Internet Governance: The State of Play

The Internet Governance Project[1]
(www.InternetGovernance.org)

September 9, 2004

The **Internet Governance Project** is a partnership of the Convergence Center, Syracuse University School of Information Studies, the Moynihan Institute of Global Affairs of the Maxwell School of Syracuse University and the Internet and Public Policy Project (IP3), Georgia Institute of Technology.

The principal investigators for this paper are John Mathiason (team leader), Milton Mueller, Hans Klein, Marc Holitscher and Lee McKnight.

[1] The Internet Governance Project (IGP) is an interdisciplinary consortium of academics at Syracuse University, Georgia Institute of Technology, and Institut für Politikwissenschaft der Universität Zürich. The principal investigators for this paper are John Mathiason (team leader), Milton Mueller, Hans Klein, Marc Holitscher and Lee McKnight. See http://www.InternetGovernance.org

Internet Governance: The State of Play

Table of Contents

ICANN (Nonstate/Formal)

RIRs (NonState/Formal) and NRO (NonState/Informal)

Root Server Operators (Mostly Non-state/Informal)

ITU-T (State/Universal)

ccTLD Associations (nonState/Formal)

Policy Function, 22

ITU (State/Universal)

WIPO (State/Universal)

UN-OHCR (State/Universal)

UNESCO (State/Universal)

WTO (State/Universal)

UNCITRAL (State/Universal)

UN-ODC (State/Universal)

EU (State/Nonuniversal)

Council of Europe (State/Non-universal)

OECD (State/Non-universal)

G8 (State/Non-universal)

Hague Conference (State/Non-universal)

ASEAN (State/Nonuniversal)

APEC (State/Non-universal)

ICANN NonState/Formal)

ICRA (NonState/Formal)

ASTA (NonState/Informal)

Recommendations, 31

- Decide on the relevant statements of fact
- Decide on norms:
  - Come to terms with the global, non-territorial status of the Internet
  - Come to terms with the end-to-end principle
- Define, guarantee and protect the roles of the various stakeholders in the Internet
- Find a foundation of legitimacy for non-state actors in governance

Introduction

The Global Forum on Internet Governance held by the UNICT Task Force in New York on 25-26 March concluded that Internet governance issues were many and complex. The Secretary-General's Working Group on Internet Governance will have to map out and navigate this complex terrain as it makes recommendations to the World Summit on an Information Society in 2005. To assist in this process, the Forum recommended, in the words of the Deputy Secretary-General of the United Nations at the closing session, that a matrix be developed "of all issues of Internet governance addressed by multilateral institutions, including gaps and concerns, to assist the Secretary-General in moving forward the agenda on these issues."

This paper takes up the Deputy Secretary-General's challenge. It is an analysis of the state of play in Internet governance in different forums, with a view to showing: (1) what issues are being addressed (2) by whom, (3) what are the types of consideration that these issues receive and (4) what issues are not adequately addressed.

There is already some governance of the Internet, as many of the studies presented to the Global Forum show. The governance takes place in a variety of organizations and regimes: some are intergovernmental, as international conventions are implemented; some are in the business world, as technical standards are developed; still others take place in civil society institutions. If all these different regimes function properly to maintain order, the Internet governance issue is simple: do no harm and let them be. However, if key component regimes do not function well, or produce contradictions or conflict with other regimes, or if major areas are missing, then the conflicts or problems must be addressed by new agreements.

Other Catalogues

In preparing this matrix of Internet governance activities, we build on the efforts of others. The Markle Foundation has prepared a useful listing of international organizations and their ICT-related projects and divisions.[2] The Markle report, however, does not focus specifically on Internet governance and provides no framework for classification and analysis of Internet governance activities and agreements, nor does it delve into the intersection or interactions between the different organizations and activities.

The International Chamber of Commerce (ICC) has also prepared a valuable initial contribution.[3] This report benefited from ICC's broad catalogue of ICT-related initiatives at the national and international levels and in the private sector. However, this report explicitly develops and justifies its definitions and the conceptual framework used to

[2] Guide to International ICT Policy Making, New York: The Markle Foundation, July 2003.

[3] "Matrix of Issues Related to the Internet and Organizations Dealing with Them." Paris: ICC, 16 March 2004.

classify and include various activities. In addition, it attempts to identify where agreements, disagreements and gaps exist, rather than simply listing activities.

Conceptual Framework

A conceptual framework is necessary if there is to be progress in dealing with Internet governance. Any international negotiation for collective agreement must build on prior levels of agreements. The first step is to agree on the "building blocks" of policy. Those building blocks take two forms, each of which is relevant to Internet governance:

- *Statements of Fact*: Before policy makers can make decisions about Internet governance, they must agree on what is "the Internet." Likewise, they need to agree on what constitutes "Internet governance." Without prior agreement on the relevant facts and definitions, higher-level discussions could be hindered by implicit and possibly unrecognized differences in understandings.
- *Norms*: After reaching a common understanding of the facts, policy makers need to agree on what is "good". Norms are standards and obligations that parties to Internet governance agree should be followed, serving as criteria to evaluate what is good and bad. But norms are little more than a "wish list" unless they are grounded in a solid factual understanding of what exists, what is possible and the costs and benefits of change. Once policy makers agree on facts and foundational norms, it is then possible for them to formulate specific rules and procedures for governance.

This report proposes statements of facts relevant for Internet governance. These are not presented as definitive; final responsibility for identifying the relevant facts lies with policy makers. However, by presenting some initial definitions based on research, policy makers can be assisted in that task. This paper does not propose norms for Internet governance. Agreement on norms is a subsequent step that should be taken by the WGIG.

Key statements of fact provide answers to the following questions:

- What is the Internet?
- What is Internet governance?
- What are the different types of governance?
- What players are engaged in what type of governance activities?

Definitions

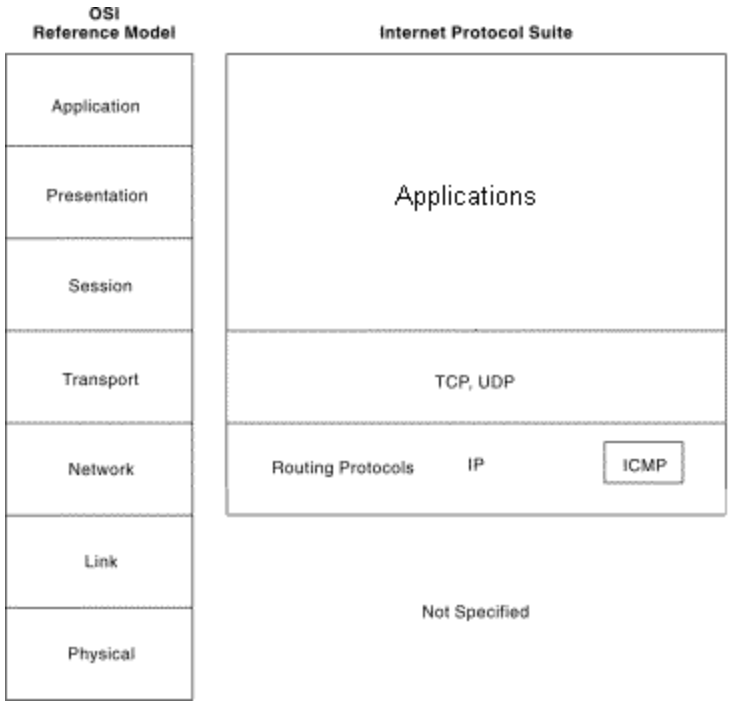
The WGIG must define Internet governance. How one defines "Internet governance" depends critically on how one defines "the Internet."

The Internet

The Internet is not a hardware standard or a physical infrastructure. It is based on a set of software instructions (known as "protocols") for sending data over networks.[4] The Internet protocols can operate on many different physical technologies, and can be used as the underlying communication mechanism for almost any kind of higher-level software application, such as accessing Web sites, word processing, streaming video, voice communication or games. The key concept is "internetworking;" the Internet protocols were designed to link networks to networks.

