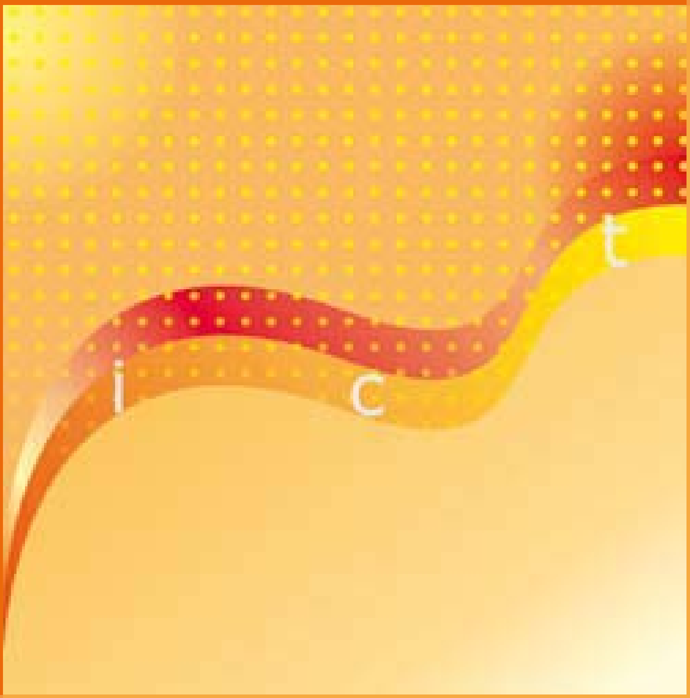
EMBARGO
The contents of this Report
must not be quoted or
summarized in the print, broadcast
or electronic media before
16 November 2006, 17:00 hours GMT

United Nations Conference on Trade and Development

INFORMATION ECONOMY REPORT 2006

The Development Perspective



United Nations

Chapter 7

THE LAYERED INTERNET ARCHITECTURE: GOVERNANCE PRINCIPLES AND POLICIES

A. Introduction

Internet governance matters because it can influence the economic and social opportunities for all peoples. Given the proven track record of the Internet as an innovation platform, it is only rational that Internet governance policy should be aimed at strengthening and improving this foundational characteristic. So far in human history, there has never been a flatter field for ambitious and competitive minds to stake their claim to technological fame and fortune. It is entirely feasible that the next Internet "killer application" may come from a developing country. Internet governance can assist this process. However, caution and deep reflection should be exercised, as misconceived policy or regulation can be harmful or even detrimental — usually to a disproportionate extent for developing countries.

The Internet governance debate is wide open. The World Summit on the Information Society (WSIS) succeeded in mainstreaming this important issue while perhaps disappointing only the most fervent optimists who may have hoped that a conclusive governance framework could have been established and set in motion. The WSIS events in Geneva and Tunis, as well as the Working Group on Internet Governance (WGIG), highlighted a diversity of views and approaches to the Internet governance issue. Perhaps the diversity was somewhat too diverse and therein lies one of the key challenges of the post-WSIS process.

What is needed in the continuation of the deliberations is convergence. However, it would be premature to seek convergence around prejudgement of an outcome. Today, and thanks to WSIS and WGIG, we have a better understanding of common terminologies and definitions. What we need to move forward is a set of criteria that will allow the development of policy and regulatory principles for Internet governance that are coherent and relevant to the Internet as a technological medium and that maintain its positive relationship with technological innovation and economic and social development.

The technical debate did not happen at WSIS and perhaps it would not have been timely. The priorities were clearly to establish "whether there are significant problems with existing governance mechanisms, and whether there are any pressing but unresolved issues that need to be tackled through international cooperation."[1] It is to be hoped that the Internet Governance Forum (IGF) — the post-WSIS successor to the WGIG — will provide a platform to engage technology and policy at the same time. This will not be an easy task as there are many public policy issues vying for the attention of the IGF. It is easy to reinterpret just about any action line from the WSIS final documents as being a governance issue, in addition to the fact that almost one third of the outcome deals explicitly with Internet governance.

This chapter proposes that Internet governance should be consistent with the layered nature of the Internet's technical architecture. More specifically, it should respect the layers principle and its corollaries. What does this mean? Unfortunately, attempting a definition at this point would be well nigh impossible. Similarly, restating the need for consistency and principles in more accessible terms can require oversimplifications that will obscure the issues at stake — and thus will be avoided. What this chapter proposes is to develop the notion of the layers principle and its relation to Internet governance from its particular elements to the point where its meaning becomes obvious. However, before going into technical and policy discussions, we will present several ideas that underscore the need for this discourse.

The layers principle is at the same time simple and opaque. The reason is that it requires an appreciation of the technology underlying the Internet protocol suite. It also requires an understanding that without the protocol, there is no Internet — in spite of all the wires, servers and networking hardware currently deployed. If we can govern well only what we understand, it follows that policymakers need to develop a sufficient technological understanding of the Internet protocol suite in order to establish quality in Internet governance.

Policymakers should go beyond understanding the economic and social implications of the Internet. They need to understand the technological Internet and how its structure is intimately related to social and economic issues and outcomes, in order to develop an effective framework of governance. Conversely, technologists need to understand that the issues of legitimacy and responsibility in governance are inseparable from efficacy. In a scenario reminiscent of the proverbial two cultures, policymakers and technologists should seek convergence. This is not unusual and we can identify similar developments in other current deliberations, such as poverty alleviation or climate change. Establishing a bridge between technologists and policymakers is therefore crucial to the positive and productive outcome of the Internet governance debate. However, rallying together in the abstract may be unproductive. Therein lies the value of developing a set of axiomatic principles upon which to focus the international debate on Internet governance.

This chapter does not suggest that the layers principle should become immovable and eternal Internet law. It does not suggest that it may be the only or most worthy principle — other principles can be developed, discussed and established. However, it does advance the idea that the layers principle and its corollaries are fundamental for establishing a rational and workable policy and regulatory framework for Internet governance. More broadly, this chapter advises policymakers that these principles are vital for building out an Internet that promotes economic democracy and innovation opportunity for all. This notion should be of particular concern for developing nations sizing up the development potential presented by information and communication technologies (ICTs). While wealthy nations could conceivably afford to occasionally use network technologies or implement governance policies that occasionally violate the layers principle, developing countries may find such a practice to be costly and detrimental to building their information societies and closing the digital divide.

The governance policy and regulatory concerns are important when we consider that eventually all ICTs will converge into the Internet (Werbach, 2002). The question is: do we recognize the value and contribution of the Internet and do we understand the role of its layered structure and open standards in permitting this amazing development of the global digital network? If we do, the only possible conclusion is that all other converging applications, such as broadcast and cable television, radio and telephony, should be guided to assimilate the Internet's qualities. Conversely, the Internet should firmly resist becoming more like these old technologies and policy should support this. This also implies a move away from governing and regulating by type of service, infrastructure or geographical reach.[2] Most importantly, it entails a conscious decision to explore network communications layers as the basis for governance policy and regulation.

