so widely in a complex matrix of public and private control.

The universality and openness of the Internet make it a prime target for attacks, whether for reasons of criminal activity, terrorism, or to advance a political agenda. The most publicly understood security problems are viruses, malicious code embedded in software that inflicts damage when the code is executed, and worms, self-replicating and self-propagating code that exploits weaknesses in protocols and software to inflict harm. These types of attacks can be costly. According to congressional testimony, the "I Love You" virus that spread throughout Asia, Europe, and North America affected 65 percent of North American businesses and infected 10 million computers.[26] Distributed denial of service (DDoS) attacks are an even

26. US House of Representatives, Subcommittee on Technology, Committee on Science Hearing on Computer Viruses, May 10, 2000.

greater threat. These attacks hijack computers, which unknowingly work together to disable a targeted computer by flooding it with requests. The targets of these attacks have included the Internet's root servers, high-profile commercial websites, and government servers.[27] Other types of Internet security concerns include identity and password theft, data interception and modification, and bandwidth piracy. Critical infrastructure protection, whether of physical telecommunications infrastructures or on a critical Internet system such as the DNS, is always a concern. Hackers can use computing systems to disrupt physical infrastructures such as when a disgruntled employee broke into a computer system controlling an Australian sewage treatment plant and released millions of liters of raw sewage into the environment.[28]

A key Internet governance question about security asks what are the appropriate roles of national governments, the private sector, individual users, and technical communities in addressing Internet security. The private sector develops and implements the majority of Internet security measures. Businesses selling products and services online implement voluntary authentication and privacy mechanisms such as public key cryptography to secure electronic commerce. Service providers, business Internet users, and individual users implement their own access control mechanisms such as firewalls. Standards institutions such as the IETF and the IEEE develop security-related protocols.

Governments also have a role. Most national governments enact policies for critical infrastructure protection and cybersecurity. For example, the US Department of Homeland Security operates a Computer Emergency Response Team (CERT) that works in conjunction with private industry to identify security problems and coordinate responses. Detecting and responding to Internet security problems is a complicated area of public–private interaction and also one requiring transnational coordination. There are hundreds of CERTs around the globe, many of which are hybrid public–private institutions. The coordination of information and responses to attacks among these public–private entities is a critical Internet governance concern.

27. For a history of some DDoS and other Internet attacks, see Laura DeNardis, "A History of Internet Security," in *The History of Information Security*, Karl de Leeuw and Jan Bergstra, eds., Amsterdam: Elsevier, 2007.

28. Parliament of the Commonwealth of Australia, Parliamentary Joint Committee on the Australian Crime Commission, Cybercrime, March 2004. Accessed at http://www.aph.gov.au/senate/committee/acc_ctte/completed_inquiries/200204/cybercrime/report/report.pdf.

Communication Rights

Finally, Internet governance involves concerns about communication rights, particularly when technical architecture design or policy formulation intersects with the public's civil liberties online. Freedom of expression and association are increasingly exercised online and institutional decisions about technical architecture can determine the extent of these freedoms as well as the degree to which online interactions protect individual privacy and reputation. The same technologies that expand freedom of expression have created unprecedented privacy concerns, and Internet governance decisions often must mediate between the conflicting values of free expression and privacy. To the extent that architectural design and implementation decisions and policies determine communication rights, this area should be construed as an important part of Internet governance.

Traditional governments have not historically had the most prominent role in Internet governance, but many communication rights areas that governments have traditionally overseen have converged with Internet infrastructure, raising questions about public versus private Internet control. For example, video delivery no longer depends on traditional broadcast structures, and voice delivery no longer depends on traditional telephone systems. Voice and video have become just like any other application on the Internet, enabled in part by new protocols such as VoIP and Internet Protocol Television. These advancements have complicated Internet governance because of the incompatibilities between prevailing approaches to Internet governance and the governance of traditional media and broadcast. Traditional Internet governance has involved private–public and multistakeholder coordination, has been international in scope, and has embraced the philosophy of making information accessible to everyone. Governments have historically provided traditional broadcast and media oversight. These approaches have been national or regional in scope and have promoted highly controlled flows of information to protect intellectual property and businesses models. Governance models in the context of this convergence are an emerging Internet governance concern, especially to those opposed to the possibility of an increasing role for governments in Internet regulation.

Organization of *Protocol Politics*

The previous section laid out a broad view of Internet governance. The development of IPv6, on its surface, would seem to involve only two facets of Internet governance: Internet standardization and critical Internet

resources. A central theme of this book is that Internet protocols and Internet resource management are not merely issues of establishing technical specifications or administering resources but are issues that traverse all Internet governance concerns sketched out in the framework described above. Protocols involve questions of technical interoperability and the establishment of critical Internet resources, but also questions about intellectual property, security, and communication rights. Many such questions have been traditionally overseen by governments, but they are increasingly being addressed in the technical architecture.

The remainder of *Protocol Politics* is divided into five sections. Chapter 2 examines how protocol selection is a political process as well as a technical issue. The chapter explores how concerns about resource scarcity emerged within the context of Internet globalization, what the alternatives were to IPv6, why they were discarded, and what was at stake in the selection process. The technical standard that became IPv6 was not the only alternative. The Internet engineers selecting the new protocol established a guideline that only technical factors would enter the selection process, but this chapter describes how a significant factor in the selection process appears to have been the selection of which standards-setting institution would have control over Internet standards.

