

Making Sense of “Internet Governance:”

Defining Principles and Norms in a Policy Context

V 2.0, April 26, 2004



Internet Governance Project
Syracuse University
The Convergence Center

Milton Mueller,
School of Information Studies

John Mathiason
Maxwell School of Citizenship and Public
Affairs

Lee W. McKnight
School of Information Studies

Executive Summary

This paper is intended to contribute to the United Nations Working Group process for defining Internet Governance. The paper:

- Proposes a concise definition of Internet governance
- Enumerates existing Internet governance regimes, showing where some of them intersect or overlap
- Identifies basic principles about the Internet and articulates norms derived from those principles.
- Provides a framework for the analysis of specific policy issues, and applies it to a few case studies
- Most importantly for the United Nations and other actors, it provides a structured way to come to an agreement on whether new Internet governance arrangements are needed and if so, how they should be institutionalized.

Making Sense of “Internet Governance:” Defining Principles and Norms

The World Summit on the Information Society’s request to Secretary-General Kofi Annan to convene a working group on Internet governance provides an important opportunity to clarify roles in one of the most dynamic features of 21st century society. The Working Group, has been tasked to:

- i) Develop a working definition of Internet governance;*
- ii) Identify the public policy issues that are relevant to Internet governance;*
- iii) Develop a common understanding of the respective roles and responsibilities of governments, existing intergovernmental and international organizations and other forums as well as the private sector and civil society from both developing and developed countries;*
- iv) Prepare a report on the results of this activity to be presented for consideration and appropriate action for the second phase of WSIS in Tunis in 2005.”*

This paper surveys Internet governance issues as they are emerging and provides a context for the examination that the Working Group will have to make. The paper is intended to assist the WG process in the following ways:

1. It enumerates existing Internet governance regimes and shows where they intersect or overlap.
2. Applying regime theory, it attempts to identify some of the basic principles about the Internet and to articulate norms that can be derived from those principles.
3. It provides a framework for the examination of international Internet policy issues, and identifies some of the specific issues which the dialogue on Internet governance will have to cover.

The paper has been updated to take account of the discussions at the February 2004 workshop of the International Telecommunication Union and the March 2004 Global Forum of the UN ICT Task Force.

The method we propose serves two purposes. First, it permits more precise analysis and understanding of existing Internet governance arrangements. Second, it provides a structured way to come to an agreement on whether new Internet governance arrangements are needed and if so, how they should be institutionalized.

I. Coming to Terms with the “G”-word (Governance)

The meaning of the term “Internet governance” needs to be clarified at the outset. The word “governance” seems to frighten many parties in the technical and business communities, who equate it with “government” or with the idea that “a single entity controls the Internet.”¹ In contrast, the term is routinely used among scholars and practitioners in the fields of international relations, public administration and political science, who do not find it frightening at all.² The label “governance” at the international level was developed rather recently in those fields as a response to the fact that in an increasingly interdependent world there are administrative and organizational problems that transcend the boundaries of national sovereigns.³ Governance in this context refers to the rules and procedures that states and other involved parties agree to use to order and regularize their treatment of a common issue. It does not mean the same thing as “government;” in fact, the term was chosen specifically to differentiate (weaker) international ordering processes from (more binding) national ones. Within states, there can be “government,” but in the non-sovereign worlds of international public organizations, civil society, and business organizations, there can be only “governance.”

This leads to a fairly simple, if abstract, definition of “Internet governance.” Internet governance can be defined as: *Collective action, by governments and/or the private sector operators of TCP/IP networks, to establish rules and procedures to enforce public policies and resolve disputes that involve multiple jurisdictions.*

The Internet is an international phenomenon, and determining the rules and procedures for its governance is neither simple nor obvious. But as we show in the next section, some forms of governance have already been adopted, and more may be needed if the institution is to achieve its full potential in contributing to the solution of the many problems confronting the international community. There are a variety of means by which governance can be secured, ranging from defining property rights and letting the forces of the market provide order, through action by national authorities, to responsibility for order being assigned to international public organizations. Which is most appropriate, as will be seen, depends on how the governance issues are defined.

¹ See e.g., “Issues Paper on Internet Governance,” Prepared by the International Chamber of Commerce’s Commission on E-Business, IT and Telecoms, January 2004. See also the Internet Society news release “Developing the Potential of the Internet through Coordination, not Governance,” (December 9, 2003) <http://www.isoc.org/news/7.shtml>

² The word is also used in the business world frequently now in reference to “corporate governance;” i.e., the accountability and management arrangements used to supervise corporations. Since this usage applies to a single organization and the Internet consists of thousands of interconnected organizations, it is not appropriate to think of “Internet governance” and “corporate governance” as parallel concepts.

³ The term was given particular importance by the Commission on Global Governance that issued its report *Our Global Neighborhood* (Oxford University Press, 1995).

II. Internet Governance Already Exists

Once the definition of “governance” is clarified, it becomes evident that international governance is already being applied to the Internet in several particular areas.