The discussion that follows owes much to the analysis developed by Werbach (2002, 2004) Solum and Chung (2003), Kruse, Yurcik and Lessig (2000) and Benkler (2000). After developing the concept of the layered Internet, the chapter will develop the layers principle while reflecting on supporting principles and corollaries and addressing criticism. The chapter will then examine more closely the nature of the layers principle from the perspective of its use in decision-making in policy and regulatory environments. The chapter will end with a discussion on the need for integrating the above notions into the post-WSIS Internet Governance Forum (IGF) process.

B. Layers and the Internet architecture

1. Protocols and layers

The origin and development of the Internet have been explained and discussed in many reference sources. Readers are invited to consider, in particular, "A brief history of the Internet" (Internet Society, 2003)[3] for more details. This chapter will, however, avoid developing a historical perspective on the architecture of the Internet.

The Internet is still changing and its underlying technology and practical uses will evolve with increases in bandwidth and convergence of various delivery technologies and media, as well as with the development of new applications. The economics will change accordingly and interaction, and sometimes conflicts, between those that provide content, delivery pipes and attention will lead to new business models and environments. Attention providers — the online public audience at large — are of particular significance in this equation as online advertisement revenue continues to grow in importance for many enterprises.[4]

While nothing stays the same, the fundamental technical structure of the Internet acts as a springboard for change. More specifically, it is the Internet protocol suite that provides the stability of the Internet. It is often called the TCP/IP suite, a name combined from the abbreviations of the two most important components in the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). However, the TCP/IP suite also includes many other protocols such as those that are used for file transfer (FTP), e-mail transmission (SMTP) or hypertext transfer (HTML), to name but a few. Fortunately for the non-technical user, this multitude of contemporary protocols has become completely opaque, as many Internet applications, such as web browsers and e-mail clients, have been designed to engage any number and combination of these as required by the user. Annex I provides a selective list of Internet protocols.

The various protocols are often categorized in layers. Lower layers perform fundamental technical functions such as networking (establishing and maintaining connections among the many computers on the Internet) and transporting data. Upper layers provide application level functionality and rely on the lower layers to work reliably, but are purposefully independent. In a particular layer, functionally equivalent protocols, and the software applications that use them, can be substituted for one another without any adjustment being required in the protocols and applications that function in a layer above or below. This greatly reduces the complexity of the Internet protocol suite and increases its robustness, as its components are not forced into predefined linkages. Rather, they communicate and process data as needed in order to achieve a final functional outcome: access to a website, the reception of an Internet-based media stream such as Internet television, Voice over Internet Protocol (VoIP) or a secure remote connection to a database such as a reservation system for an airline. It is important to remember that the Internet transfers all data, be it e-mail messages, financial data or an Internet telephone conversation, by dividing up the data files or streams into smaller parcels, called data packets, labelling their order for reassembly at the destination computer and giving them origin and destination addresses. The Internet protocol suite will use a particular combination of protocols to channel these packets to their destination as efficiently as possible, reassemble them and present them to the user, and call for repeat sending of certain data packets if these are lost or arrive in a corrupted state.

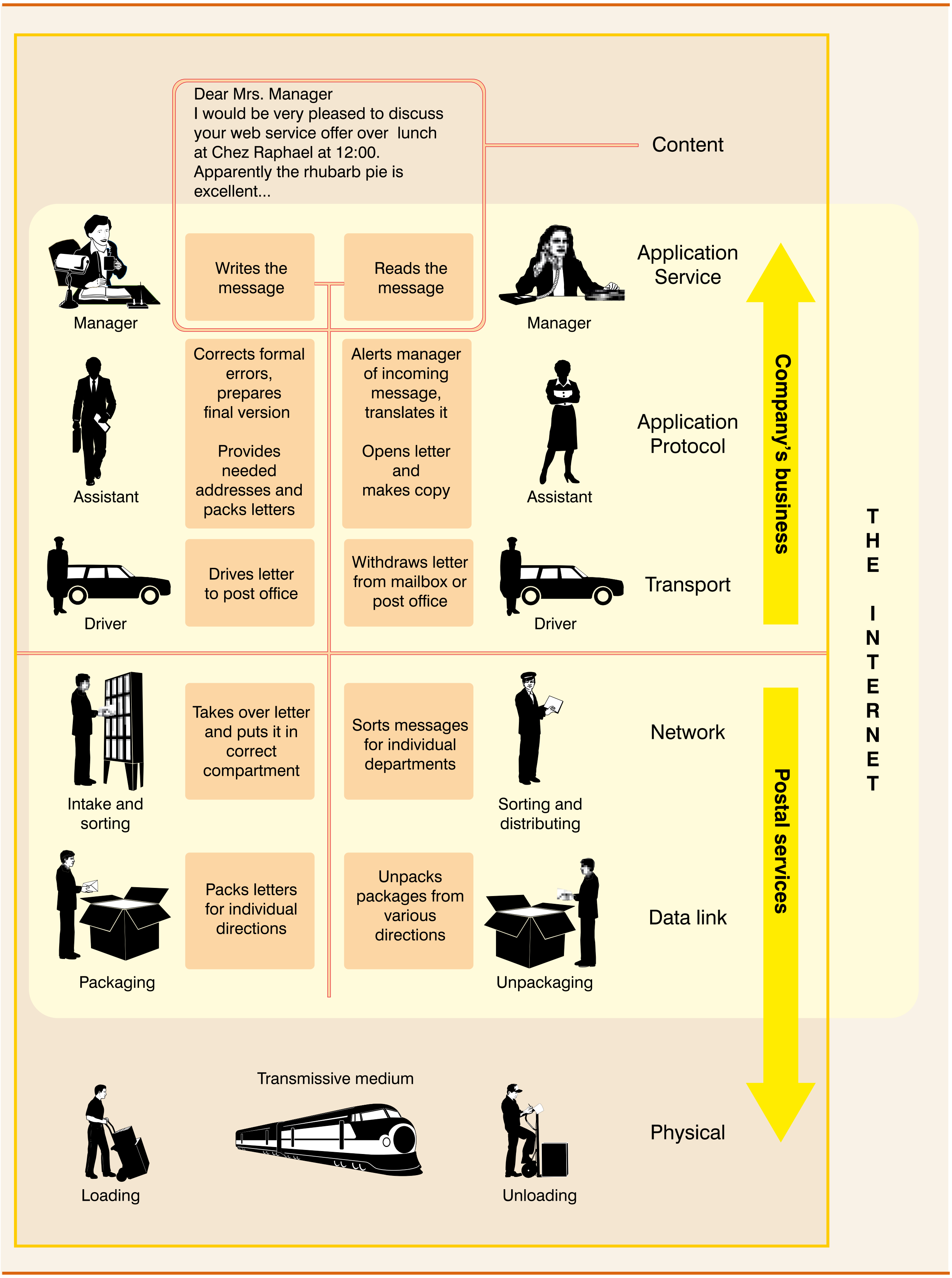
From a technical perspective, four separate layers of Internet protocols are often cited, in addition to the fifth lowest layer — the physical network layer of optic fibre or metallic cables and radio links, hubs, repeaters, and so forth. These are the data link layer, the network layer, the transport layer and the application layer. The TCP/IP suite merges the physical layer and the data link layer into a "host-to-network" layer and remains undefined in the suite as it varies from host to host and network to network (Tanenbaum, 1996).