A widely-accepted reference model divides data communication systems into distinct "layers." The schema, known as the OSI model, further clarifies the scope of what we mean by "the Internet." (Figure 1) Under the OSI model, Internet Protocol (IP) would be classified as a "layer 3" standard.[5] The Internet is not a specific software application; it is a carrier that allows software applications to communicate and interoperate.

Figure 1



Thus, we define *Internet* as the global data communication system formed by the interconnection of public and private telecommunication networks using Internet

[4] Internet Protocol (IP) works by dividing messages up into "packets" and attaching sender and receiver addresses to those packets so that they can be routed to their destination. A closely related protocol, TCP, governs error control and the rate at which packets are sent.

[5] In the OSI model, layer 1 refers to physical (hardware) standards, such as those defining how fiber cables, radio frequencies or copper wires are constructed and make signals. Layer 2 standards define basic data structures and access control mechanisms on physical transmission media. Layer 3 is called the "networking" layer. It refers to the higher-level information about how the communicating devices are addressed and how the data they transmit is routed from sender to receiver.

Protocol (IP), TCP and the protocols required to implement IP internetworking on a global scale, such as DNS and packet routing protocols."[6]

Basic Facts about the Internet

The Internet as it exists today has several characteristics that have to be taken into account in any discussion of governance. These include the following:

- **Standards Commons**: The Internet is based on open and non-proprietary standards that can be freely adopted by anyone. Occasionally patented technology is incorporated into an Internet standard, but only if it is available at reasonable and nondiscriminatory rates.
- **Private Market**: The networks interconnected through the Internet protocols are owned and operated by autonomous organizations, mostly in the private sector. Most of the investment is small scale and private. Services and interconnection are coordinated primarily on a market, contractual basis.
- **End-to-End Principle**: The Internet protocols were designed to provide a neutral, transparent channel for the widest possible variety of information services. On the Internet, the network's job is limited to transmitting simple data units as efficiently as possible, leaving responsibility for software applications and other higher-level functions, such as authentication and encryption, to the devices connected to it. In other words, most of the intelligence and responsibility is located in devices at the *ends* of the network, not in the channel itself.[7]
- **Global**: The Internet's methods of establishing communication are non-territorial. The routing structure is independent of political jurisdictions and connection costs are insensitive to distance and political boundaries. This has created a non-territorial arena for human interaction and thus for policy and governance. At the earliest stages of the Internet's development it might have been possible for its connectivity arrangements to be structured to conform to national boundaries. Address blocks might have been given to countries instead of to global or regional entities, a national or territorial address assignment policy might have been adopted instead of Internet service provider-based address assignment, and global top-level domains could have been eliminated and everyone forced into country codes. But this is not the way the Internet evolved, and any attempt to force it into a territorial model now would involve enormous transitional costs.

[6] This definition recognizes that an enormous number of applications have been developed that run on top of the IP protocols, but only a few of them are truly core to the functioning of the Internet. We include DNS as a core Internet protocol, for example, because the growing number of applications using the Internet make the detachment of names from IP addresses ever more necessary. Likewise, routing of IP traffic would almost certainly grind to a halt without CIDR, BGP and a few other critical routing protocols.

[7] Our use of the term "end to end" is based on paragraph 2.3 of RFC 1958, "Architectural Principles of the Internet" (June 1996). We recognize that some definitions of "end-to-end" focus on the "transparency" of the connection between hosts, and that this form of "end-to-end" is regularly violated by Network Address Translators, proxy servers and firewalls. But we do not consider transparency to be an inherent feature of the Internet.

Internet Governance

We define *Internet governance* as "collective action, by governments and/or the private sector operators of the networks connected by the Internet, to establish agreements about the standards, policies, rules, and enforcement and dispute resolution procedures to apply to global internetworking activities." In other words, our matrix of IG institutions includes only those legal, regulatory and policy problems that are arise as a direct consequence of the involved parties' mutual use of the Internet protocols to communicate globally. Note that our definition includes private sector actors as parties to governance. If one understands how the Internet's architecture distributes decision making power over the internetworking process, this cannot be avoided.

The definitions are designed to draw a clear boundary around Internet governance issues. Under our definitions any technical standards or resource assignment issues that occur at layers 1 and 2 are not considered Internet governance problems, and most (but not all) issues in the application layer are not considered part of Internet governance. But public policy issues cannot be so easily bounded, because intergovernmental policies or treaties don't fall into neatly defined "layers." Policy can "govern" various aspects of internetworking by affecting the physical layer or by shaping the external economic or legal environment in which the Internet operates, for example by regulating the business of Internet service provision or penalizing spammers. But to qualify as Internet governance, the *object* of the policy must be to somehow affect internetworking using the Internet protocols.

In the early stages of the WSIS process, definitional debates centered on the distinction between a "narrow" definition that encompassed only ICANN-related functions (Internet resource allocation and assignment), and a "broad" definition that seemed to include anything and everything related to ICT governance. Both extremes miss the mark. Confining concepts of Internet governance to ICANN is arbitrary; any objective analysis reveals that WIPO treaties, e-commerce conventions and other developments must be considered forms of Internet governance, because they directly target and behaviors that rely on communication via the Internet protocols.

On the other hand, the definition advanced here also counteracts a widespread tendency to blur the line between "Internet governance" and "governance of all forms of communication and information." Conflating those two things is a mistake the WGIG cannot afford to make. Even our limited definition of "Internet governance" encompasses a very large range of issues and activities, as Tables 1 and 2 show. If its scope is defined even more broadly it will be impossible to develop coherent responses to problems. Internet is just a subset of information and communication technologies (ICTs). There are many governance issues related to ICTs that cannot be affected by developing rules or policies for the Internet. Our definitions facilitate a clearer focus on the problems specific to global internetworking. If accepted and used consistently by the WGIG participants, the definitions prevent Internet governance from becoming a proxy for other problems that really have little to do with the Internet.

We recognize that the Internet can be affected by governance in adjacent areas. For example, spectrum availability, which is really a physical layer problem that is not specific to the Internet, might affect the applications and uses of the Internet. To capture these kinds of interrelationships, one would need a broader (and much fuzzier) definition of Internet governance.

Is the "digital divide" an Internet Governance Issue? Only partly. Under our definitions, gaps in physical telecom infrastructure development would *not* be considered an "Internet governance" issue. Disparities in physical access facilities involve *all* forms of ICT, not just the Internet. Those gaps reflect disparities in economic development and access to finance capital. Changing the way internetworking with IP is governed cannot, by itself, make fundamental changes in that situation. On the other hand, Internet governance can affect the distribution of *Internet-related* resources such as IP numbers or domain names. It might also affect the way Internet service providers pay each other for interconnection, or the degree of competition in the supply of Internet services, which in turn might affect development or the distribution of wealth.

If one ignores the crucial distinction between Internet and ICTs generally and attempts to use "Internet governance" as the lever for addressing global disparities in all forms of ICTs, one is likely to fail at both Internet governance and at bridging the digital divide. Internet governance regimes cannot do much to improve financing of or access to infrastructure; by the same token, constructing or extending physical infrastructure will not by itself resolve the transnational governance issues unique to global internetworking. The WGIG has to be clear about what problems it is trying to solve, and recognize that it cannot solve all of them.

The Three Governance Functions

What is meant by "governance?" Here as before, precise and clear distinctions are helpful. We have already provided a general definition of Internet governance. Within that framework, three distinct types of governance functions have been identified and form the basis of the inventory. They are: 1) technical standardization, 2) resource allocation and assignment, and 3) policy formulation, policy enforcement, and dispute resolution. Each function is characterized by different processes and expertise, different methods of "enforcement," and is often carried out by different organizations. It clarifies the analysis greatly to keep the three functions distinct.

Technical Standardization

The first function is technical standardization. This has to do with how decisions are made regarding the basic networking protocols, software applications, and data format standards that make the Internet work. Organizations that perform these functions define, develop and reach consensus on technical specifications. The specifications are then published and have value as a means of coordinating equipment manufacturing, software design and service provision in ways that ensure technical compatibility and

interoperation. The technical standardization functions of the Internet have been performed mainly by non-State actors, as our tables will show. In Internet governance, there is often a close relationship between technical factors and policy. Policy choices may be constrained by technical architecture or concerns about technical feasibility; by the same token, there is sometimes pressure put on technical standards developers to embed or reflect policy decisions in their standards development.

