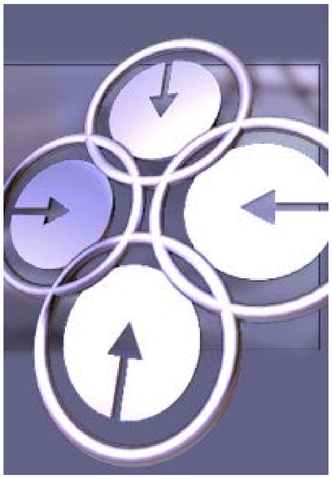
Making Sense of "Internet Governance:"

Identifying Public Policy Issues



Internet Governance Project
Syracuse University
The Convergence Center

Milton Mueller,
School of Information Studies

John Mathiason
Maxwell School of Public Administration

Lee McKnight
School of Information Studies

Making Sense of “Internet Governance:” Identifying Public Policy Issues

The official Declaration and Action Plan of the World Summit on the Information authorized the UN Secretary-General to convene a working group on Internet governance. The Working Group, once established, 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.”*

No other aspect of the WSIS second phase has generated the same level of interest and activity as this task, and at this point it seems unlikely that any other WSIS-related activity will. But that is all right. As a topic, “Internet governance” is almost as broad in scope as the “Information Society.” Like one of those Russian nested toys, we have opened the WSIS Phase 1 egg to find inside an Internet governance egg; and as I will argue in this paper, when we open up the “Internet Governance egg” we find a mini-WSIS nestled inside.

I have been asked to address the second item in the WG’s charge: identifying public policy issues that are relevant to Internet governance. This paper goes about that in the following way. First, it enumerates existing Internet governance regimes (yes, there already are lots of them), showing what kind of policy issues they address and where they intersect or overlap. This exercise quickly leads to the discovery that Internet governance raises so many policy issues that it is impossible to identify and discuss all of them in any detail (and besides, any such list might be obsolete in a few months). Instead, we outline a conceptual framework for categorizing the policy issues. We then examine four specific policy issues in more depth: 1) the privacy issue as it is being played out in the context of ICANN and the Whois protocol for domain names, 2) music downloading, 3) top-level domains and 4) spam.

This paper is derived from a larger and more comprehensive paper that will be presented at the UN ICT Task Force's Global Forum in NYC next month. That paper's modest goal is to do most of the WG's work for it by sketching the elements of an Internet governance regime. Using a regime theory framework, it will identify some of the basic principles about the Internet and articulate norms that can be derived from those principles. The method we propose in that paper permits more a precise discussion of existing Internet governance arrangements, and 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 term "Internet governance" needs to be clarified at the outset, especially the meaning of "governance." The word 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, political science, and management who do not find it scary 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."

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.

- 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

[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).

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.

- 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."[4]

- 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" in anyone's book.

- 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 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.

[4] 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

- 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,[5] 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.[6]

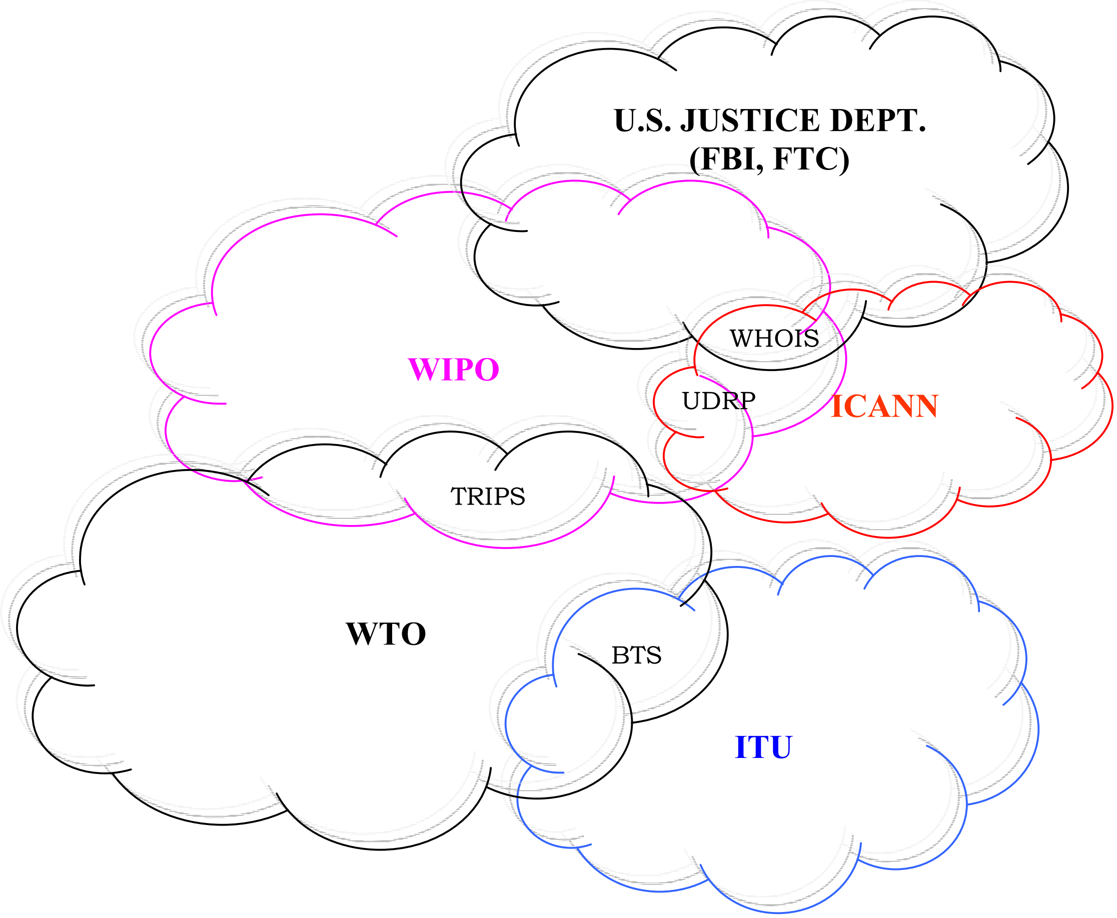
Figure 1 diagrams some of the Internet-related international regimes, both real and proposed, and shows where they overlap.