The data link layer takes a raw digital transmission facility of the physical layer and transforms it into a connection that appears free of transmission errors. Senders break their data into data frames, transmit the frames sequentially, and processes the acknowledgement frames sent back by recipients. The data link layer corrects the errors and controls the flow of data between two adjacent nodes in a network. The network layer works to get data from the source network to the destination network. This generally involves routing packets that in their headers contain the sender's and recipients' Internet (IP) addresses across a network of networks — the Internet. The common protocol in the network layer is the Internet Protocol — the IP in the TCP/IP. The transport layer resides in between the application layer and the network layer and primarily provides the service of referencing applications on the senders' and the recipients' computers in order to provide coherence and reliability. It is the first end-to-end layer. All layers underneath the transport layer are concerned with connections of adjacent nodes in networks, while the transport layer is only concerned with the connection between the source and ultimate destination computers. The common protocol in this layer is the Transmission Control Protocol — the TCP in the TCP/IP. The TCP will typically ensure that data packets arrive correctly and in order, it will discard duplicate or corrupt packets and it will call for corrupted packets to be resent. Other transport layer protocols exist, besides the TCP, that are more suitable for telephony or streaming media. Finally, the application layer is the layer that most common Internet programs will work in, in order to communicate web pages, share files or data, or transmit or receive data streams. Chart 7.1 illustrates, in an analogy of communication between two businesses intermediated by a postal company, what happens at each layer of the Internet protocol suite.[5]

In many ways the layer structure described is similar to the International Organization for Standardization and the International Electrotechnical Commission standard Open Systems Interconnection (ISO/IEC OSI 7498-1 or just "OSI") model for networks.[6] It is also known as Recommendation X.200 of the International Telecommunication Union. The OSI was issued in 1984 and updated in 1994, and identifies

Chart 7.1

Internet protocol suite layers: A postal analogy



Dear Mrs. Manager
I would be very pleased to discuss your web service offer over lunch at Chez Raphael at 12:00. Apparently the rhubarb pie is excellent...

Content
Manager
Writes the message
Reads the message
Manager
Application Service
Assistant
Corrects formal errors, prepares final version
Provides needed addresses and packs letters
Alerts manager of incoming message, translates it
Opens letter and makes copy
Assistant
Application Protocol
Driver
Drives letter to post office
Withdraws letter from mailbox or post office
Driver
Transport
Company's business
Intake and sorting
Takes over letter and puts it in correct compartment
Sorts messages for individual departments
Sorting and distributing
Network
Packaging
Packs letters for individual directions
Unpacks packages from various directions
Unpackaging
Data link
Postal services
Transmissive medium
Loading
Unloading
Physical
THE INTERNET

seven layers with similar properties and functions as the Internet protocol suite. Without going into technical detail, the Internet suite can be understood as a special case of the OSI, even though it preceded it in practice. The OSI model is often used as a general and more comprehensive reference model from which others could develop detailed interfaces, which in turn could become standards. A fuller description of the OSI model is provided in annex II.

2. Internet layers and concepts

While the previous exposition of Internet layers and protocols is technically correct, analytically and from a policy and regulatory perspective, the discussion will need to redefine the layers in order to provide a conceptual, rather than technical, framework for exploring Internet governance issues. For the purpose of analysis, various authors have grouped the various layers slightly differently. This does not affect the analysis to a great extent, but it can create confusion. Thus it may be useful to review the various ways in which Internet layers have been bundled in recent literature.

Paralleling the technical definition of the Internet layers in section B.1 above, Solum and Chung (2003) define six layers: the physical layer, the link layer, the Internet Protocol layer, the transport layer, the application layer and the content layer. They note that the TCP/IP protocol suite is independent of the physical network hardware and that it is the link layer that is responsible for this freedom. The link layer exists in the form of device driver for a particular piece of network hardware. Using new hardware requires the development and installation of a new device driver that opens that hardware to the Internet protocol. In this way, the link layer enables the interconnection of the widest variety of disparate computer and network hardware, thus promoting competition and innovation. The Internet Protocol layer handles the movement of data packets around the network. The transport layer is where the files received from the application layer are broken up into data packets to be handed over to the Internet Protocol layer, and, moving in the opposite direction, the data packets received from the Internet Protocol layer are assembled into files to be delivered to the application layer. The application layer protocols are used to enable web communication, e-mail, file transfer and other functions more familiar to everyday Internet users.

Werbach (2002) suggests only four layers: the physical infrastructure layer, the logical layer, the applications layer and the content layer. Physical infrastructure consists of the underlying copper wire and optical fibre networks, terrestrial wireless and satellite communications. Setting up the physical layer usually requires substantial upfront investment. The owners, typically telecommunications companies, have often indicated that they are natural monopolies. While this is debatable, it has necessarily primed the physical layer as an obvious candidate for regulatory oversight and intervention.[7] The logical layer ensures the management and flow of data across the network. At the logical layer governance issues will typically be related to the functioning of the Domain Name System and the nature and role of bodies such as ICANN.[8] The application layer is where most end-user functions reside: web browser, Internet telephony, remote access to company Intranets, and so forth. Many of these applications used to be specialized services provided using proprietary infrastructure. Cable television or wired telephony are obvious examples. As the companies providing such services often own the physical infrastructure, and as the services are distinct, regulating by type of service seemed perfectly logical in the pre-Internet era. However, today this is becoming an increasingly dubious proposition given the ongoing technological assimilation of all services into the Internet. The content layer is the actual data or information made accessible by applications that depend on the logical layer as it uses the physical network to shift the content from providers to users. Historically, the regulatory treatment of content depended on the type of service — the content of a telephone conversation was often subject to different regulation from that of a television broadcast. However, the Internet does not distinguish between data packets of a VoIP or a video stream, and this causes regulatory conundrums. Is an e-mail circular to several hundred members of a particular club a private message or a broadcast?

Benkler (2000) proposes that we think of three layers. At the bottom of these three, there is the physical layer — the wires, cables and equipment that connect our computers. Above that is the logical layer that controls who gets access to what and what gets to run where; and above that, is the content layer — the actual substance of our communications. Each of the layers can vary in openness, ownership and control. The Internet is the most open digital communications network we have as its protocols and performance are neutral towards the contents of individual data packets, in spite of the fact that the physical network is largely privately owned and that there are many proprietary applications that are Internet-enabled. However, as the layers are effectively interdependent in the sense that we cannot

Chart 7.2
Conceptual layers of the Internet

Technical layer	Conceptual layers according to…			Subject[1]	Governance issues
	Solum and Chung	*Werbach*	*Benkler and Lessig*		
Content	Content	Content	Content	Text, data, graphics, audio, video, etc.	Spam, local content
Application services	Application layer	Application layer	Logical layer or the Code layer	Browsers, e-mail clients, anti-virus software, streaming media players, etc.	Data protection, privacy rights
Application protocols		Logical layer		HTTP, FTP, DNS, BitTorrent, etc.	Cybercrime
Transport (TCP)	Transport			TCP, UDP, etc.	DNS root server system
Network (IP)	Network			IP (IPv4, IPv6) etc.	IP addressing
Data link	Data Link			Ethernet, Wi-Fi	Stability
Physical network	Physical network	Physical network	Physical network	Binary transmission	Access, costs

[1] For definitions of various protocol acronyms see Annex 1.

achieve a successful communication if one layer does not function or cooperate, it is entirely feasible to take control of a particular layer through another and without owning it. The most obvious example is making public domain material — the content layer — accessible with a proprietary application — the logical layer. If such an application has a dominant market share, it can restrict use of public domain content and any attempt to lift such restrictions are illegal under the World Intellectual Property Organization's Copyright Treaty and counterpart national laws, such as the United States' Digital Millennium Copyright Act and the European Copyright Directive.[9] While the openness of the Internet is a matter of technological choice and is achieved through its layered architecture and open protocols, governance policy and the accompanying regulatory regime can affect this openness, both positively and negatively.