Resource Allocation and Assignment

The second function is resource allocation and assignment. When usage of a global resource, such as the IP address space, radio spectrum or telephone country number codes, must be exclusive, usage must be coordinated or administered by an organization or some other mechanism. The assignment authority allocates or partitions the resource space and assigns parts of it to specific users. They also develop policies, procedures or rules to guide the allocation and assignment decisions. This function was the original source of controversy in Internet governance, where disputes concerning the assignment of top-level domain names led to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN).

Resource assignment is not the same thing as technical standardization. Technical standards may *create* a virtual resource that requires exclusive assignment when put into operation (e.g., the technical standards defining the IP protocol creates an address space, and the DNS protocol defines the domain name space). But defining and reaching consensus on the standard is a completely different function from the subsequent allocation and assignment of the resources. Some organizations combine both functions (e.g., IEEE Ethernet group, ITU);[8] other organizations (e.g., ICANN, IETF, North American Numbering Council) do not. The issue of the authority behind the organizations or mechanisms is important in resource allocation. Who is ultimately responsible for the decisions made, in legal and political terms, becomes important and often the entity that has legitimate authority can affect how resources are assigned. When resources are scarce, control of the institutions becomes important to the concerned actors.

Policy Formulation, Enforcement and Dispute Resolution

The third function is policy making. This refers to the formulation of policy, enforcement and monitoring, and dispute resolution. It involves the development of norms, rules and procedures that govern the conduct of people and organizations, as opposed to the structure and operation of the technology. While the Internet itself is merely a channel for communication and, in that sense, is policy-neutral, many public policy issues arise either as a consequence of its use by a growing number of people in an international context, or

[8] But when the same organization combines both standards making and resource allocation/assignment, the two functions are almost always carried out by separate departments or divisions.

because States and non-State actors want to respond to national and international problems by regulating the technological system itself.

Including this third function defines what can be termed the broad view of Internet governance. While some have argued that by dealing with policy issues, the scope may become too broad, we intend to show that it is the *linkages* between policy issues and the rules and procedures for standardization and resource assignment that produces the most significant governance problems. A more comprehensive view of Internet governance can help solve the problems that issue-regimes face when they confront the non-territorial way in which the Internet functions.

Categorizing Actors in Internet Governance

The international nature of the Internet means that most Internet governance has to take place through multilateral actors. Some of these are international organizations through which States transact their business, but many are non-State in nature. Within the category of State actors are those whose membership is open to all States, and those that limit membership by region, economic status, or some other criterion. Among non-State actors, some have been formally established and legally recognized, while others are informal.

Whether governance takes place in one or another venue is important. It affects the authoritative nature of the decisions, the legitimacy of the decisions, and the degree to which governance regimes permit or foreclose choice and competition.

State Institutions with Universal Membership

International organizations composed of States that are open to all recognized governments have been the traditional building block of global governance. Since the end of World War II, the UN system has formed the nexus of global governance. The UN Secretary-General has been given a role in Internet governance as a result of the first phase of WSIS. A number of organizational units within the United Nations deal with specific aspects of governance through the international conventions that they service. They include the human rights regime supported by the Office of the High Commissioner for Human Rights, the model laws supported by the Secretariat of UNCITRAL, and the organized crime conventions supported by the Office on Drugs and Crime. The ITU and WIPO are State/Universal actors concerned with the technical and policy issues associated with telecommunications and intellectual property respectively. In addition, the World Trade Organization monitors the Internet aspects of trade and UNESCO has a concern with education and freedom of expression.

State Institutions with Non-Universal Membership

Many of the issues related to Internet governance are dealt with in select groups of States. These are usually regional in nature, but some are based on economic interests. This includes the OECD, comprised of 30 States from a number of different regions that develops internationally agreed instruments, decisions and recommendations, and the G8.

It also includes regional organizations like the Council of Europe and APEC. These organizations can develop principles, norms and rules that bind their members.

Formal Non-State Institutions

A considerable amount of Internet governance takes place in non-State institutions. A major example is the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for allocating top-level domain names and IP addresses. This organization is incorporated in California and formally reports to the United States Department of Commerce. Another example is the Internet Systems Consortium, also chartered as a California not-for profit organization, which manages a globalized root server and issues the dominant software that implements the Internet's DNS protocol.

Informal Non-State Institutions

Internet governance is sometimes provided by informal institutions. These include particularly the Internet Engineering Task Force (IETF), which has defined most of the technical standards used by the Internet. Another example is the North American Network Operators Group (NANOG), an email list used to exchange technical alerts and information among Internet service operators. In addition, a number of informal groupings of civil society, including corporations, have worked to develop norms and standards relevant to the Internet. An example is the Anti-Spam Technical Alliance (ASTA) whose founding members include America Online, British Telecom, Comcast, EarthLink, Microsoft, and Yahoo! The World-Wide Web Consortium is a major grouping dealing with application software standards over the Internet and also plays a role in the development of technical standards in such areas as internet accessibility for persons with disabilities.

State Actors

In a few cases, national governments could also be considered "multilateral actors" because their decisions can affect the operation of the entire Internet. For example, United States government entities like the Department of Commerce, the Federal Communications Commission, the Justice Department and the Department of Homeland Security can make decisions with extraterritorial effects (sometimes deliberately, sometimes inadvertently). The report highlights a few of those cases (e.g., the U.S. Department of Commerce relationship with ICANN), but concentrates most of its attention on the multilateral actors through which most States and non-state actors work on the international aspects of the Internet.

The State of Play in Internet Governance Processes

The matrix that has been developed is based on two tables. Table 1 shows which organizations have been actively involved in Internet governance. Table 1 is a matrix with *organizations* forming columns, and *issue-areas* as rows. The activities in the cells are color-coded by *type of governance function* (technical standardization = blue, resource allocation/assignment = yellow, and policy = green). In a few cases, it also identifies where studies and meetings are taking place, although there is no attempt to

comprehensively cover this type of non-governance activity. Table 1 thus provides a quick overview of which organizations are active in which areas, what type of governance function they are performing, and the overall pattern of Internet governance.

Table 2 is a larger table with rows for each issue-area and three columns. The first column, "Agreements," provides a short description of the agreements in each issue. The second column provides a short description of areas of disagreement. The third column identifies gaps or concerns. To reach these observations, the method of analysis used was to examine the proceedings of the organizations in which the discussions have been taking place and from that to extract the necessary conclusions. An agreement is said to exist if it is embodied in a decision formally reached by an intergovernmental body (in the case of State-based organizations) or by the organization's stakeholders (for non-State-based organizations). This can be a convention (which would be legally binding), or a resolution adopted by consensus (that would be normatively binding). A disagreement is when there is clearly more than one position and the body concerned has not yet been able to resolve it. Finally, a gap exists if an issue that should be considered from the perspective of other forums, but is not being considered at all.

Table 1: Who is Doing What

As can be seen from Table 1, a large number of organizations, both State and non-State, are actively involved in Internet governance. Governance is fragmented; no one organization dominates any of the issue areas, and there are almost no issue areas in which only one organization is involved. Among state actors there is a clear segmentation of organizations by issue area, but the segmentation is breaking down in certain key areas. Notably in e-commerce and intellectual property, States have had to confront the impact of the Internet on pre-existing international agreements. As these implications have become clearer, the scope of the issue has grown; e.g., intellectual property protection policy has spilled over into free expression policy and trade policy, while e-commerce issues also spill over into trade. One surprise is how little systematic activity there is in the area of competition policy.

ICANN is involved in policy governance that touches on several issue-areas as they relate to domain names: free expression, privacy, and trademark protection. Its resource allocation/assignment activities also affect competition policy, authentication, security and global resource management as they pertain to domain names and IP addresses. ICANN's unique basis in private contracts gives it real leverage to address a broad range of issues related to the resources it manages.

Governance of technical standardization and resource allocation/assignment is largely in the hands of non-State actors. One of the key organizations, the IETF, is not a formal organization.