Specifically:

- The Internet Corporation for Assigned Names and Numbers (ICANN) sets policy for domain name dispute resolution, engages in economic and technical regulation of the domain name supply industry, and controls the allocation and assignment of top-level domains and the top of the Internet Protocol address hierarchy. Efforts to portray this as mere “technical coordination” are mistaken. ICANN’s main activity is to establish a system of rules, rooted in contracts, to order the global supply of domain names. These contractual rules are used to resolve fundamental public policy problems involving domain names and intellectual property rights, privacy, competition policy, and resource allocation. In other words, most of what ICANN does is “governance;” very little of its time and resources involve technical coordination.⁴
- The Council of Europe’s Draft Convention on Cybercrime deals with criminal offenses committed through the use of Internet and other computer networks, such as copyright infringement, computer-related fraud, child pornography, and breaches of network security. Although not confined to the Internet, it certainly encompasses “governance” of important aspects of Internet use. The Council has also adopted a Declaration on “Freedom of Communication on the Internet.”⁵
- The UN Commission on International Trade Law (UNCITRAL) has adopted a model e-commerce law and considers its purpose to “further the progressive harmonization and unification of the law of international trade,” thus paving the way for Internet-based e-commerce. Likewise, the Hague Conference on International Private Law affects consumer protection and consumer-business and business-business transactions over the Internet. Harmonization of the rules and procedures governing transnational commercial transactions over the Internet is “governance.”
- The World Intellectual Property Organization (WIPO) in December 1996 concluded two treaties updating copyright and related rights for digital media, which it promotes as “the WIPO Internet treaties.” More recently, WIPO has proposed a treaty creating new forms of protection for broadcast content that could have profound implications for webcasting and Internet multimedia transmissions. WIPO also cooperated with ICANN in the development of domain

⁴ For an extended analysis of ICANN and the policy issues associated with domain names, see Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (MIT Press, 2002).

⁵ Declaration on Freedom of Communication on the Internet and Explanatory Note. 28 May 2003. http://www.socialrights.org/spip/IMG/pdf/Freedom_of_communication_on_the_Internet.pdf

name – trademark dispute resolution policies, and in 2001 proposed the creation of entirely new domain name rights with no basis in trademark law. This is “governance.”

- The Internet’s rapid international diffusion in the 1990s would not have been possible without domestic policies and trade agreements liberalizing the provision of “value-added” information services using telecommunication facilities. These agreements preceded the WTO, but were extended and institutionalized by the WTO’s Basic Telecommunication Services agreements. The WTO also promulgated the TRIPS (Trade-related aspects of intellectual property rights) agreement, which treats copyright infringement as a trade barrier and requires WTO members to adhere to minimum standards of protection and enforcement. While not exclusively concerned with Internet-based intellectual property issues, the application of TRIPS standards could be applied to Internet-based infringers.
- International governance can also be achieved through the unilateral action of strong states. E.g., the U.S. Federal Trade Commission has proposed an “International Consumer Protection Act” focused primarily on transnational law enforcement involving Internet transactions. The U.S. also passed the “Anticybersquatting Consumer Protection Act” globalizing some aspect of U.S. legal jurisdiction over domain name disputes. Similarly, the European Commission’s competition policy reviews have had and will probably continue to have transnational impact on the Internet. For example, before clearing the merger of two U.S. companies, WorldCom and MCI, in 1998 the EU required MCI to divest its Internet service provider business. The same transnational impact characterized the EU’s Data Protection Initiative. Is this “governance” or “government?” Perhaps somewhere in between.

There have also been proposals for governance regimes that have not succeeded, such as the global content classification regime proposed by the Bertelsmann Foundation,⁶ proposals emerging from the Asia Pacific Economic Council (APEC) regarding an international settlements regime for Internet service providers, or the Council of Europe’s “right of reply” proposal to regulate web site content.⁷ Figure 1 diagrams some of the Internet-related international regimes and shows where they overlap.

The International Chamber of Commerce has prepared a more detailed matrix of issues related to the Internet and the organizations that are active in those areas.⁸

With all these localized regimes in place involving (or potentially involving) the Internet, why do we need to discuss “Internet governance” as a whole? Why not let international actors continue to respond to the problems posed by the Internet in a piecemeal fashion?

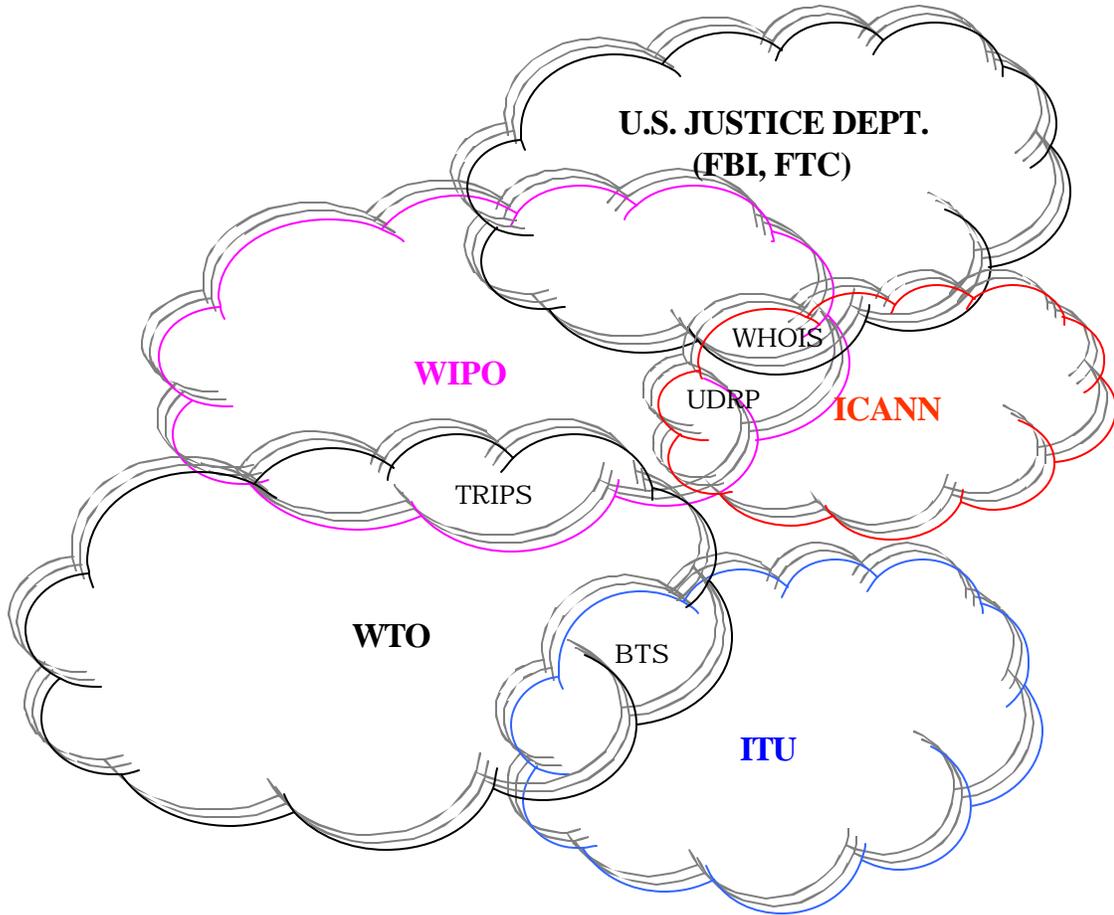
⁶ “Memorandum on Self-regulation of Internet Content,” Bertelsmann Foundation, Gutersloh, Germany, 1999