The differences in the above definitions are about how much the middle layers — in between the physical network and the content — are bundled. Solum and Chung unbundled them completely, while Werbach bundles the link, protocol and transport layers but leaves out the application layer that prepares content for users. Benkler bundles everything, observing that it is all a set of software protocols and applications. Benkler's logical layer is equivalent to the "code" layer of Lessig (2001), whereby how it is designed and how it performs are the de facto law of the Internet, and governance issues will necessarily relate directly to who designs, manages and owns particular parts of the "code" or logical layer. Recent developments show that control of the lowest physical layer also provides leverage for asserting governance. Network providers argue that high data volume applications, such as search engines, need to pay a premium for their disproportional use of bandwidth or that quality-sensitive services using streaming media desire and will pay a premium for transport priority, and suggest that their data will need to be tagged for priority, thus creating multiple data classes.[10]

Chart 7.2 gives a comparative overview of the different ways in which the layers can be rearranged into conceptual categories. The governance issues in the rightmost column are only indicative. Their actual placement in the layer should be the result of national and international policy processes and necessarily subject to ongoing examination. Technological progress, including the build-out of broadband networks as well as the development of new application protocols and services, may evolve particular concerns that are not apparent in the present circumstance. From a policy perspective, some issues may become irrelevant. Others may require relocation to different layers and new policy issues may arise as well.

3. Generating principles from layers

Establishing the relationship between the Internet architecture and governance should be treated as a matter of paralleling the layered structure with a corresponding policy and regulatory structure. The established linkages between technical layers and policy layers would serve as a kind of check and balance: social and political requirements, even when expressed legitimately, will need to consider the consequences. Similarly, any need for technical change should be subject to societal considerations. Requests and requirements would need to be debated and dealt with at the levels where they would be implemented. This empowers but also increases the shared responsibilities of the technological and political stakeholders in the process.

Not only is the understanding of Internet architecture essential to sound Internet governance, but also, vice versa, the development of new Internet technologies and innovation will need to embrace societal concerns as expressed through governance policy and practical regulation. Often, the issues will not be entirely new and will deal with the Internet versions of topics related to good governance and democracy, monopolies and antitrust law, problems of jurisdiction, intellectual property rights and many others. Besides the layers principle, a number of policy principles relating to Internet governance and policies have been advanced in the past and share many notions. However, they are not intellectually pedantic and, indeed, they may overlap or be directly derivative of each other or present a different viewpoint on the same or a similar issue.

The principle of layer-consistent Internet governance and the notion that minimizing of layer crossing in regulatory practice is a good thing, are often sourced to the work of Lessig (1999, 2001), where they appear as a discussion of the *code thesis* and the *end-to-end principle*. The *code thesis* states that the Internet is an artificial and engineered environment: humans design and implement it as they desire and to the extent that current software and hardware technology permits. The Internet does not have any natural properties. Its "inherent" nature is built into it through the design and implementation of its protocols and applications. For example, the only reason why the Internet seems to be exterritorial is because the logical layer does not distinguish data packets by geographical origin or destination.[11] This is a matter of how the protocols are written, and they can be redesigned to do otherwise. Thus, the sum of all the protocols and applications in the logical layer — the code — takes on some of the properties of a law, in the sense that it regulates the behaviour of Internet users.[12] Solum and Chung (2003) use the analogy of physical architecture — "just as the architecture of a building enables and encourages humans to move and congregate in certain ways, so the architecture of the Internet enables some activities by users and regulators while discouraging others".[13]

The *end-to-end principle* describes one of the key feature of the architecture of the Internet: the intelligence lives on the network periphery, in the application layer. In other words, functionality should be provided in the applications that are active in the application layer as used by users, but not by the network itself. This allows the logical layer to efficiently manage data transmission. The principle is sometimes described as a "stupid network" with "smart applications". As already noted, the logical layer does not, by design, discriminate or differentiate data traffic generated by different applications. Saltzer et al. (1981, 1998) argue that this lack of functionality encourages greater network reliability and decreases potential future costs of build-out and innovation.[14] Isenberg (1997) explains that the main advantages of the "stupid" Internet over the "smart" telephony network system derive from the fact that the Internet transport is neutral with intelligent and user-controlled endpoints. He also points out that its design is built on the notion of increasing and plentiful bandwidth and computing resources, while the transport is guided by the needs of the data – a particular combination of the many protocols and applications functioning in the logical layer will be engaged depending on the nature of the data being transported.

Most recently, the debate has continued through the discussion on *network neutrality*.[15] A network is neutral when it does not distinguish between the applications, or content, that depend on it, nor on the identity or nature of its users. Furthermore, entities operating a neutral network should not favour particular content or applications in order to gain a competitive advantage for certain types of services. If the Internet is to remain a platform for competing applications and content, it is important for the platform to remain neutral in order to ensure that competition is based on merit as expressed by users' preferences (Wu, 2005; Cerf, 2006). However, non-discrimination towards content and applications is a necessary but insufficient condition for network neutrality. A further condition is that of interconnection — network operators have the right to connect with other operators' networks and the obligation to accept connections and data from all other operators as well. A final requirement is that of open access. Not to be confused with similar issues in the technology and intellectual property debate, open access means that any end-user can connect to any other end-user, even when these are using a different network operator's infrastructure. Box 7.1 describes policy thinking and processes regarding the neutrality debate in the United States.

Box 7.1

Network neutrality in the United States: Policy processes and regulatory wisdom?

In February 2004, the Chairman of the Federal Communications Commission (FCC) of the United States, Michael Powell, proposed a set of non-discrimination principles. The principles of "Network Freedom" stated that Internet users in the United States must have the following four freedoms:

1. Freedom to access content;
2. Freedom to run applications;
3. Freedom to attach devices;
4. Freedom to obtain service plan information.

Later, in August 2005, his successor, Kevin Martin, restated these four freedoms in a FCC policy statement on "New Principles Preserve and Promote the Open and Interconnected Nature of Public Internet", as follows:

1. Consumers are entitled to access the lawful Internet content of their choice;
2. Consumers are entitled to run applications and services of their choice, subject to the needs of law enforcement;
3. Consumers are entitled to connect their choice of legal devices that do not harm the network; and
4. Consumers are entitled to competition among network providers, application and service providers, and content providers.