Table 2: The Nature and Depth of Agreements

Table 2 shows that the agreements cover many areas, but often do not extend much beyond general norms; agreement is broad but not deep. Examples include the CHR Resolution 2003/42, the Durban Declaration, Articles 17 and 19 of the Covenant on Civil and Political Rights, and the Council of Europe Resolution on Free Expression. All articulate widely accepted norms, but none are based on common understandings of the basic facts of the Internet and therefore cannot translate the norms into specific rules and procedures that would make them globally enforceable. Frequently, the absence of an agreement about implementation is a deliberate result of the international system, which is based on territorial sovereignty and prefers to leave enforcement to the national governments. Lack of deeper agreement about implementation leaves the international organizations without the ability to monitor the application of agreed norms and procedures.

Many agreements are sector-specific and tend to neglect linkages with other areas. For example, the WIPO treaties on circumvention of copyright protection may not mesh with UNESCO-supported norms regarding the promotion of science and culture. The ICANN policies regarding access to contact data about domain name registrants may conflict with some widely accepted international norms regarding privacy and some national laws. Where there are deep agreements, most notably in electronic commerce and privacy, they have been realized in non-universal organizations like the OECD, so they are limited in their application. In other areas, the absence of an agreement about implementation leaves international organizations without the ability to ensure consistency in the application of agreed norms and procedures by national governments.

Two factors may inhibit deeper agreements about Internet governance. First, policy bodies have not formally recognized and accepted the non-territorial nature of the Internet. Traditional international agreements are based on the assumption of territorial jurisdiction, and this foundational condition simply does not hold here. There is no consensus on, and in most forums no real discussion of, the nature of the Internet as a globalized channel of communication.

ICANN's private sector-based, contractual approach to Internet governance was originally put forward as a solution to the problem of non-territoriality. Whatever its normative merits, the ICANN regime has potentially global effects, because contracts allow policies and norms to be translated directly into rules and enforced upon any private actors. But, as noted in Table 2, there are still fundamental disagreements about the ICANN regime. One of the most important is the supervisory and contractual authority over ICANN and the DNS root zone held unilaterally by the U.S. Government. There are also disagreements about the nature of ICANN, that concern the role of the Government Advisory Committee and the lack of effective participation by developing country governments and stakeholders.

Consensus is also inhibited by the lack of recognition, acceptance and understanding of the end to end principle. Absent basic agreement here, it is unlikely that solid consensus

in many policy domains can be reached. If, for example, it is agreed that the Internet should continue to conform to the end-to-end principle, the focus of policy would be on the senders and recipients of messages rather than the channel itself. If, on the other hand, governments believe that control and other policy mechanisms should be built into the underlying Internet code, the focus of policy might be on that.

Catalogue of Organizations by Governance Function

In this section the report expands upon Table 2 with a narrative discussion. The discussion takes each of the three governance functions, identifies and describes the organizations involved in that area, and mentions the relevant agreements, disagreements, and gaps.

Technical Standardization Function

In our view, there are really only two venues that are critical to the development of core Internet standards on a global basis: the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU), specifically, the ITU-T. Of these, IETF-related activities constitute the dominant force in Internet standards. ITU-T is moving into the development of Internet standards and sees that move as critical to its future, but at the present time its work on Internet standards can be seen as supplementary to (and sometimes competitive with) IETF activity. The World Wide Web consortium (W3C) is relevant because it develops application-layer standards that facilitate private governance arrangements – but it does not really develop technical standards that govern IP internetworking as such.

Based on our definition of the Internet, we do not include global general standards organizations such as IEEE or ISO or regional standards organizations such as ETSI as participants in Internet technical standardization. IEEE plays a very important role in the development of Layer 1 and Layer 2 standards often used in conjunction with the Internet, but it does not develop protocols central to the operation of the Internet as such.

IETF (Nonstate/Informal)

The IETF is unincorporated. It is not an organization per se but a set of organically evolved practices maintained by a combination of oral culture, RFC documents defining a process, and working groups focused on specific problems. Two appointed groups, the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), take responsibility for overseeing certain aspects of the standards development process. Standards that emerge from the working groups with a "rough" or declared consensus are given an IETF-wide last call. They must then be approved by the IESG. There is an appeals process in which the IAB can overrule the IESG. To the extent that IETF has any legal identity, it is derived from the Internet Society (ISOC), which funds the RFC Editor, reviews and approves the selection of IAB members (which in turn reviews and approves IESG members), and generally provides something close to a central organizational focal

point for many of those active in IETF. However, IETF as a standards development process is open to any individual whether they are ISOC members or not, and in theory those involved in IETF standards work do so as individuals, not as representatives of corporations or governments. IETF's budget is about US$ 2 million.

As an informal non-state organization one cannot speak of "areas of agreement" or "disagreement" in IETF in the same way one would in reference to an international treaty. But one can identify some of the fundamental principles that have become institutionalized, self-reinforcing aspects of the IETF standards process:

- Standards must be open and nonproprietary
- The end-to-end principle[9] is considered a critical norm
- Standards should be simple, scalable, and extensible, and multiple implementations possible
- Standards documentation should be open, public and freely available
- Participation is open and participants act as individuals, not as formal representatives of corporations, governments or organizations.

ITU (State/Universal)

Formed in 1865, the ITU is the oldest intergovernmental organization in the world. The organization is currently divided into three sectors: Telecommunication Standardization (ITU-T), Radiocommunication (ITU-R), and Development (ITU-D). ITU as a whole has 189 member states, supplemented by various "sector members" – mostly corporate equipment manufacturers and service providers, but also some international organizations. Each of its three sectors has its own committees, conferences and working methods. Over the course of its growth and development for more than a century, ITU has taken on a heterogeneous set of functions, ranging across standardization, policy making, resource assignment and allocation, sector research and statistics gathering, education, the promotion of telecoms development in developing countries, and running trade shows. For the years 2002-2003, the budget of the Union as a whole was 342 million Swiss francs, or about US$ 279 million.

For reasons explained above, we concentrate exclusively on ITU-T when discussing the standardization function. ITU-T's standardization work is carried out by "Study Groups" restricted to ITU-T members. These develop standards known as "Recommendations." Study Groups' work is carried out primarily by industry representatives (sector-members) but the product must be approved by member states. Unlike IETF's "rough" or "declared" consensus, ITU-T SGs operate on the basis strict consensus – no recommendations can be approved unless all member states agree to them, or refrain from opposing them. Unlike IETF, ITU-T charges for access to most of its key standards documents, and participation of private sector or civil society organizations requires

[9] 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.

payment of substantial membership fees. Most of ITU-T's Internet-related work takes place in Study Group 2 (E.164-related standards, including ENUM issues, voice QoS over IP networks) Study Group 13 (MPLS), Study Group 16 (Multimedia, H.323) and Study Group 17 (security, certificates and directories).

ITU – IETF Relations

ITU-T and IETF represent two distinct phases of standardization. With its emphasis on "rough consensus and running code" IETF was a place to create new standards for a new industry (Internet service). ITU-T on the other hand maintains and upgrades standards in a long-established industry and technology. Now that the Internet has matured, IETF has to make the transition to the latter kind of standards-making, and its processes will have to adapt.

ITU-T and IETF make an effort to work together, and many ITU-T Study Groups liaise with IETF on Internet-related standards. Perhaps inevitably, however, the relationship is sometimes competitive. IETF's position as the definer of the core IP-related standards, its more focused nature, its resident expertise in those standards and the principles on which they are based, and the backing of major multinational corporations gives it the upper hand in Internet standard-setting. What ITU has that the IETF lacks is the participation and support of the world's undeveloped and developing countries. With its one country, one-vote governance at the highest levels of its authority, the ITU's processes are much more reflective of global politics than IETF's.

Any changes to the governance regime in standardization must recognize and accept a basic constraint: the world of information and communication technology development is too large, complex and diverse to be managed in any single forum. The producer groups involved can and will migrate to whatever standards development venue suits their interests.