⁷ http://www.coe.int/T/E/Human_Rights/media/7_Links/Right_of_reply_hearing.asp#TopOfPage

⁸ See http://www.iccwbo.org/home/menu_electronic_business.asp

It is an important question – one that contains an implied critique of the WSIS mandate that is more legitimate and pertinent than the pretense that Internet governance doesn't or shouldn't exist as an issue at all.

Figure 1 - (Some) Internet Governance Regimes



We recognize the possibility that the concept of “Internet governance” is too big for its own good. In a digitized communication-information environment, most electronic hardware, most software applications, and practically all information services can be linked to the Internet in one way or another. Thus, “Internet governance” has the potential to encompass virtually anything and everything that involves communication and information. Top-down regimes that attempt to comprehensively “order” such a large and complex space are likely to be less responsive to unique conditions in a particular policy domain – and possibly inimical to freedom, less efficient, and less effective.

Nevertheless, three reasons can be adduced why it is worth asking, at least, about the bigger picture. First, one cannot know whether a comprehensive governance regime is better or worse than what we have now unless one tries to sum the parts into a whole and assess what, if anything, is missing or not working effectively. There is, in other words, a need for agreement on fundamental conceptions about the nature of the phenomenon the international system is dealing with. In regime theory, these agreements about basic facts are called “principles.” We elaborate on that concept in Section IV below. Secondly, localized regimes can be dictated by special interests, such as wealthy and well-organized industrial interests, powerful states, or some combination of the two. In smaller domains these special interests may have the clout to establish rules that, while congruent with their own immediate needs, are unfair or dysfunctional from a broader perspective. Third, even when the localized regimes are good on their own terms there may be overlaps, contradictions, or loopholes amongst them because they all evolved relatively independently of each other. Some of the policy issues related to these are discussed in Section V.

To conclude, a key issue for the UN Working Group is: How much unification or integration of the international governance frameworks pertaining to the Internet is needed? What are the dangers and potential benefits of a comprehensive approach?

III. Regime Theory

The Working Group will be discussing how to create an “Internet governance regime.” The classical definition of a regime is “sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors’ expectations converge in a given area of international relations.”⁹ Put another way, a regime is a set of agreements on how to create and maintain order in a given area. In terms of Internet governance, it would be the agreements made by governments, civil society and international organizations about how critical elements of the Internet should be managed so that the Internet functions effectively and in an orderly manner for the benefit of all.

In practice, regime creation follows a sequence of agreements on central issues. First, the principles, defined as statements of fact, causation and rectitude, are agreed. Without an agreement about the nature of the problem or issue, no subsequent agreement can be

⁹ Steven D. Krasner, “Structural Causes and Regime Consequences: Regimes as Intervening Variables,” in Krasner (ed), *International Regimes*, Ithaca: Cornell University Press, 1983, p. 2.

reached on what to do about it. Then, there must be an agreement about the norms that apply. These are the standards and obligations that the parties to a regime agree should be followed. Once the norms are agreed, rules can be defined. These are prescriptions and proscriptions for action. As a final step, once the rules are agreed, the decision-making procedures and the institutions through which they are made can be agreed.

The UN ICT Task Force devoted a session to the discussion of principles in its March 2004 Global Forum. The discussion took two forms. First, many in the Internet technical community and the business community repeatedly called upon the UN process to “first, do no harm.” In addition to that, there were calls for “transparency,” “accountability” and “participation.” All of these were put forward as “principles.”

It would be more accurate to call these contributions *norms* rather than principles. That is because they describe desirable results but tell us nothing about how to accomplish those results or what other desirable goals we have to give up to achieve them. Unless normative appeals such as these are connected to fundamental statements of fact and causation about the Internet and the constraints governing its effective operation, they are just expressions of desired outcomes, like asking for fine weather and bumper crops. As such, they offer the UN Working Group little substantive guidance. It is unlikely that anyone, for example, could disagree with an aphorism such as “first, do no harm” It would be easy to obtain consensus that any new international governance arrangements should not make things worse than they are now. The real political accomplishments, however, will come when the involved community can come to an agreement about what constitutes “harm” and what actions make things “worse” or “better.” A true *principle* would make a concrete and meaningful statement about that, and thus would help guide toward better governance arrangements. That is why this paper uses a more restrictive and “academic” definition of the term “principle.” It is the only approach that will lead to any results.

The speed with which a regime can be set up depends on how long it takes to agree on each of the steps. Sometimes the first stage, agreeing on the facts and their implications, is easy, but more often it is the most difficult stage. For example, the agreement on the factual principle that human behavior could alter the global climate was critical to further agreements on the climate change regime. In the case of the Internet, a key agreement will have to be reached about what the Internet is and its logical consequences.