An often-cited positive case for network neutrality is when in early 2005 the FCC imposed fines on a local telephone carrier that was blocking voice-over IP service.[1] While awareness about the network neutrality issue has grown during the current debate, it is interesting to note that the United States Government has not codified this policy, but prefers that the FCC uses these principles in its ongoing policy activities. Clearly, policy may not need to translate into codified regulation, and recent developments proposing amendments to the United States Telecommunications Act of 1996 include advice to the FCC urging it to study and be alert to abusive business practices, such as discriminating against particular services, but do not propose specific language for network neutrality regulation.[2] However, during 2005, various civil society organizations and Internet-based businesses have been urging lawmakers to include Internet neutrality legislation in the revision of the Telecommunications Act, but without apparent success. The formal debate in the United States Senate is expected to resume in October 2005.[3]

[1] See the news story at http://news.com.com/2102-7352_3-5598633.html; the FCC decision is filed at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf.

[2] See http://commerce.senate.gov/pdf/06telcom.pdf.

[3] See http://news.com.com/Net+neutrality+fans+rally+in+25+cities/2100-1028_3-6111489.html

It is essential to keep in mind that the technological framework came first: most political, economic or sociological analysis has been an afterthought trying to make sense of the Internet, because it needs to be understood by policymakers in order to be governed. This holds true even if the policy conclusions mandate a deregulated approach. The effect of the layered structure of the Internet, first and foremost at a technical and functional level, is to liberate innovation and creativity on the Internet and substantively level the playing field for new entrants with designs and visions for ground-breaking uses and applications. Because the Internet's intelligence lives in the application layer, innovation is decentralized and the opportunity to devise new applications is available to all creative individuals with Internet access.

Unsurprisingly, many remarkable Internet projects, such as the Yahoo and Google portals, eBay.com, the Apache web server and Skype, to name but a few, started out as small projects conceived by motivated and creative individuals. End-to-end design, open protocols and transparent layers mean that innovators need only invest in developing software to run in the application layer. The application layer itself exists on every computer that has an Internet connection and does not enter into the cost of innovation. Innovators do not need to register their applications with any institution as the logical layer takes care of compatibility on its own — if innovators do not design their applications to respect the public TCP/IP protocols, their applications will simply not work. Box 7.2 highlights the importance of ensuring that the Internet continues to provide an open and accessible commercial development platform for technology companies and innovators from developing countries.

Entry barriers are further reduced because transparent layers turn consumers' computers into general-purpose Internet appliances. This means that a consumer need only invest in the software application itself in order to make use of it. This is in stark contrast to, say, the telephony system, where additional functionalities require the user to buy a more sophisticated telephone appliance or contact the telecom operator in order to subscribe and configure a centralized service, such as a voice mail box.

Another interesting issue is the notion of network effects, whereby the value of an application will increase with the number of users, all else staying the same. For any network technology there is a tipping point in the rate of adoption when application becomes sufficiently valuable to broaden its appeal from early adopters to ordinary users. Reducing the cost of adoption increases the likelihood that these networking effect gains will be realized, and realized earlier. If costs are too high for early adopters, the tipping point may never be reached. Thus the economic contribution of layer transparency and the end-to-end nature of the Internet are fundamental for innovation. Without it, motivation among inventors and investors would be lacking.

Nowhere is this more apparent than in the market for anti-virus and desktop security products. This particular product is interesting because security concerns have increased exponentially, with virtually every computer being connected to the Internet. A significant number of successful companies are not from the technology leader — the United States — and while their installed base and growth are unlikely to threaten and uncrown the market principals, Norton/Symantec and McAfee, their existence speaks of potential and possibilities. Table 7.1 provides a list of companies that are managing to compete with the dominant vendors precisely because the Internet provides a neutral, open

Box 7.2

Competition, choice and Internet governance [1]

The choice of the correct technology is fundamental to strengthening the ICT strategies of any company or institution. The Internet is central to making this choice because it allows Brazilian information technology companies to develop and innovate a range of products and services while relying on the established parameters of the Internet protocols. In this sense, the IT sector in Brazil is on equal terms with global ICT providers. Within our region, we can even generate advantages over global technology suppliers by providing a credible, secure and trustworthy relationship to our clients, built upon our long experience in the Brazilian information technology market. The Brazilian IT environment is a sophisticated and very competitive marketplace, reaching $12 billions in yearly sales volume. Almost all of the IT global players have operations in Brazil, increasing the level of local competition to higher standards.

The Internet governance issue is important for technology businesses that rely on the Internet protocols and network infrastructure being kept operational, transparent and non-discriminatory. This is important across all types of commercial activities, but in particular for application development, where highly trained teams are designated to develop and implement custom-made solutions and meet the requested technological requirements of domestic and international clients. In the application development, Brazilian software companies have developed strong competencies in several business areas, such as finance and bank automation, telecommunications, health and small and medium size enterprise business management software. Information technology security, e-business and e-government applications are also delivered to the highest international standards of quality and sophistication. While it is entirely feasible to produce such applications for proprietary data networks and protocols, developing and running them using the public protocols of the TCP/IP suite brings out the competitive advantages of Brazilian technology businesses and improves the scope of choice for its clients.

Therefore, Internet governance should work to secure open functionality and access to the Internet as a commercial data network and as an innovation catalyst. It should work to limit the danger posed by, and the harm done by negative by-products such as spam, cybercrime or viral attacks. It must do this in cooperation with the technology industry. Many of the problems may be mitigated, if not resolved, with specific and tailored applications or technology strategies that can be developed and delivered by the Brazilian software industry. Cooperation is particularly important in security issues because, in the final instance, software products and services will be dependent on the overall stability of the Internet.

[1] This commentary was provided by Djalma Petit, Business development coordinator of Softex, Brazil. SOFTEX is a Public Interest Civil Society Organization that promotes the growth and extension of the Brazilian software industry. Its work is directed at creating business opportunities, attracting investors and consolidating the image of Brazil as a software producer and exporter.

Table 7.1

Selected examples of international anti-virus software producers

Name	Country	Website
Virus Chaser	China	www.viruschaser.com.hk
Rising Anti-Virus Software	China	www.rising-global.com
F-Secure	Finland	www.f-secure.com
F-Prot	Iceland	www.f-prot.com
BitDefender	Romania	www.bitdefender.com
Doctor Web	Russian Federation	www.drweb.com
Kaspersky Anti-Virus	Russian Federation	www.kaspersky.com
NOD32	Slovakia	www.eset.com/
Panda	Spain	www.pandasoftware.com

and layered communications platform — their clients can install and test alternative products without any concessions to hardware providers, existing suppliers of anti-virus or other software and, lastly, the physical network operators.

4. Criticism of proposed principles

The arguments presented for developing governance policy principles, based on the notions of a layered, end-to-end and neutral Internet, are sometimes criticized as giving Governments an excuse to increase obtrusive and unnecessary regulation where market forces suffice. Moreover, Yoo (2004) argues that principles such as the end-to-end concept should not be necessarily translated into regulatory mandates as this could "become the source of, rather than the solution to, market failure. Such considerations are particularly problematic when the industry is undergoing dynamic technological change...". Regulating the Internet to conform to open standards and principles is often opposed by the operators of the physical layer. Arguments range from suggesting that network neutrality principles may translate into a more intrusive regulation of the Internet to the notion that codifying open protocols will disadvantage companies that want to differentiate their services by, among other things, using alternative proprietary protocols that will favour certain applications or services over others. For example, certain ISPs may want to specialize in e-mail services, while other would be more interested in providing streaming media, and others still may stay with providing generic Internet connectivity.