W3C - World Wide Web Consortium (Non-State/Informal)

The W3C does not develop Internet standards *per se*. It develops important standards and technologies regarding data structures and formats that are commonly used on the Internet, but these applications ride on top of the Internet protocols just as many other applications produced by private enterprises or small-scale standards coalitions do. We include W3C here because its standards are sometimes intended to facilitate private governance arrangements. For example, its Platform for Internet Content Selection (PICS) was designed to permit end users to filter content according to criteria of their own choosing. The W3C work on standards for Internet accessibility for persons with disabilities also takes on a normative role.

Resource Assignment Function

The Internet protocols create two critical resource spaces: the IP address space and the domain name space. Less critically, it also requires unique and exclusive assignment of protocol port numbers in certain cases, and Autonomous System Numbers. A relatively

new IETF-defined protocol, ENUM, also creates an area in which resource assignment for ITU and IETF standards intersect, as ENUM maps the ITU's E.164 standard telephone numbers to domain names.

Four key organizations perform the resource assignment functions for the Internet: 1) the Internet Corporation for Assigned Names and Numbers (ICANN), 2) the regional Internet address registries (RIRs), 3) the Internet Software Consortium, and 4) International Telecommunication Union (ITU). In addition to these four identifiable entities, there is also a diverse set of root server operators in the U.S., Europe and Japan associated with different organizations but not formally integrated into a corporate entity nor formally bound to any governance regime. One might also include international associations of country code top level domain (ccTLD) managers, such as CENTR and APTLD, as actors in this space. We will discuss each of these organizations in turn, and then describe some of the issues surrounding resource assignment.

ICANN (Nonstate/Formal)

ICANN is a California nonprofit public benefit corporation, the creation of which was invoked by the U.S. Department of Commerce following a public proceeding in 1997-98 that invited international participation. ICANN took over the resource assignment functions associated with the Internet Assigned Numbers Authority (IANA), an informal IETF-associated entity run by University-based computer scientist and Internet pioneer Jon Postel. IANA had been funded via grants from U.S. government agencies. In 1998 it was detached from the IETF complex of organizations, and bundled with a new, policy-formulation body (ICANN). ICANN was deliberately set up as a private sector, multi-stakeholder governance organization, although it included some governmental input through its Governmental Advisory Committee (GAC) and its contractual relations with the U.S. government.

ICANN engages in governance in two ways: via resource assignment and via policy making related to the resources. In this section, we will discuss areas of agreement and disagreement only as they pertain to resource assignment, leaving policy issues to the next section.

In terms of areas of agreement, there is widespread consensus among the stakeholder groups involved in ICANN, including the civil society groups, that a private sector, multi-stakeholder governance regime is preferable to an intergovernmental one. There is also widespread agreement on the need for a central coordination body to manage the DNS.

There are many areas of disagreement. Most fundamental, by reference to the original concept of ICANN, is its inability to incorporate most of the country code top-level domain managers (ccTLDs) into its regime. Without the full participation and binding commitment of these essential elements of the global DNS, ICANN's governance is necessarily limited and fragmented. The structure and processes through which ccTLDs are represented in ICANN's policy formulation processes, and the contractual arrangement under which they might be formally bound to the regime's rules, are still,

after six years, unsettled and a source of conflict. However, it should be noted that many participants in the process believe that the limits on its power that come from such fragmentation are not necessarily a bad thing.

The root server operators have tried to avoid ICANN politics altogether rather than bargain and negotiate with it. Key root server operators have participated in ICANN advisory committees as individual experts, but with the exception of Verisign, a root server operator that is formally contracted to the U.S. and to ICANN as a domain name registry, the root server operators have simply pursued their own way. Indeed, many of them promulgate a philosophy that argues, persuasively to many steeped in Internet traditions of distributed authority, that maintaining the independence of the root server operators is a healthy thing for the Internet.

Another major area of disagreement concerns the special role of the US Government as contracting authority for ICANN and supervisor of its changes to the root zone. The original policy document for ICANN promised to end U.S. supervision after two years. U.S. supervision has however continues until 2006 under the current contract. While this is not a major source of controversy within ICANN itself, it is a critical source of contention among other governments, and was one of the factors leading to the formation of the WGIG.

A more subtle but longer term area of disagreement concerns the relationship between ICANN rules and IETF standards. It is unclear whether, or to what degree, ICANN should, in regulating the suppliers of domain name services, make compliance with the relevant standards documents compulsory or not.

Other important areas of disagreement include: the absence of a clear policy or process for the addition of new top-level domains; the degree to which ICANN is, or should be, accountable to individual users of the Internet; the degree to which ICANN is, or should be, accountable to or responsive to governments or independent of them.

RIRs (NonState/Formal) and NRO (NonState/Informal)

The Regional Internet Registries (RIRs) are responsible for distribution of Internet Number resources, including Autonomous System Numbers and IPv4 and IPv6 addresses. IP addresses are the most important identifiers for the Internet's operation. IP packets cannot work without unique address assignment and scalable routing techniques that permit packets to find their destination. There are now four RIRs: ARIN (encompassing North America, parts of the Caribbean and parts of Africa); RIPE-NCC (Western and Eastern Europe, parts of Africa, parts of the Middle East); APNIC (Asia, Far East); and LACNIC (Latin America). Efforts are underway to create an African RIR (AfriNIC). All existing registries are private sector nonprofits with roots in the Internet technical community and a membership composed primarily of Internet Service Providers, telephone companies and Internet hosting services.

As service organizations with control of valuable resources, the membership base and finances of the RIRs are strong. Most RIRs charge fees for address allocations. RIPE has

nearly 4,000 members, APNIC and ARIN have nearly 1000. ISPs that receive a direct allocation of IP address space from ARIN are automatically accorded membership. Any individual can also join ARIN for a $500 annual membership fee. To our knowledge, there are no major disagreements regarding policy and governance within the RIRs, or across RIRs. Longer term, important issues about economic policy regarding address allocation could arise. The fee structures of the RIRs may discourage some kinds of smaller scale utilizations of wireless networks. One could debate whether RIRs should compete with each other over pricing, whether they should maintain territorial monopolies on assignments, and whether addresses should be auctioned. Those issues have not surfaced as major points of disagreement yet, however. All of the address registries strongly support the private sector-based, "self regulatory" model of governance, and oppose movement of these functions into intergovernmental or governmental institutions. They have, however, had concerns about and disagreements with ICANN.

The Number Resources Organization (NRO) was formed in response to those concerns. It is an instrument of collective action among the RIRs that strengthens them in their relationship to ICANN. It also allows organizations outside of the RIRs to interact directly with all of them at once instead of dealing with each RIR separately. As of this writing, it is unincorporated. The MoU on which it was founded creates a framework for a global IP address policy development process which in some ways acts as a substitute for ICANN's Address Supporting Organization. Indeed, some of NRO's founding documents and discussions make it clear that the organization was formed in part as an entity that might step in to meet the need for IP address allocation should ICANN fail. At the current time, however, NRO and ICANN are working together.

Root Server Operators (Mostly Non-state/Informal)

Root servers are a critical part of the resource assignment regime of the Internet. They provide authoritative data about the top level of the domain name hierarchy. Most of the Internet domain name system's 13 root server operators are not formally tied into a governance regime of any kind. Those operated by ICANN itself, and a special root server operated by VeriSign under contract with the U.S. Department of commerce, (and perhaps also those operated by the US military) are contractually or legally bound to the ICANN regime or accountable to the US government. The others, however, are operated by heterogeneous actors in different nations. An informal "Root Server Technical Operations Association" at www.rootservers.org now gives them something of a common voice. They describe themselves as "different professional engineering groups" and stress that they are not involved in policy making or data modification – they just publish (and do not edit) the root zone file and answer queries. Their presentations emphasize the value of diversity and coordination over hierarchy and coercion in coordinating the resource.

The Internet Systems Consortium (ISC) is a private, non-profit corporation based in California. It operates the "F"-root server, provides DNS hosting for more than 40 top-level domains, and (most importantly) produces BIND, an open-source software implementation of the DNS protocol that has dominated that field since the early days of

the Internet.[10] ISC's position as the dominant supplier of DNS software and its control of a root server that is "mirrored" globally makes it an important actor in the resource assignment/infrastructure operation space. ISC calls itself the "leading supplier of public infrastructure for the global DNS."