Participants in the Internet standards process first articulated concerns about the Internet running out of addresses in the early 1990s. At the time a set of protocols known as OSI protocols were in competition with Internet protocols to become the universal standard for interconnecting diverse computing environments. The chapter describes how the two final alternatives for the next generation Internet protocol involved a choice between an IETF originating protocol and an OSI-related protocol promoted by the International Organization for Standardization (ISO). If the ISO protocol had been selected, the ability to control and change the key Internet protocol would likely have rested with ISO rather than the IETF, which had historically been responsible for the development of Internet protocols.

By examining IPv6 against its discarded alternatives, this chapter reveals the conflicts among institutions, between trusted insiders and newer participants, and between dominant companies and new entrants, all within the context of increasing Internet globalization. Another chapter theme is the phenomenon of protocol selection occurring extraneous to contemporary forces of market economics.

Chapter 3 examines how the design of protocols can involve decisions that affect the public's civil liberties online. The public policy embedded in

technical standards can present an opportunity either to advance the libertarian ideals historically associated with the Internet's underlying protocols or to restrict access, regulate speech, or impose censorship. Protocol design reflects the values of protocol designers. As Internet engineers designed the technical specifications of IPv6 in the years following its selection, they weighed design decisions related to issues of Internet user anonymity and location privacy. The chapter explains the privacy issue that Internet engineers addressed, describes the process whereby Internet engineers opted to design some privacy protections into the protocol, and recounts contemporaneous concerns raised by privacy advocates, particularly in the European Union. The chapter addresses the implications of private standards-setting institutions establishing public policy, the question of institutional legitimacy, and the issue of how, considering technical barriers to public participation, the public interest can realistically enter these decisions.

Chapter 4 examines the politics of protocol adoption, including the ambitious national IPv6 strategies of governments in China, Japan, the European Union, Korea, and India. Many of the rationales for upgrading had less to do with the increasing reality of Internet address depletion than with promoting other socioeconomic objectives. This chapter suggests that the *promise* of IPv6 aligned with broader political objectives such as European unification goals or attempts to reverse economic stagnation in Asia. The chapter also describes how US politicians began linking the prospect of product development and expertise in IPv6 with the objectives of fighting a more distributed war on terrorism and improving US economic competitiveness in the context of globalization and the outsourcing of American jobs to China and India. The chapter examines how IPv6 advocates and stakeholders also linked the protocol with a number of social and economic development objectives ranging from global democratic reform to third world development. One related issue is the role of open intellectual property rights in Internet standards in opening the possibility of global competition and innovation. Another is the ongoing narrative among advocates of IPv6 providing inherently greater security, a promise that has proved to be highly contestable. Another theme of chapter 4 is how many governments have rejected laissez-faire protocol adoption in favor of sweeping government mandates backed by economic inducements. Finally, the chapter describes the most interesting aspect of government IPv6 adoption policies. National protocol upgrade deadlines have passed with no significant deployment of IPv6. The chapter describes the transition challenges that have hindered IPv6 implementation and assesses prospects for the emergence of a transition strategy.

Chapter 5 examines the Internet address space and how technical protocols create new scarce resources. When the value of these resources becomes clear, their possession and control become a source of global tension. The management and control of Internet addresses is a fascinating issue because a centralized actor has always controlled and allocated these resources and because they have never been exchanged in free markets. This chapter examines the origination and allocation of the Internet address space, the emergence of debates about address scarcity, the evolution of control of IP address assignment, and the near depletion of the IPv4 address space. In the context of describing this evolution, the chapter examines three Internet governance questions: (1) the question of who controls (and who should control) the allocation of Internet addresses; (2) the manner in which these scarce resources are allocated, whether directed toward market efficiency, distributive justice, rewarding first movers, or other objective; and (3) the overarching question of whether there exist sufficient addresses to meet current and anticipated demand.

Chapter 6 presents a general framework for understanding the political and economic implications of protocols in their design, implementation, and adoption. Drawing from the history of IPv6 and other protocols, this chapter examines six ways in which technical protocols potentially serve as a form of public policy: (1) the content and material implications of standards can themselves constitute substantive political issues; (2) standards can have implications for other political processes; (3) the selection of standards can reflect institutional power struggles for control over the Internet; (4) standards can have pronounced implications for developing countries; (5) standards can determine how innovation policy, economic competition, and global trade can proceed; and (6) standards sometimes create scarce resources and influence how these resources are globally distributed.

Whereas Internet protocols and other technical standards have broad political and economic implications, issues regarding who decides in matters of standards setting and how they decide are key questions, especially to the extent that private industry engages in the establishment of public policy. The IETF is only one of many organizations setting standards, ranging from physical infrastructure to applications, necessary to enable the universal exchange of information over the Internet. The IETF has a generally open and transparent approach even though many barriers to public participation exist. But other institutions have different standards-setting norms that lack the openness and transparency of IETF processes. This chapter suggests best practices in Internet standards setting

based on principles of openness, transparency, and economic competition. The rationale for promoting so-called open standards are technical, economic, and political—with the technical rationale of open standards promoting maximum technical interoperability, the economic rationale of enabling competition and minimizing anticompetitive and monopolistic practices, and the political rationale of maximizing the legitimacy of standards-setting organizations to make decisions that establish public policy in areas such as individual civil liberties, democratic participation, and user choice.

The final section of chapter 6 shifts attention back to IPv6 and the limits of both protocol openness and government intervention in influencing standards adoption. The wide discrepancy between a decade of promises about imminent IPv6 adoption and the reality of slow deployment has been one of the most intriguing stories in the history of the Internet. The chapter concludes by exploring the possible implications of IPv4 address depletion and the slow deployment of IPv6 to global Internet access needs, to Internet governance structures, and to the future of the Internet's underlying architecture.