All international agreements include statements of what should be expected of the parties involved. In the case of the Internet, these standards of behavior and obligations will have to apply to all of the actors: corporations and other businesses, epistemic communities, governments at all levels, and international organizations. They will define the contours of governance. As our analysis will show, there are many unresolved normative issues with regard to the Internet, but these can and should be resolved.

Agreement on rules, decision-making procedures and institutions is inevitably the last step in negotiating a regime. Partly this is because this step involves what are termed “financial implications” for the parties to the regime. Mostly, however, it reflects the fact

that the rules, procedures and institutions have to be appropriate in terms of both principles and norms. To a large extent, the agreement on principles and norms will determine what rules, procedures and institutions will be needed.

IV. Principles for the Global Internet

In this section we begin the process of articulating basic principles upon which an Internet governance regime can be based. This particular set of principles should be considered provisional; its intent is to provide a basis for beginning the discussions and negotiations of the Working Group. The normative implications of each principle will be articulated in the next section.

A. The Global Commons Principle

The Internet is based on global, open and nonproprietary standards. The networking protocols upon which it is based can be freely adopted by anyone. They are published openly and can be used by anyone without paying a fee. Its core standards and practices are developed by a relatively open epistemic community, which while spearheaded by formal hierarchies such as Internet Architecture Board, IETF and W3C, really consists of a broad and informal conglomeration of technical experts located in universities, research institutes, small consultancies, large corporations and governments. This is in contrast to the older model of standardization, in which standards documents were developed by formally appointed representatives working in closed committees, and often sold as very expensive documents.

B. The Private Market Principle

The Internet is a decentralized network of networks. The networks connected by Internet protocols are owned and administered by autonomous organizations: the private networks of households, small businesses, large enterprises and nonprofit organizations as well as the (usually privately owned) public data networks, both large and small, of Internet Service Providers and telecommunication companies. This aspect of the Internet leads to privatization and decentralization of network operations and policies. By facilitating interoperability, Internet leads to privatization and decentralization of software applications and information content as well.

The private market principle has important infrastructural implications. As a software protocol, Internet can run on any available physical telecommunication infrastructure: wired or wireless, copper, fiber or coax. The Internet can aggregate large numbers of relatively small private investments in physical telecom infrastructure into an interconnected whole. Most of the investment is small scale and private.

This principle also means that the Internet's capacity for self-governance is great. Private networks or users can build electronic "fences" or adopt filters or practices that can, to some extent, shelter themselves from undesirable forms of communication while

maintaining some form of compatibility and interconnection with the rest of the world. Whereas traditional notions of government and governance imply uniformity, Internet permits variation in policies adopted in response to the same problem.

C. The End-to-End Principle

The Internet was designed to follow, as much as possible, the “end to end argument,” which is one of its few general architectural principles. End-to-end means that the design of the network is not optimized for any particular service or set of applications; the network provides basic data transport only, leaving applications and other forms of user-specific information processing to the devices attached to the ends of the network.¹⁰ This permits the network to serve as a relatively neutral and transparent platform for the widest possible variety of applications and services, including services that have not been anticipated by the designers. The end-to-end principle is believed to promote innovation, network growth and market competition, and a more rational, direct allocation of costs. When functions and applications are built into the network they have to be shared by everyone, regardless of whether they use them. Under an end-to-end regime, on the other hand, the users of new services and applications pay most of the additional costs associated with them, because most of the implementation costs of specific services and applications are borne by people at the endpoints.

Although we present commons, market and end-to-end as three distinct principles, it would be better to think of them as interrelated. At the endpoints, the free market and privatization rule; at the core standards level, a commons is in place. The end-to-end principle ensures that commons and market complement each other. The market in applications, content and networking requires neutral coordinating mechanisms that enable interoperation. With end-to-end, the sharing and coordinating mechanisms are deliberately minimized to provide maximum scope for initiative and innovation, and there is a clear separation between the parts of the system that are subject to private initiative and control, and the parts that are subject to global coordination and non exclusive access.

D. Resource bottlenecks exist – and are getting worse as scale grows

The Internet standards, while open and nonproprietary, create resource spaces that cannot be governed as a commons. As the scale of the Internet increases and society’s dependence on it grow, the value and stakes associated with assignment and control of these resources increases. Assignment and use of these resources must be exclusive and coordinated. We refer here to responsibility for DNS root servers, the assignment of top-

¹⁰ Certain functions “can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system. Therefore, providing [such] function[s] completely] as a feature of the communication system itself is not possible. J. Saltzer, D. Reed and D. Clark: “End-to-end arguments in system design”, *ACM Transactions on Computer Systems*, 2(4):277-88, Nov. 1984

level domain names, IP address allocation and assignment, and ISP routing tables. Control of these resources is concentrated, predictably enough, in the hands of the technologists and companies that developed the Internet first. There are legitimate grounds to investigate the technical, economic, and political impact of this legacy control. Some of the most difficult equity and distributional issues in Internet governance can be traced to this principle. These resource bottlenecks serve as a magnet for political intervention, much of which has the potential to be destructive.

E. Moral Neutrality

To those with the means to access it, Internet increases the transparency, speed and accessibility of information content and services. But this enabling power applies to “bad” as well as “good” information and communication behavior. The same properties of the Internet that empower users to interconnect and interoperate create opportunities for criminal behavior, theft, fraud, and misappropriation. The low cost of acquiring new accounts and new identities, the ease with which any infrastructure can be used to access the Internet, the delegation of significant amounts of control to the edges, means not only that all of societies’ traditional problems (e.g., obscenity, terrorism) come in to the online world, but that new difficulties uniquely responding to the opportunities of cyberspace (spam, phishing, denial of service attacks, viruses) are created as well.