In at least one instance, the privatized "stewardship" model followed by the Internet developers has allowed actions to be taken quickly and decisively to address governance problems. An example is ISC's deployment of anycast technologies to expand the geographical distribution of DNS root servers. ISC's Paul Vixie used an innovative technical configuration to "mirror" root servers all over the world, entering into private agreements with Internet operators in many different countries. On the other hand, the long-term implications, both policy and technical, of this implementation of anycast are not well understood.

ITU-T (State/Universal)

ITU plays its most critical resource assignment role as global allocator of radio frequencies (ITU-R), but as a physical layer issue radio allocations are considered out of scope in discussions of Internet governance. ITU-T is involved in resource assignment and administration issues directly related to the Internet due to its role as the assignment authority for telephone country codes under its E.164 standard.

The ENUM protocol, which was developed by IETF, maps E.164 telephone numbers into domain names. The importance of this protocol, which is too complex to be explained in any depth here, is its potential to facilitate interconnection of Internet communications with the public switched telephone network; i.e., to serve as a bridge between personal computers (or other digital devices connected to the Internet) and the traditional telephone network. Deployment of ENUM, however, raises privacy, consumer protection, authentication/security, and institutional issues.

Three years ago a disagreement between ITU and the Internet Architecture Board (IAB)/IETF broke out over administration of the ENUM domain name space. IAB/IETF, supported by the US government and major telecommunication companies, favored making <e164.arpa> the root of the ENUM delegation tree and giving the European address registry RIPE-NCC the authority to assign country codes. The ITU favored considering alternatives to the <e164.arpa> top-level domain. The consensual result for now was that RIPE-NCC administers country code assignments under the e164.arpa domain, but ITU reviews and approves requests for country code delegations from RIPE. ITU considers the issue of the control of the top level domain used by ENUM to be still unresolved.

[10] ISC claims that more than 75% of the world's DNS name servers run some version of BIND.

ccTLD Associations (nonState/Formal)

Country code domain name registries by themselves might be thought of as exclusively a national issue. However, the refusal of many ccTLD managers to join the ICANN regime fully and their self-organization into associations makes them an alternate source of global domain name governance to some degree. The ccTLDs control a considerable part of the name space. Two organizations of note are CENTR, the Council of European National TLD Registries, and APTLD, the Asia-Pacific Top Level Domain Association.

Policy Functions

A wide variety of policy issues related to the use of the Internet can be identified. They include balancing intellectual property protection with fair use and free expression, trade and e-commerce, taxation, law enforcement and crime prevention, content regulations and freedom of expression, spam, data protection, privacy and surveillance, security, rights to domain names, competition policy in the domain name industry, and domain name user privacy. Some of these issues are addressed by existing international regimes, some are addressed at the national level, others are not fully addressed yet. They involve controversies between different countries, different philosophies about the role of regulation generally and disputes among private actors. Because the issue areas are often segmented into distinct categories, conflicts among different policy regimes may go unnoticed. Moreover, the framing of the issues in their respective forums are usually based on the traditional concepts of territoriality that do not work well in the borderless venue provided by the Internet.

The policy functions that have been identified have several common elements. Most are efforts to cope with the borderless nature of the Internet in fields where traditional law and practice depends on territoriality. As a result, the philosophical differences between States that have impeded global solutions to many issues continue to be in play. This has the consequence that there are some agreements on principles and norms that should apply from a regime to the Internet, such as non-discrimination in the trade area. At the same time, there are many differences in terms of specific rules and procedures. As a consequence, few areas have managed to obtain universal agreements and most devolve the responsibility for implementing norms back to the national level.

ITU (State/Universal)

In addition to its standard-setting and resource allocation/assignment functions, ITU has made policy recommendations in a few areas. Most of them are concentrated in the issue-area of what we call "operational policies." One exception is the Plenipotentiary 2002 Resolution 130 about "security." The resolution calls for "strengthening the role of ITU in information and communication network security" and enhancing cooperation around security issues. Like many other "agreements" concerning the Internet, this resolution is little more than a statement of some broad norms, and lacks a common factual understanding of how the Internet's architecture or protocols are related to security problems. Therefore it cannot translate the norms into rules or procedures that would actually structure behavior.

ITU-T has also attempted to develop policy agreements concerning interconnection of Internet service providers. Table 1 places this is the "Operational Policies" category but it could also be viewed as a trade issue. An ITU Study Group is investigating "International Charging Arrangements for Internet Services (ICAIS). ITU passed Recommendation D.50, a very general, normative statement about compensation for Internet interconnection. ITU however, lacks both the depth of agreement and the regulatory leverage needed to strongly affect Internet charging arrangements.

WIPO (State/Universal)

Intellectual property is an issue-area that has been revolutionized by the Internet. Accordingly, there is considerable activity in this area. The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) were both created in 1996. In conjunction with the formation of ICANN, WIPO sponsored the First Internet Domain Name Process in 1998, which led indirectly to ICANN's UDRP. In 2001 it initiated a Second Internet Domain Name Process proposing new rights to names, such as extending protection to the names and acronyms of intergovernmental organizations and to the official long and short names of countries. WIPO's Joint Recommendation Concerning the Protection of Marks and Other Industrial Property Rights in Signs on the Internet was agreed in 2001, but has not yet been accepted into national laws. WIPO is also negotiating a Substantive Patent Law Treaty and there are discussions underway regarding protection of databases and the application of copyright protection to Internet broadcasting. There are significant disagreements, both among states and between states and civil society advocacy groups, regarding these topics. Even the business trademark interests do not like many of the WIPO II domain name proposals and they have as yet failed to find agreement and implementation from ICANN.

In intellectual property, many of the issues that appeared to be resolved in the mid-1990s have led to conflicts with other regimes and norms, making the environment unsettled. As law professor Peter Yu wrote, "there remains wide disagreement among countries regarding issues such as 'moral rights,' 'fair use,' duration of copyright, protection in data, rights in sound recordings, exhaustion of rights, work-for-hire arrangement and, most recently, circumvention of encryption technologies and Internet service provider liability."[11] For example, the extent to which WIPO's "Internet treaties" of 1996 conflict with freedom of expression and "fair use" is clearly unresolved, as the ongoing controversies regarding circumvention of copy protection and peer-to-peer exchange of music files shows.

UN-OHCR (State/Universal)

A central element of governance is the protection of human rights of all persons. Applied to the Internet, this includes particularly rights of freedom of expression and communication. The impact of efforts to regulate the Internet on these rights has been a major point of contention when specific proposals have been tabled in different forums.

[11] Peter Yu, "Conflict of Laws Issues in International Copyright Cases, Gigalaw.com, http://www.gigalaw.com/articles/2001-all/yu-2001-04-all.html

At the same time, the extent to which this has been part of the policy dialogue is highly variable.

The international norm on freedom of expression is found in the Universal Declaration on Human Rights and is codified in the International Covenant on Civil and Political Rights in articles 17 and 19. These norms were reaffirmed by the WSIS Declaration. They do not, however, specifically address the Internet.

The Commission on Human Rights, in its resolution 2003/42 addressed the Internet by calling on States to 'refrain from imposing restrictions which are not consistent with the provisions of article 19, paragraph 3, of the International Covenant on Civil and Political Rights, including on: … (c) Access to or use of modern telecommunications technologies, including radio, television and the Internet.' In general, the focus has been on access rather than on content, although the same resolution recognized `the positive contribution that the exercise of the right to freedom of expression' that the media and new technologies, including the Internet, can make to the fight against racial discrimination.

Some Internet content control issues have been taken up within the larger human rights regime. That regime is built around the seven human rights treaties, the work of the Commission on Human Rights and the world conferences concerning human rights. Two issues have been dealt with there. The first is child pornography, which for the Internet is explicitly covered by the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Sixty-seven States that have become parties to the Convention have undertaken to reflect its rules in national laws. There is clearly a global consensus on the norms because the Optional Protocol was adopted by the General Assembly. The fact that only 67 of 190 States are party to it, however, suggests that consensus about specific rules has yet to be obtained. Further, the issue of international enforcement remains unresolved.