Critics will also argue that proposing additional or new regulation unnecessarily complicates the existing and fairly evolved regulatory frameworks for telecoms and goes against established regulatory modes that are, by and large, by type of service. This could require the re-regulation of all services, operators and communications infrastructures — a time-consuming activity with an ambiguous outcome. Finally, some critics maintain that the Internet has succeeded in becoming a global innovation platform and has outgrown and out-competed the proprietary data networks precisely because it has been free from government regulation, as opposed to the highly regulated telephony market. Thus, there is no real practical reason to explore the introduction of new regulation. On the contrary, any attempt by Governments to regulate the Internet, including by those with a genuine intention to preserve its neutrality, carries the risk of breaking it.

There are many ways to answer the criticisms and, indeed, several have already been pre-empted in the previous sections of the discussion. However, two issues need to be clarified in particular. The first is the notion that the Internet developed because it was not regulated or, at least, not overregulated. While the technological development was guided by practical concerns, the commercial build-out has been dependent on user demand that was fuelled by freedom of choice. These freedoms have been safeguarded precisely by telecom regulations that have ensured consumer access to competing ISPs, the possibility to use a wide range of competing hardware and software platforms, and a multiplicity of application, services and content. Such telecom regulation, often described as non-discrimination, is a precursor to Internet network neutrality and is still valid today as last-mile access to most consumers is physically dependent on the network operator that is often the historical incumbent and has a favourable, if not monopolistic, market position.

The second issue relates to the criticism that embracing a set of principles necessarily leads to their codification in some form of regulation. A basic principle for considering codification is that activities that result only in a certain loss should be formally regulated. However, this is not an exclusive principle. In this sense it is the law in many countries that automobile passengers must wear seat belts: there is no conceivable benefit at the level of society in not wearing one. Similarly, financial services companies are required to establish minimum capital reserves of various levels: avoiding this obligation will eventually lead to the failure of a number of institutions with consequences for clients, shareholders, staff and management. Policymakers should be aware that in between general principles and hard law there is a range of options and policy mixes that embrace varying degrees of education, policy awareness building, capacity building, economic incentives, self-regulation, supervisory activities and, finally, regulatory and legal processes. Whatever the policy tool, each and every one should be subject to review by referencing it to the layers principle and it corollaries.

C. Layers principle and policy concerns

1. The layers principle as a policy source

Having, we hope, conveyed the wisdom of maintaining a layered, and therefore neutral, open and transparent Internet, we will now develop a more detailed exposition of the layers principle in order to enable policy conclusions for Internet governance to be drawn. The discussion will largely follow that of Solum and Chung (2003). In essence, the layers principle states as follows: respect the integrity of Internet layers. In other words, Internet governance policy and regulation should avoid interfering with and changing the layered nature of the Internet architecture. This principle can be devolved into two arguments: the principle of layer separation and the principle of minimization of layer crossing.

The principle of layer separation states that the separation between Internet layers as designed into its basic technological architecture must be maintained. This means that policy or regulation that would require one layer of the Internet to differentiate the handling of data on the basis of information available only at another layer should be disallowed. In practice, the principle of layer separation would proscribe any policy or regulation that requires network operators to filter and censor data packets coming from a particular application, such as VoIP, P2P file-sharing or e-mail.

The principle of minimizing layer crossing states that governing authorities primarily use or develop policy or regulation for content or activity for a particular layer that is meant to be implemented precisely at that same layer. However, as this may not always be feasible, governors should minimize the distance between the layer at which policy aims to produce an effect and the layer directly targeted by the policy or regulation. The notion of distance is related to the proximity of technological or conceptual Internet layers as explained in box 7.1 and chart 7.1. In this sense, the maximum distance would be that between the physical network layer and the content layer. Adjacent layers, such as the content and application layers, are “nearby”. In this sense, the “greater the number of layers crossed, the worse the regulation; the fewer the layers crossed, the better the regulation”.[16] An example of a policy that violates this principle would be a regulation addressing copyright issues by requiring action at the IP layer by blocking of certain Internet addresses. Another example would be addressing bandwidth congestion by blocking of port assignments that are used by high-bandwidth applications.

The layers principle does not intend to provide a general theory of Internet governance and relevant regulatory policy. It aims only to support governing authorities with two bottom-line parameters that need to be considered each and every time a particular governance policy or regulation is proposed. This begs the question: do we actually need a comprehensive theory of Internet governance and regulation? UNCTAD (2005) has argued that as the Internet is a platform for many existing human activities, in at least the first instance, the policy, governance and regulatory goals that apply to those activities as conducted outside the Internet should also apply to the Internet. Any comprehensive regulation of the Internet should be very proximate to the existing and accepted notions of legal and political theory in general. In this sense, redesigning policy and regulation for many activities that have to some degree moved online may be inefficient.

The layers principle should be a sufficient criterion for evaluating most policy or regulatory proposals for Internet governance. However, governing authorities should, especially when in doubt or when issues are ambiguous cross-reference with the related principles as presented in part C.3 of this chapter. Where layer violation is justified, governing authorities should choose that policy or regulation that proposes crossing the fewest layers in order to achieve the policy objective.

An alternative to associating Internet governance policy and regulation with the layers principle and related corollaries would be to establish judgement on a case-by-case basis, analysing the net outcome of the expected costs and benefits of a particular policy. While this approach may have a common-sense appeal, it also presents several problems. The first is that the cumulative impact of multiple decisions may be different from a mere sum of the individual impacts, and this notion may not enter the decision-making process. One possible reason could be the growth of network effects, during the period when individual decisions were taken, which substantially change the assumptions. While adjusting for changing assumptions may be workable for each policy case on its own, after a cumulative policy outcome has been reached, a full rollback of policy and regulation may prove difficult if the cumulative network effects are judged undesirable. The other is that the fundamental premises of the issue may be severely affected by the actual case-by-case judgements. For example, regulators may mandate one or several changes in the TCP/IP suite that decrease its layers separation and users may be able to develop a workaround or a tolerable compromise. However, the cumulative effect of a larger number of layer violations may produce a threshold that becomes a significant disincentive to programmers and innovators seeking to fix, upgrade or develop new applications and online activities.

A case-by-case approach may not be well suited where the risks to innovation due to a change in Internet architecture and as a result of policy or regulatory activity are very difficult to estimate. Compounding the problem is the lack of institutional and human capacity to consider the impact of Internet governance policy and regulation on its ability to provide an accessible ICT innovation platform. While understanding the purpose, structure and functions of the Internet architecture is not impossibly complicated, policymakers are more likely to make good decisions by respecting the layers principle as a general rule and cross-referencing it with its corollaries, while using a case-by-case assessment of the effects of particular policies and regulations as a component of, rather than a decisive input into, the policy process.