F. Multi-stakeholder governance.

The organizations with control of key Internet resources are highly distributed and multifarious and cannot be regulated in a top-down manner via agreements among states alone. Overlapping communities of technologists, educational and research institutions, private corporations, and civil society organizations constitute an informal and diverse “Internet community.” Standards organizations affecting networking in particular are diverse and rely primarily on voluntary adoption. Moreover, information technology may empower companies and individuals to opt out of undesirable, burdensome or economically unsustainable institutional arrangements and to re-associate on new terms. There is always the possibility of system bypass; on the whole this is a healthy aspect of the world economy. This key constraint on international governance must be recognized and taken into account.

V. Norms for the Global Internet

The standards and obligations for parties that flow from these principles can be deduced as follows.

A. The technical model should be preserved

A future Internet regime must not interfere with the basic technical principles of the Internet (standards commons; decentralized responsibility for networks, content and services; end-to-end architecture). The basic model is not broken; in fact, it has an unparalleled record of success in facilitating communication, public access to

information, adaptation to changing conditions, and making efficient use of available infrastructure.

B. Do not allow the commons to be privatized

Ownership of infrastructure, software or services should not become concentrated in the hands of commercial providers to the point that it threatens the open, nonproprietary status of the core Internet standards. Global competition policy initiatives should be guided by this norm.

C. Do not transform the standards commons into a basis for regulating the private market.

This may be less of a threat in the short term, but it is equally dangerous. Maintenance of standards can become an excuse to engage in extensive regulation of business conduct. Overzealous applications of the end-to-end-principle may become an excuse to regulate conduct at the edges. At its worst, such regulation can change the essential character of the Internet from an association that adds value to all who are connected, to a compulsory compact that binds users in dysfunctional or suboptimal relationships. While action should be taken to prevent privatization of the Internet networking process and standards themselves, the freedom of subsets of users to “secede” from the Internet’s network federation in order to implement new technologies and new, possibly even incompatible standards should not be limited, so long as it does not technically harm the existing public Internet. Concepts of “harm” should not include so-called “economic harm” caused by end users adopting more efficient forms of communication.

The inherent tension between norms b) and c) are currently being faced in ICANN’s encounter with VeriSign’s Sitefinder initiative. This is an area where analysis yielding more precise definitions and criteria for intervention/nonintervention are needed.

D. Resource allocation and assignment rules and procedures should be consistent with the end to end principle

Insofar as is possible, resource assignment procedures should be uniform, objective, and impersonal, and facilitate the coordination of decentralized private activity at the endpoints. Discretionary, politicized merit assignment regimes are bad; objective mechanisms such as auctions or random selection are as a rule better, because they are more predictable, avoid costly investments in rent-seeking, and are more open to newcomers such as newly developing economies and smaller entrepreneurs. For an example of the application of this norm to domain name policy, see Mueller and McKnight (2003).¹¹

¹¹ M. Mueller and L. McKnight, “The Post-Com Internet: Toward Regular and Objective Procedures for Internet Governance.” *Telecommunications Policy* (forthcoming). <http://dcc.syr.edu/miscarticles/NewTLDs2-MM-LM.pdf>

- E. Management of technical resources should not be overloaded with policy functions.

This norm is intended to counter the growing temptation to use control of exclusive resources critical to the functioning of the Internet to exert leverage over areas of policy unrelated to the function of the resource itself. For example, the attempt by intellectual property owners and some law enforcement agencies to turn domain name registration data into a completely accurate form of public identification would convert a technical function into a law-enforcement function. The temptation by governments and other entities to grab on to any point of leverage must be resisted.

- F. Regulation of the fraudulent and criminal aspects of Internet use must be directed at the responsible endpoints, not at the internetworking process itself

The idea that the content of Internet communication should be regulated through controls within the channel itself rather than sanctions on the sender or receiver should be resisted. Not only is it technically difficult to monitor communications over the Net, but efforts may make the functioning of the Net less effective or impose major externalities on innocent parties. There is an analogy with other efforts to deal with illicit activities where, as in the case of drug trafficking, the best approach is to address supply or demand rather than trying to interdict transportation.

- G. Infrastructure development should be decentralized and competitive

Digital divide subsidies, if there are to be any, should go to users and not centralized suppliers or governments. For most users, the main costs of the Internet are in terms of the equipment and software necessary to connect with the network (terminal equipment, access lines, access charges) rather than the costs of using the public network itself. The experience to date shows that competition among suppliers of that equipment and software has served to stimulate investment and growth, and reduce prices. Providing resources to end users, particularly in developing countries, to acquire those elements of end user infrastructure should serve to stimulate and encourage development while maintaining a maximum degree of choice and diversity in supply.

- H. Multi-stakeholder governance should be encouraged, maintained, strengthened

More than most aspects of international life, the Internet involves governments, private business, civil society and international organizations alike. None of them, individually, can assure good governance of the Internet. As a result, governance institutions should be structured to involve all three parties based on their specific role in the aspects over which governance is sought. The rhetoric of tripartite representation is not enough, however; we must pay close attention to the details of representational structures and make sure that end users and individuals are adequately empowered. For example, many of the main application software products that power use of the Internet have been

developed by private corporations with input from users – sometimes well-organized. The main parties to governance of this element should be those who produce and use the technology.

VI. Policy Issues in Internet Governance: A Framework

The political context for these principles and norms is reflected in a set of policy issues that have been suggested as requiring some form of Internet governance. Almost all are connected with the end-to-end principle but should be seen in terms of the norms that we have suggested. As the long list of existing Internet governance regimes above showed, there are now many issues: spam, domain name trademark conflicts, law enforcement surveillance activities, DNS root server system management, intellectual property, trade and security. As a start, some kind of classification scheme might be more useful than promulgating a long list of isolated and transitory “issues.”