The second is racist communication over the Internet. It has been argued that presentation of racist content contravenes the Convention on Racial Discrimination. The Durban Declaration of the World Conference on against Racism, Racial Discrimination, Xenophobia and Related Intolerance that took place in 2002 contains specific references to the Internet. This indicates a general consensus on the norm that extreme racist content should be prevented. However, there is no consensus about how to address the problem.

The issue of privacy has not been addressed in the human rights regime. However, General Assembly resolution 45/95 of 14 December 1990 on Guidelines for the Regulation of Computerized Personal Data Files, which is the most recent pronouncement by that universal body on the issue, provides for protection of files under a general concept of privacy, but also states that "[t]he procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State". It also assumes that the issue will be handled on a bilateral basis at the international level.

UNESCO (State/Universal)

UNESCO's mandate to promote "the free flow of ideas by word and image" and to "maintain, increase and spread knowledge" can be easily and directly linked to Internet governance issues.

UNESCO staff has prepared a "Position Statement" on Internet governance outlining a set of norms reflecting its mandate. The statement asserts that Internet governance mechanisms should be based on the principle of "openness", encompassing interoperability, freedom of expression and measures to resist any attempt to censor content. It believes that the "inherent openness of the Internet infrastructure must be preserved" and that new Internet governance arrangements must not "be subjected to governmental control, nor should they facilitate or permit censorship." UNESCO favors requiring "a precise correlation between new [Internet governance] mechanisms and the problems they seek to address." It believes that technical innovation must continue to be encouraged; and that new mechanisms should not inhibit interoperability, cause instability, nor slow down the continued technical development of the Internet. Any global Internet management system or mechanism must be technically competent, transparent and non-partisan.

In October 2003 UNESCO's member States adopted a "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace" that agreed on the norms of freedom of expression, universal access to information, cultural and linguistic diversity and equal access to education. UNESCO is also promoting an International Convention on the Protection of the Diversity of Cultural Contents and Artistic Expressions, which might have implications for Internet content, ownership of Internet content providers, or media-Internet convergence. The UNESCO convention is being promoted by those who wish to achieve a "cultural exception" to WTO-based rules on free trade in media industries, and thus illustrates the existence of another potential regime conflict in the Internet governance space.

WTO (State/Universal)

The international trade negotiations, focused on the World Trade Organization and the United Nations Commission on International Trade Law (UNCITRAL), have had difficulty keeping up with developments in the Internet. There is a consensus that the principles of free-trade that are embodied in the GATT and GATS treaties should be applied to Internet. In particular, the liberalization of telecommunications services, culminating in the 1997 WTO treaty on Basic Telecommunications Services, helped to accelerate the development of the Internet in many parts of the world. How trade principles apply to particular forms of e-commerce in practice, however, has been subject to debate. The general principles, that e-commerce must be dealt with using the same criteria as other trade issues and that there should be a moratorium on customs duties on digitalized trade, have been in place since 1998 (renewed at Doha). However, how to classify digitalized products for the purpose of applying the trade regime continues to be contentious. This has implications for software development of the Internet itself, since it is not clear how to deal with software that is central to the integrity of the Internet.

UNCITRAL (State/Universal)

The United Nations Commission on International Trade Law (UNCITRAL) has focused on how to apply earlier agreements on trade law that were based on territoriality to the non-territorial Internet. The Model Law on Electronic Commerce was adopted in 1998, but has only been converted into national legislation in twenty countries and in most of these this was done without an agreement on the key elements of certification and electronic signatures. Moreover, there is considerable variation among national adoptions. An effort to negotiate a convention on "the use of data messages in [international trade] [the context of international contracts]" in one of UNCITRAL's Working Groups has proceeded very slowly and even the title of the convention is still not agreed. Moreover, the draft convention does not cover contracts concluded for personal, family or household purposes and does not deal with consumer protection.

The issue of authentication has been addressed universally through the Model Law on Electronic Signatures of UNCITRAL adopted by the General Assembly in 2001. The Model law sets out understandings of what would constitute acceptable digital signatures, but is primarily guidance for adjusting national laws. In fact, as of 15 April 2004, only two countries (Thailand and Mexico) had reported applying the model law. The specifics of how to build authentication into software are not addressed.

UN-ODC (State/Universal)

The United Nations Convention on Organized Crime, that is supported by the UN Office on Drugs and Crime (ODC) refers in Article 29 to the need for training in "Methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology." However, it does not provide specific requirements for how to address "borderless" crime. The Convention provides a starting point, but also includes controversial approaches, particularly in extending cross border surveillance, and critically it offers very weak support for human rights and privacy.

EU (State/Nonuniversal)

For those aspects of government for which sovereignty has been ceded to the European Union, the EU functions as though it were a national government. For the other aspects, where national sovereignty is retained, the EU functions as an international organization. In this context it has provided guidance on the organization and management of the Internet as well as some of the policy issues that it has defined as falling under that rubric. One of these is data protection. EU Directive 95/46/EC of 25 October 1995 "aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when this processing is lawful." The directive is intended to harmonize national laws on data protection and has entered into force. With respect to Whois data, the EU states that "Neither the Registrars, nor the registries, nor ICANN can claim any rights over this type of information."

In the area of taxation, the EU, through Council Directive 2002/38/EC, of 7 May 2002 as regards the value added tax arrangements applicable to radio and television broadcasting services and certain electronically supplied services, has established union-wide norms

for taxing e-commerce. "For consumption taxes such as VAT, cross-border electronic commerce should result in taxation in the jurisdiction where consumption takes place and the supply of digitised products should not be treated as a supply of goods. Under the provisions of the European Union (EU) VAT system, this means that such digitised deliveries are treated as services for tax purposes." How to apply this set of procedures to non-EU businesses providing services to EU residents is still somewhat unresolved.

Council of Europe (State/Non-universal)

A Council of Europe Declaration on Freedom of Communication on the Internet was adopted by the Committee of Ministers on 28 May 2003. The Declaration specified a series of norms to protect free flow of information. While not legally binding on States, it suggested that public policies should work to open up the Internet rather than limiting it, although it also included a standard caveat regarding national security, crime and public health exemptions to the provisions.

The Council of Europe Convention on Cybercrime tries to unify national laws dealing with several different types of crime. The Convention was agreed, but has been ratified by only six States, all in Eastern Europe. It has been criticized by civil rights groups as taking a too interventionist approach and therefore conflicting with human rights norms. The Council of Europe's Declaration on freedom of communication on the Internet provides for privacy in terms of communication and anonymity for senders and receivers. However, its limitations are not well-defined. Under the Optional Protocol, privacy does not protect persons who engage in child pornography.

OECD (State/Non-universal)

The OECD's codification of privacy guidelines in its 1980 Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, while predating the Internet, articulated widely accepted norms that have proven to be relevant to debates over Internet governance. Implementation and enforcement of these norms remains at the discretion of national governments. Many believe there is a conflict between ICANN's Whois database policies and the OECD guidelines.

The issue of how to tax Internet transactions shows some of the limitations of regime formulation. The OECD has been discussing the issue for a number of years, but has not been able to agree beyond general norms such as non-discrimination. It has agreed on general criteria for assessing proposals, but absent an agreement on such matters as where taxes should be collected and on what – a problem similar to that faced by the WTO – progress has been slow. In addition, there are disagreements on how to determine where an entity to be taxed is located.

G8 (State/Non-universal)

The G8 is an informal group of eight countries: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States of America. The European Union also participates and is represented by the European Commission. The Lyon Group is composed of senior experts tasked to review and assess existing international agreements and procedures to fight organized crime. Its November 2001 recommendations, coming

in the wake of the September 11 terrorist attacks on the United States, called for weakening privacy laws to enhance "public safety and other social values" and increased powers for law enforcement agencies.

In May 2000, the G8 held a conference in Paris on security and confidence in cyberspace that brought together high-level government and private sector specialists from all of the G8 member countries to discuss cybercrime and the use of the Internet for criminal purposes. These efforts were followed up with conferences in Berlin (October 2000) and Tokyo (May 2001).