Developing such a capacity anywhere, and not the least in developing countries, would mean establishing national governance and regulatory institutions such as those found in the financial sector, medical profession or the food and pharmacological industry. The report of the WGIG specifically states that "resources have not been available to build capacity in a range of areas relevant to Internet management at the national level and to ensure effective participation in global Internet governance, particularly for developing countries".[17]

Aside from the usual problems of sources of funding, length of political decision-making processes and a pending debate on the scope and depth of assigned duties and powers, a particular problem is that the Internet is a general-purpose technology. Thus the governance problems would not have a specific sectoral focus but would, as noted earlier, face a diversity of issues from intellectual property disputes to electronic commerce security, and on to human rights problems such as freedom of speech and privacy. This would be unfeasible as it risks questioning the policy and regulatory authority of existing governing and legal institutions.

These notions extend to the international policy level as well. The post-WSIS governance debate continues through a newly founded institution, the Internet Governance Forum (IGF). The IGF should be supported in debating and establishing a set of principles for Internet policy and regulation. The layers principle and the associated principles of the end-to-end, transparent, open and neutral Internet should be considered foundational as they can ensure that the Internet remains an open and accessible innovation platform that promotes a democracy of opportunity not yet witnessed in the history of technological development.

2. Policy concerns and perspectives

The established linkages between the technological Internet — its layers of open protocols and applications — and its rationalization through a set of principles need to be reconciled with existing governance policy and practice. A number of questions arise at this point. One is: how would new regulation interact with existing regulation? Looking at the layers, many countries should be able to identify regulation that could apply to the physical layer in the form of telecom regulation. Also, there may be regulation content either from the perspective of ethics, moral codes and conventions, privacy and freedom of expression, or by analogy with the perspective of broadcasting. Another question would be: does one codify the logical layer or behaviour in the logical layer? What are the actual Internet governance concerns? It may be worthwhile to consider the actual issues that have made Internet governance a major debating point at WSIS. Table 7.2 lists major issues of Internet governance concern in four Asian developing countries.

D. WSIS, Internet governance and principles

The discussions on Internet governance became a central focus during the WSIS process. The process itself consisted of two summit meetings, held in Geneva in December 2003 and in Tunis in June 2005, as well as of a series of preparatory meetings,[18] and, specifically on governance issues, the work and output of the Working Group on Internet Governance (WGIG) and the subsequent establishment of the Internet governance Forum (IGF).[19]

The Geneva summit in 2003 provided an unambiguous indication that Internet governance issues were clearly the domain of public policy as devised and implemented by Governments at a national level, and as negotiated and resolved among Governments at the international level.[20] In order to develop a framework and strategy

Table 7.2

Internet governance concerns in selected Asian countries and in the WSIS process

		China		India		Pakistan		Thailand		WSIS public policy concern
	Regional rank average	% dissatisfied	local rank	% dissatisfied	local rank	% dissatisfied	local rank	% dissatisfied	local rank	
Cybercrime, online fraud	1	100.0	1	95.0	2	89.3	3	96.4	2	✓
Virus attacks	2	100.0	2	94.4	3	90.9	1	98.2	1	
Spam	3	96.2	3	95.6	1	90.9	2	94.6	3	✓
Illegal content	4	84.9	5	84.9	4	85.1	4	78.6	4	
Privacy online	5	85.8	4	62.7	12	62.8	8	64.3	5	✓
Availability and cost of Internet	6	56.6	10	80.5	5	52.1	11	40.4	12	
Wireless Internet: Spectrum and access	7	55.7	11	66.0	11	63.6	7	54.4	6	
Reliability and speed of Internet	8	68.9	6	75.5	7	56.3	10	36.8	13	✓
Online access to government information	9	68.6	7	76.1	6	57.9	9	48.2	7	
Availability of local language software	10	26.9	21	60.4	13	48.8	13	43.9	9	
Availability of local content	11	32.7	20	53.2	16	44.5	16	45.6	8	✓
e-Commerce payment systems	12	60.6	8	58.5	15	50.0	12	35.1	15	
Fair access to/protection of intellectual property	13	59.4	9	67.9	8	70.9	5	43.9	10	
Internet telephony (VoIP)	14	49.1	14	66.5	10	68.6	6	35.7	14	
Network interconnection/ backbone access	15	41.5	16	39.2	17	48.7	14	30.4	19	✓
ISP market conditions	16	47.6	15	67.1	9	47.1	15	33.9	18	
Secure server/encryption	17	55.2	12	60.1	14	37.6	17	42.1	11	
Access to technical standards and their adaptability	18	36.2	19	34.0	19	35.7	19	35.1	17	
Domain names with non-Roman character sets (IDN)	19	40.0	18	34.2	18	36.4	18	35.1	16	
Domain name management	20	40.0	17	32.7	20	34.5	20	26.3	20	✓
IP address allocation/management	21	52.4	13	29.3	21	27.4	21	23.6	21	✓
Own skills for using Internet	22	9.5	22	13.3	22	4	22	3.5	22	

Source: based on UNDP-Apdip (2005), WGIG (2005b).

for the Internet governance deliberations, the Geneva summit established a temporary body — the WGIG — that was mandated to define Internet governance, to identify the most relevant governance issues, to develop a consensus on the roles and responsibilities of Governments, international organizations, the private sector and civil society from both developing and developed countries, and finally, to prepare a report as an input for the Tunis summit, which was held in June 2005.[21]

The work of the WGIG and the resulting report, together with the deliberations during the preparatory sessions and at the Tunis summit, further increased the profile of the Internet governance issue. While it can sometimes be difficult to judge the substance and quality of intergovernmental discussions on the basis of their documentary outputs, in terms of pure quantity the Tunis summit statements on Internet governance are roughly seven times longer than the Geneva outcome. In relative terms, the Internet governance component in the summit outcomes increased from around 4 per cent in Geneva to 30 per cent in Tunis.

A large number of analytical contributions were made in an attempt to provide a breadth of consideration, but also to influence the process. MacLean (2004) and Drake (2005) provided an insight into the detail of the concerns and discussions. They engaged the opinions of the direct participants in the WGIG and successfully drew attention to the large diversity of views and proposals and the varying principles and politics that underpin them. This was a positive contribution to the formal process and the outcomes of the WGIG and the Tunis summit in the sense that enquiring readers may seek out the root arguments and proponents for many of the positions taken, as well as the consequential compromises that became the foundation for the work of the IGF after WSIS. The WGIG also publicly released the background document, which was not negotiated and not subject to consensus acceptance, but served as the foundation of its final report.[22]

The WGIG final report, formally entitled the Report of the Working Group on Internet Governance, is a concise document focused on addressing a subcomponent of one key WSIS principle: the provision of a stable and secure infrastructure.[23] In its introduction it underscores the notion that "the WGIG was guided primarily by the key WSIS principles. In particular, the WSIS principle relating to the stable and secure functioning of the Internet was judged to be of paramount importance"[24]. It goes on to perform one of its key tasks — to define Internet governance:

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

The stated notion of shared principles, norms, rules and decision-making procedures does not, however, reappear to any significant extent in the continuation of the text, which is preoccupied with developing a list of Internet governance public policy issues and producing a proposal regarding who does what, addressed to governments, the private sector and civil society. This is not surprising given that the referential segment on principles in the WGIG background document is fairly brief, while admittedly to the point. In the main, it is the last bullet point of paragraph 24, and paragraph 25 that suggest the following:

> The end-to-end principle: the neutrality of the Internet, chiefly concerned with the effective transportation of packets, enables its intelligence to reside largely at the networks' ends through applications in computers, servers, mobile and other devices. This has enabled the development of a wide range of new ICT activities, industries and services "at the ends" and turns the Internet into an important tool within the wider context of economic and societal development. …Any proposal for change would have to assess whether any of these elements, which are important for the functioning of the Internet, would be affected in one way or another.