A. Policy Domains

We begin by identifying a set of policy domains, that is, areas where there is a common type of policy problem. In each of these domains, there is a recognizable type of activity that is the (actual or potential) subject of governance, and the various principles and norms used by national governments and international regimes to approach that type of a problem are understood. Such a list, which looks very much like a list of communication-information policy issues in a national/domestic polity, might look something like this:

1. Content regulation and Culture.
2. Data Protection, Privacy, and Surveillance.
3. Intellectual Property Protection and Fair Use
4. Trade and E-commerce
5. Competition Policy
6. Security and Survivability of Public Infrastructure
7. Subsidies and Wealth Redistribution

Of course, policy issues don't fit into neat boxes. How the international system handles privacy rights on the Internet, law enforcement, and intellectual property have become closely interrelated. In domain name policy, all three of those areas have been linked to resource assignment rules and procedures, as we will see in our analysis of the Whois issue. Likewise, in our treatment of gTLD addition policy issue, we will see how a problem in global resource assignment can raise issues in competition policy, content regulation, and IPR. But while issues are not isomorphic to categories, a framework at

least clarifies the common *types* of problems that are raised by any given Internet-related policy issue.

B. Meta-Areas of international concern:

There is another way of bundling or categorizing the issues. Regardless of the specific topic of the policy issue, one can look at why and how it creates a problem for an international system based on sovereign, territorial states. Thus, a meta-classification scheme can be defined based on three broad categories: how to apply national jurisdiction to activities that are global or cross-jurisdictional in scope; how to facilitate transnational law enforcement activities; and how to manage and interoperate technical infrastructure and resources that are global in scope. Each of the different policy domains listed above can each create one or more of these types of problems:

1. Jurisdiction application

For Internet users and suppliers, a great deal of ambiguity still exists about what particular national law might be applied to them. A content regulation issue, such as the France vs. Yahoo case on Nazi memorabilia, can raise important questions about how territorial laws are applied to multinational publishing of Internet content. The same is true of an Intellectual Property/Fair Use policy issue such as KaZaa. The Hague Convention on Private Law fits here, as does an analysis of the impact of the EU data protection law on other jurisdictions.

2. Law enforcement harmonization and cooperation

Even in cases when there is no ambiguity about *which* national law or international treaty will be applied, in order to actually enforce it law enforcement activities may need to broaden their scope via transnational cooperation regarding identification, surveillance or law enforcement interoperability agreements (extradition, dual criminality, etc.). Law enforcement cooperation can span any number of policy domains; for example the Cybercrime treaty deals with security and survivability by criminalizing certain kinds of hacking; and it affects content regulation through its approach to child pornography.

3. Global Resource Management

This refers to the need for coordinated sharing, and/or exclusive assignment, of transnational resources related to communication and information, such as radio spectrum, satellite orbital slots, top-level domain names, IP addresses, and telephone numbering. When such management is best handled at the global level, international agreements might be needed, although it is always an open question whether these agreements should come from governments or from specialized self-regulatory

arrangements in the private sector (e.g., Ethernet address assignment or root server operation).

Thus, as a first cut for the identification of policy issues, we suggest 1) asking what type of international coordination problem it poses (one of jurisdiction, law enforcement, or global resource management); and 2) mapping the issue to a policy domain, to clarify the principles, norms and regulatory techniques that might apply.

VII. Analysis of Specific Policy Issues

We turn now to a short analysis of four distinct policy issues in Internet governance that illustrate the problems that have to be addressed by governance. After describing the issues, we raise the question whether these issues should be handled via a localized governance regime or more comprehensive arrangements. Our intention is to raise that question, not answer it definitively. We use the cases mainly as examples of the kind of decisions an Internet governance regime would have to face, and while we have opinions about the answers that may be evident from the discussion, our main purpose is really to foster discussion.

Two out of the four specific policy issues discussed will be focused on ICANN-related issues. This is not because we think that ICANN is the only or the most important aspect of Internet governance, it is simply what we know the most about.

A. ICANN and the WHOIS database

The Whois protocol and directory are components of the Internet's domain name system (DNS) and its Internet Protocol address assignment registry. We will confine our attention in this discussion to DNS. Whois contains information about registrants of domain names and their name servers. In addition to the personal identity of the registrant, Whois contains extensive contact information, such as street address, telephone number, email address, and fax number. This information is available to anyone on the Internet who knows the domain name. The information for an entire set of registrants can also be purchased in bulk from domain name registration companies, according to rules and prices set by ICANN.

Created back in the days when the Internet was a closed network restricted to a few researchers and U.S. government contractors, the Whois protocol's original purpose was simply to provide technologists running an experimental data communications network with the off-network contact information they needed to notify each other when breakdowns and problems occurred. But when the rise of the World Wide Web after 1993 made domain names into valuable property, Whois was transformed. Trademark owners concerned about cyber-squatting found it to be an indispensable means of acquiring the information they wanted to issue legal challenges (or in U.S. legal community terminology, "serve process") to domain name registrants. The influence of

the IPR lobby pushed ICANN into adopting strict requirements to make Whois contact data complete and accurate, and require registrars to sell that data (basically, their customer lists) in bulk to any information service or IPR holder that wants it, as long as they do not use it for “marketing purposes.” In short, Whois was transformed into a surveillance tool for law enforcement agencies (LEAs) and IPR holders.

Whois gives anyone in the world access to personal contact data in an indiscriminate, anonymous fashion, without need for any due process. Although you can do as much mischief with a telephone number as with a domain name, most countries do not require telephone companies to allow anyone in the world to type in your telephone number and see your name and home address, who your service provider is, etc. Because Whois capabilities emerged via a historical accident, however, and LEAs and IPR holders moved quickly to institutionalize these functionalities, established privacy and due process norms were bypassed. The mainly U.S.-based IPR interests have used their privileged access to US lawmakers (and in turn U.S. lawmakers’ somewhat privileged role over ICANN) to push for harsh criminal penalties to make the Whois data accurate. These parties do not agree with the common argument that many registrants enter inaccurate data elements precisely because the information is exposed to anyone and everyone.