Hague Conference (State/Non-universal)

Starting in 1992, the Hague Conference on Private International Law tried to develop a Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters. In the late 1990s it became evident that the proposed Convention would have far-reaching consequences for e-commerce transactions involving the Internet, because it had the potential to result in global enforcement of non-harmonized laws. As one critic put it, "The treaty gives nearly every member country jurisdiction over anything that is published on or distributed over the Internet. If the treaty (as written) is widely adopted, it will cripple the Internet." (Consumer Project on Technology, June 2, 2001). In 2002 the negotiations, facing complete failure, were significantly narrowed to focus on clauses specifying which courts will have jurisdiction over disputes arising in B2B contracts.

ASEAN (State/Nonuniversal)

In September 1996, ASEAN held a Forum on the Internet expressing concerns primarily about the content regulation issues posed by the rapid rise of the World Wide Web and the discovery by Asian governments that their citizens were being exposed to content over which their national governments had little control. The joint press release observed that "the trans-border nature of the Internet would open individual countries to external influences and affirmed the importance of having safeguards against easy access to sites which ran counter to our cherished values, traditions and culture." No enforcement measures, rules or procedures for dealing with this problem were agreed.

In November 2000 ASEAN passed the "e-ASEAN Framework Agreement" on some very general norms focused on the economic development potential of ICTs. The member states agreed to facilitate the development of information infrastructure, facilitate the growth of e-commerce, liberalize trade in ICT-related products and services, reduce the digital divide, increase ICT literacy, and promote the use of ICT applications in the delivery of government services. Some of the trade facilitation measures of the agreement do have enough specificity to be effective, such as an agreement to harmonize tariff nomenclature and customs valuation for ICT products, but this does not directly deal with the Internet.

APEC (State/Non-universal)

The 2000 APEC Ministerial Meeting on the Telecommunications and Information Industry adopted a short agreement on "APEC Principles for International Charging Arrangements for Internet Services." The generality and lack of rules, procedures or

enforcement capability in the document is similar to ITU recommendation D.50 and as such reflects the lack of consensus among Internet service providers and governments about the degree to which Internet interconnection should be governed by means of freely developed business contracts or be more regulated by governments.

A 2001 APEC Economic Leaders Declaration in Shanghai, confirms the WTO customs moratorium on electronic transactions, and urges national finance ministers to "ensure that any taxation of internet services or electronic commerce is clear, consistent, neutral and non-discriminatory."

ICANN NonState/Formal)

ICANN has considerable leverage over the domain name registration industry as a policy maker because entry into the industry is governed by contracts with ICANN. The terms of these contracts are developed by the policy-making processes of the GNSO and adopted by the Board. The contracts function as rules governing the Industry and can be enforced either through the courts or through withdrawal of the right to operate.

ICANN's contractual agreements with registries and registrars impose a vertical separation (analogous to wholesale/retail) of the registry and registrar functions that is motivated by competition policy concerns. Competition policy is also implicated in ICANN's control over new top level domain additions, as this provides it with control over the number and type of competitors in the registry market. While ICANN's registry-registrar split commands widespread agreement, its TLD addition policy is a source of continuing disagreement. ICANN has adopted a purely ad hoc approach to additions, failing to articulate any rules and procedures, and only a basic norm (stability) regarding their addition.

The ICANN-WIPO Uniform Domain Name Dispute Resolution Procedure (UDRP) can be considered a global governance regime for the protection of trademarks in the domain name space. WIPO initially developed a proposal for such a dispute resolution procedure, but the final policy was made by ICANN and implemented using its contractual powers over registrars and registries. Although many critics have questioned its fairness and its impact on free expression, the UDRP is very popular among trademark holders and is accepted by the domain name registration industry. Few question any longer the general need for a global and expedited dispute resolution procedure. Thus, we count this as an "area of agreement," but note that there are many calls for improvement.

Privacy issues are also dealt with in ICANN. ICANN's rules require registrants of domain names to display their contact data in a database that can be accessed using the Whois protocol and displayed to anyone on the Internet. Trademark interests, law enforcement agencies and some other information service provider interests who profit from the use of the data favor keeping this data readily available. Privacy advocates in civil society, government data protection authorities, domain name registrars, many customers, and some registries, on the other hand, favor restricting access more. There is also a related debate about the regulations regarding accuracy of the data. This is an area

of deep disagreement within ICANN; policy development processes have been going on around it for several years.

Freedom of expression issues arise in the context of ICANN's DNS-related policy development. Selections of a top-level domain name string (e.g., .sex, or .kids) raises concerns about the content of the string itself (should offensive words be allowed – and what about words that are offensive in one language and innocuous in another?). There are also issues about the appropriateness of the content under a specific TLD and the rules governing that. In addition, ICANN's domain name dispute resolution process often pits owners of trademarks against critics or commentators who want to use those names for expressive purposes. The decisions on these cases are completely inconsistent and provide registrants and users of domain names no guidance regarding what is permissible and what is not.

ICRA (NonState/Formal)

The Internet Content Rating Association is an association of major Internet-related businesses, including Microsoft, AOL, Verizon, BT, Deutsche Telekom's T-Online, and some regional self-regulatory associations such as South Korea's R3. It is devoted to the promulgation of content rating standards that allow Internet users to effectively classify and block what they consider to be undesirable content. The method relies on voluntary adoption and self-rating by web site managers. Internet users can then download a free label filter software to allow or disallow access to a particular website based on their own preferences. ICRA sometimes works with governments and Internet service provider associations in specific countries to encourage adoption of the content rating scheme, for example Hong Kong. ICRA provides an example of how private sector self-regulatory activity provides an alternative to more traditional forms of governance in areas where laws are not harmonized. The usefulness of its filters, however, are limited by the minimal level of adoption by both content publishers and users.

ASTA (NonState/Informal)

Spam -- unwanted and unsolicited email sent indiscriminately to users – is generally considered unacceptable. The discussion of how to deal with it takes place at both national levels, where some governments, like the United States, have tried to pass legislation controlling it, and at the level of civil society. A major actor is the Anti-Spam Technical Alliance (whose founding members include America Online, British Telecom, Comcast, EarthLink, Microsoft, and Yahoo!).

In this area, again, we see shallow agreements on norms, but none on facts. That is, there is no consensus about whether the problem can (or should) be dealt with through technical standards, modified charging arrangements, legal regulation and sanctions, or some combination of all those efforts, nor is there an understanding of what implications various paths of attack would have for the Internet as a whole. Adding complexity, the spam issue overlaps with freedom of expression, in that any attempt to block all unsolicited email would act as a severe constraint on the right to communicate.

Recommendations

The analysis above suggests the following course of action for the WGIG.

First, the WGIG should decide on the relevant statements of fact. This paper has proposed definitions of the Internet, Internet governance, and several other facts. In this analysis, the assumption has been made that the Internet should be defined precisely in terms of the use of specific protocols for global interconnection. The WGIG needs to decide whether to adopt these, replace them with other definitions, or modify them.

Second, the WGIG should look beyond statements of fact to *norms.* This report has identified two of the most pressing normative issues. One concerns the end to end principle. There is an emerging consensus reflected at the March 24, 2004 ICT Task Force Global Forum, and other meetings, that the Internet's status as a neutral channel with intelligence and control concentrated in the end points is responsible for much of the success of the Internet and should not be disturbed. This norm, however, has not been formally accepted and its implications for governance structure have not yet been agreed. Lack of agreement about the implications of the non-territorial nature of the Internet is another key normative issue. In establishing norms, the Working Group must decide first whether internetworking should conform to the end-to-end principle, and whether its structure and governance should continue to be globalized. If those norms are accepted, then the focus of policy and governance will be on the senders and recipients of messages rather than on the channel itself, and certain constraints on governmental action can be accepted as the basis for developing policy.

Finally, the Group should consider how to define, guarantee and protect the roles of the various stakeholders in the Internet. In a state-based international system, it will be important find a foundation of legitimacy for non-state actors in governance, giving them both authority and accountability. The Group should consider how the implications of clear agreements on definitions, facts and norms could best be reflected in international agreements that could take into account the unique characteristics of the Internet.