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

[5] "Memorandum on Self-regulation of Internet Content," Bertelsmann Foundation, Gutersloh, Germany, 1999

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

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. Such overarching regimes face the twin dangers of being so broad and general as to be ineffective; or, if efforts are taken to make them effective, becoming inimical to freedom, diversity and efficiency.

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 our larger paper.) 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.

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. Policy Issues in Internet Governance: A Framework

Now let us turn to the identification of "policy issues." As the long list of existing Internet governance regimes above showed, there are lots of them: spam, domain name trademark conflicts, law enforcement surveillance activities, DNS root server system management, content issues, etc. As a start, some kind of classification scheme might be more useful than promulgating a long list of isolated and transitory "issues."

1) 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:

a) Content regulation and Culture

b) Data Protection, Privacy, and Surveillance

c) Intellectual Property Protection and Fair Use

d) Trade and E-commerce

e) Competition Policy

f) Security and Survivability of Public Infrastructure

g) 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 the domain name space expansion 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.

2) 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:

a) 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.

b) 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.

c) 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 DNS 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.

IV. Analysis of Specific Policy Issues

We turn now to a short analysis of four distinct policy issues in Internet 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 down 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 have moved quickly to institutionalize its new 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 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.

European domain name 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, their existence actually points in exactly the opposite direction. 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.

Even as we speak, ICANN is revisiting its Whois policies.[7] But is ICANN the right place to resolve this issue? One can argue for a "yes" or a "no" 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/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; but those who are being subject to surveillance are pretty much left out of the discussion.

[7] See http://gnso.icann.org/issues/whois-privacy/

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. The counter-argument is based on the "fair use" principle that is derived from human rights law. Internet service providers who consider themselves innocent third parties invoke some variant of what is called "common carrier" principles in the Anglo-American world. The conflict of principles 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 how (and with whom) intellectual property law can be interpreted and enforced, or override the immunities of common carriage. 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, in contrast to the Whois issue, we do not have a localized, settled regime that is biased, but no regime at all. One could, therefore, 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 sold. 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 (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 precedessor, 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 (the Internet root at that time was still run informally by technologist Jon Postel) 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 effort 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.[8] 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

[8] For a more detailed analysis of this issue, see the paper by Mueller and 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

which didn’t (a guessing game it proved to be horribly bad at), and what business policies should be followed by applicants. 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. Worst of all, 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 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. 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.[9]

Spam could 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. Approaching spam as a technical issue, however, probably would lead to a far more intrusive policy with many more unintended consequences and externalities 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,[10] although those solutions seem to presuppose the existence of reliable global

[9] OECD Workshop on Spam, Brussels, Belgium, Feb. 2-3, 2004. http://www.oecd.org/document/0/0,2340,en_2649_33703_21648384_1_1_1_1,00.html

[10] T. Loder, M. Van Alstyne and R. Wash, "Information Asymmetry and Thwarting Spam," working paper, January 2004, University of Michigan. Request copy of paper from mvanalst@umich.edu .

identification and accounting mechanisms that do not yet exist, and if they existed, might be used to eliminate spam anyway. 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.

V. Conclusion

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 over-centralization and diffuse 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.