This unanticipated use of the Whois directory has created some benefits, it can be argued. Quite apart from the systematic exploitation of the Whois by IPRs and LEAs, many individual Internet users have come to appreciate being able to easily look up who or what is behind an Internet email address or web site; that function in some cases facilitates greater accountability on the net. But the availability of the information also causes problems. The information in the directory can be harvested by spammers. Registrars’ Whois servers are pounded by scripted queries of data miners. Identity theft and stalking are facilitated. If larger and larger numbers of people acquire domain names and use them to participate on the Internet, one must ask whether they deserve the same levels of privacy enjoyed by users of the telephone or owners of license plates on automobiles. More fundamentally, the indiscriminate access to personal contact data violates established international norms regarding data protection.¹²

European registrars have voiced concerns about the applicability of the European Data Protection Directive, and are wondering whether they might be legally liable if they conform to ICANN’s policies. Some countries have laws that require commercial entities with web sites to publish specific contact information about themselves on the website; e.g., the German “Impressum” laws. Although these types of laws are often cited as a factor in support of ICANN’s Whois policies, it proves just the opposite. If national laws can meet the needs of LEAs and consumer protection authorities with regulations requiring display of data, then there is no need for the Whois database to do it. In short, Whois brings international data protection/privacy principles and norms into conflict with ICANN’s contracts governing domain name registration.

¹² See the presentation of George Papapavlou, European Union, before the ICANN Rome meeting, March 3, 2004. <http://icann.org/presentations/papapavlou-whois-rome-03mar04.pdf>

ICANN is now revisiting its Whois policies in a systematic way. But is ICANN the right place to resolve this issue? One can argue for either answer to this question, but anyone concerned with the consistency and fairness of Internet governance cannot fail to agree that it is an argument we need to have. Despite repeated efforts by privacy advocates to raise this issue within ICANN, for three years the ICANN regime has successfully fended off any attempts to consider the privacy issues inherent in the collection and publication of personal names and contact data.

In general, ICANN is dominated by IPR interests. Representation in the GNSO, its main policy development organ for domain names, is skewed such that business and IPR interests completely control 3 of the 6 constituencies, and registrars and registries control another two. There is no real representation within the system for individual domain name registrants and only one constituency for noncommercial users' interests. Within ICANN's Governmental Advisory Committee (GAC), national data protection authorities are not well represented relative to other governmental interests, such as commerce and law enforcement. In short, the ICANN regime is likely to generate a great deal of solicitude for those who want access and use the WHOIS data; those who are being subject to surveillance are pretty much left out of the discussion.

This case was chosen to illustrate how an Internet public policy issue can be situated at the intersection of multiple policy domains, but when responsibility for the issue is under the aegis of one particular localized international regime (in this instance, ICANN) it may bias the policy making process in a certain direction. In this case, a broader, more global perspective on the issue might result in a better outcome.

B. IPR - Music downloading

The issue of large-scale exchange of digitized music files over the Internet also illustrates some of the problems for the various regimes that intersect. The corporate recording industry, through its associations in different parts of the world (RIAA in the United States), has tried to deter file sharing of copyrighted music by seeking civil and criminal penalties for individuals that they believe have been distributing music. They have also sought to compel Internet service providers to divulge the names of their customers, and to bring the developers of sharing software (like Kazaa) into court. They have also tried to prosecute programmers who have developed sharing or code-breaking software. The basis for these actions is found in intellectual property law. Counter-arguments are based on the "fair use" principle that is derived from both human rights and copyright law, and in common carrier law that absolves mere transporters of data from responsibility for illegal activities of its users. The matter has been complicated by the fact that some of the questioned servers are off-shore or in different countries (Kazaa's home corporation is chartered in Australia and its server is now off-shore as well). If it were just a matter of transnational law enforcement, the solution might be relatively simple. There is, however, no international consensus about what "fair use" means in an Internet context, nor about the degree to which Internet service providers can be required to assist in, or held responsible for, law enforcement. Moreover, the economic effects, positive or negative, of large-scale file sharing, whether done using proprietary software (like Apple's iTunes)

or open system methods, are still in dispute. Here again, once could make a case for a broader international dialogue about what norms and rules we want to apply in this case. IPR enforcement will be more reasonably bounded, and more widely accepted as legitimate, if its standards emerge through such a dialogue.

C. gTLD addition

The economic asset that keeps the ICANN regime afloat is its policy authority over the DNS root zone file. This gives ICANN the authority to decide which new generic top-level domains (gTLDs) will be created. GTLDs are potentially valuable resources; each top-level domain creates a new name space within which second-level domain name registration services can be registered. In terms of our classification scheme, gTLD addition is an international issue because it involves a need for globally exclusive resource assignment. In terms of policy domains, adding new top-level domain names can be connected to content regulation issues (should certain types of content be “forced” into certain domains? should obscene domain names be permitted?), competition policy issues (do new TLDs create competition? should new TLDs be awarded to incumbents? should there be a vertical separation between registrars and registries?), and IPR issues (what kind of rights to names should be created or recognized within a TLD?).

The market for gTLD registry services is highly concentrated; US company VeriSign controls about 85% of the market due to its ownership of the ICANN contract to operate the .com and .net domains. A company closely affiliated with the ICANN regime, Afilias, Inc., controls about 10% of the remainder due to its contract to run the .info and .org gTLDs. The rest is controlled by Neustar and a few other tiny players.

There has been tremendous controversy over how gTLD resources are assigned. The controversies began in 1995; at that time 100% of the gTLD market was controlled by one company (VeriSign’s predecessor, Network Solutions, Inc.) and the Internet community was calling for hundreds of new TLD names and operators. That budding market was squashed, however, by debates over who had the authority to add TLDs and later by the concerns of trademark holders.

In principle, the ICANN regime possesses all the right ingredients to handle this issue well. It has close relationships to the Internet technical community and domain name registrars and registries, and makes some efforts to include domain name registrants in its policy formulation processes. Unfortunately it has botched the job. It has fostered artificial scarcity and kept the industry highly concentrated. Asked to provide “technical coordination” of the root zone file, somehow ICANN set itself up as arbiter of what TLDs sounded good and which didn’t, which TLDs had adequate customer demand and which didn’t (a guessing game it proved to be horribly bad at), and what business policies should be followed by applicants. ICANN’s own board chair compared the TLD selection process to the vetting process of a venture capital firm. And of course, ICANN bent over backwards to ensure that user demand for new TLDs was subordinate to trademark interests, forcing registries to institute complicated and costly “sunrise”

procedures to give trademark owners special claims. Thus, instead of setting up impartial and regular procedures for TLD additions that would allow anyone to play, such as auctions, random selection or fee-based application processes, it turned TLD additions into a politicized, expensive, unpredictable and discretionary process. After nearly six years of existence, ICANN still has no defined process for adding TLDs.

It seems clear that ICANN's *ad hoc* approach to TLD resource assignment has discriminated against entrepreneurs and applicants not well connected to ICANN or the Internet Society, especially those outside the US and Western Europe. Advocates of multilingual domain names were not given a chance, and applicants from newly-industrialized countries were thwarted by deeply complex legal requirements and the need for intricate U.S.-based political lobbying of ICANN staff and Board members. Of course, contention for TLD resources was exacerbated by the incredibly narrow – and completely arbitrary – supply restrictions placed on name space expansion by ICANN.

In this case, a more internationalized Internet governance process might be used to pressure ICANN to adopt more reasonable and inclusive TLD addition policies and procedures, while leaving the localized regime in place.

D. Spam

Spam represents a kind of Internet use that most email recipients find abusive, and which imposes major costs on the infrastructure. The UN ICT Task Force's Global Forum identified spam as a highly suitable topic for Internet governance, because it is a problem that is unique to the Internet, universally reviled, and trans-jurisdictional in scope. Many nations and sub-national governmental units such as states and provinces have already passed laws against various aspects of spamming. However, the sources of spam may not reside in the territory to which the law applies, or the problem of identifying and tracing the spammers may require international cooperation. Thus, in terms of our policy issue identification framework, it is primarily a coordinated law enforcement issue. The OECD has initiated discussions of spam that seem to be following this path.

While spam is usually approached as an issue of nuisance regulation or privacy, it is also a content regulation issue. Effective control of spam must distinguish between commercial and noncommercial communication, and make sure that regulations do not interfere with the basic right to communicate.

Spam can also be approached as an infrastructure management issue. If governments and international organizations possessed the consensus and political will to attempt strong interventions in the way Internet service providers function, they could attempt to rewrite protocols and implement authentication procedures that would facilitate spam control. Approaching spam as a technical issue, however, probably would lead to a far more intrusive policy with many more unintended consequences imposed upon innocent or borderline uses and users. Moreover, there are a variety of private, market based technical responses that may yet prove to be the best way to approach spam. The growing market for software that filters spam is one example. Better authentication protocols and

technologies might also have a major impact. Some of the more radical proposals involve economic and institutional arrangements that involve charges for the receipt of unwanted emails.¹³ Those theoretical solutions, however, sometimes presuppose the existence of reliable global identification and accounting mechanisms that do not yet exist. The point is that in the spam case, as in many other Internet policy issues, “governance” solutions must be assessed against the dynamically changing alternatives posed by the technology itself. The UN process must guard against the assumption that any problem encountered on the Internet requires a solution that involves global governance.

VIII. Conclusion

This paper is intended to contribute to the dialogue surrounding the UN Working Group on Internet governance. It has proposed a definition of Internet governance and enumerated existing localized Internet governance regimes, showing the complex, overlapping relationships that exist among them. The paper provides a broad framework for pursuing the global dialogue on governance: a regime-theoretic framework that first identifies principles about the Internet and then derives norms from those principles. Once principles and norms are agreed, the next step is to develop rules and procedures that can implement the norms on a global basis. That aspect of the project will be taken up in the next paper in this series. The articulation of principles and norms in this paper is meant to be a first step; undoubtedly we have overlooked relevant items and we accept the inevitability and desirability of debate and discussion of the principles and norms we have proposed.

This paper has shown that Internet governance is already taking place in a variety of localized international regimes, each driven by a distinct politics. While any sweeping global governance regime for the Internet simultaneously raises dangers of intrusive overcentralization and irrelevance, we think that the problems, loopholes, and unsavory politics associated with certain aspects of the existing evolution of governance makes it worthwhile to take a more comprehensive look at the system as a whole.

The paper also created a framework for the identification of public policy issues associated with Internet governance, and looked in greater detail at four specific areas of policy. That survey and examination supported the argument that some kind of broader dialogue about Internet governance at the global level is needed. The concept of “governance” in this regard need not be synonymous with “more intrusive governmental regulation;” it might also mean more just and efficient policies in those areas where current regimes are failing.

¹³ T. Lorder, M. Van Alstyne and R. Wash, “Information Asymmetry and Thwarting Spam,” University of Michigan working paper, See also R. Wetzels, “Spam-fighting Business Models – Who wins, who loses?” *Business Communications Review* 34, 4 (April 2004) 24-29.