Thus the consideration of a set of principles for governance as a key public policy issue, which will serve as a reference framework for considering all other policy issues and can provide guidance as to acceptable or hazardous levels of policy interference in the Internet architecture, has been left open. It is now up to the successor to the WGIG — the IGF — to consider the need to re-establish the issue of instituting foundational principles for Internet governance. The first meeting of the IGF will start on 30 October 2006 in Athens. The provisional agenda calls for a debate on, among other issues, Internet governance and development, and in particular the notion of openness. While these can provide a handle to initiate discussions on establishing governing principles, at the time of writing it is difficult to predict how the deliberations will develop. The current UNCTAD Information Economy Report will be in print at the time of that meeting and may need to consider a follow-up to the IGF process in its 2007 edition.

Table 7.3
Thirteen DNS root servers

Letter - Name	Operator	Location
A	VeriSign	Virginia, USA
B	ISI University of Southern California	California, USA
C	Cogent Communications	Distributed using anycast
D	University of Maryland	Maryland, USA
E	NASA	California, USA
F	Internet Systems Consortium	Distributed using anycast
G	US Department of Defense	Ohio, USA
H	US Army Research Lab.	Maryland, USA
I	Autonomica	Distributed using anycast
J	VeriSign	Distributed using anycast
K	RIPE NCC	Distributed using anycast
L	ICANN	California, USA
M	WIDE Project	Distributed using anycast

Source: Internet Society (http://www.isoc.org/briefings/019/)

The Tunis summit itself, aside from considering the WGIG final report and mandating the IGF, conducted an energetic discussion on the Internet governance theme. Many delegations from developing countries felt that the United States Government, mainly through the relationship between its Department of Commerce and ICANN, had too much influence in managing the Internet.[25] Furthermore, some developing countries argued that the fact that the 13 domain name root servers were all located in the developed world — several are controlled by United States Government or military institutions — in itself posed a threat to the Internet's alleged global, open and accessible nature. Table 7.3 provides an illustrative list of DNS root server locations.

At first sight, it seems that few DNS root servers are located outside the United States. The M server is operated by the Widely Integrated Distributed Environment (WIDE) Project in Tokyo, and the K server is managed by Amsterdam-based Réseaux IP Européens Network Coordination Centre (RIPE NCC). Autonomica is based in Sweden. Several of the listed servers are using the anycast protocol to point to many addresses around the world, accessing 80 server locations in 34 countries, including many developing countries.[26] It is interesting to note that the anycast[27] protocol has been implemented without much ICANN involvement, without a formal policy process and without official consultations with the US Department of Commerce (Peake, 2004).

Developed countries, and in particular the United States, countered mainly by suggesting that the Internet governance system, narrowly defined as a set of technical coordination activities such as those carried out by ICANN, was not broken and therefore that while ICANN itself could benefit from reform, it did not need replacing with new or existing institutions, in particular not those from the United Nations system. They also affirmed their conviction that a deregulated, private-sector and market-based model for the build-out of the Internet was and would still be more efficient and effective than a top-down regulated environment aimed at balancing diverse national interests through regulatory measures that consider the Internet to be a public service.[28]

The compromise position was reached by adopting a set of agenda points. These had several outcomes. One was the previously noted establishment of a discussion platform, namely the IGF. Another was the introduction of a set of soft principles advocating that the Internet governance processes be multilateral, transparent, democratic and open to all stakeholders. These principles are positive and difficult to criticize. While they describe an ideal process of governance, they do not provide references for analysing concrete Internet policy or regulatory proposals. In this sense, they have crowded out the consideration of Internet-specific principles, such as the layers principle, the end-to-end principle or the network neutrality principle, discussed earlier in this chapter.

Finally, the process has produced a set of public policy issues. These are the administration of the root zone files and root server system of the Domain Name System (DNS), IP addressing, interconnection costs, Internet stability, security and cybercrime, spam, freedom of expression, meaningful participation in global policy development, data protection and privacy rights, consumer rights and multilingualism. While current at the time of writing, these issues may prove to be static and outdated because of technological development. Many also contain significant technological scope while the scope for policy reflection may be rather limited in the case of, say, spam, where there is a unanimous agreement that it is undesirable, the real problems being a lack of resources and capacity, rather than an evolved policy framework. The WSIS requested the IGF to consider these issues and present the discussions and outcome to the UN Secretary-General, who will report periodically to the UN member States on the Forum's operation.

While the WSIS and WGIG processes have produced a better understanding of Internet governance, what is needed is a point of convergence for the future deliberations of the IGF. A set of principles that would serve as policy and regulatory guidelines for Internet governance, such as the layers principle and its corollaries, are needed in particular if information society stakeholders see an advantage in further developing the Internet as a global, accessible and open communications platform and maintaining its positive relationship with technological innovation and economic and social development.

E. Conclusions and recommendations

The Internet is a truly remarkable technological platform. Barely a year goes by without our hearing yet again, of some extraordinary and innovative Internet development that is impacting on our social and economic life. Most recently, blogs have led the global media industry to re-examine its basic journalistic credos and principles. Wikis are redefining the scope and nature of communal knowledge development and have led to an examination of our understanding of encyclopaedic activities. Web services, discussed in some detail in chapter 6 of this report, may bring about a new burst of productivity growth among firms and economies. Online office software, torrent-based broadcasting, distributed always-on video telephony — what will be next?

A more interesting question is perhaps, who will be next? Individuals or small teams developed some of the most noteworthy Internet applications. These include Yahoo, eBay, Amazon, Google and Skype. Many free and open source software projects have been matured into world-class applications also by small teams, albeit with community support.[29] It is entirely conceivable that a globally important application will emerge from the sheds and bedrooms of tech-savvy youths from a developing country. Developing country Internet governance policy should therefore strategically support the build-out of national Internet infrastructure and should participate in strengthening its role as an open and accessible innovation platform through activities at national and international policy levels.

What all these technologies have in common is that they take advantage of several fundamental characteristics of the Internet. The first is that the TCP/IP suite takes care of itself. It is robust and reliable, but it does not interfere and treats all data equally — in fact, it cannot do otherwise because it lacks the necessary functionality and this is part of its purposeful design. The second is that it does not care about what applications are using it nor about the type of content they generate. The Internet does not care who the user is: it leaves this decision to the developer of the application. Finally, the Internet is a layered suite of public protocols where each layer performs a specific and separate function without concerning itself with the processes in other layers.

However, the Internet is a human product and its characteristics are not a given fact; rather, they are subject to change. While its present characteristics were designed by technologists, its future may be decided by governing authorities and policymakers. Thus, it is imperative that policymakers analogize the technical design values of the Internet into conceptual principles that define it and explain its success, from a social, political and economic perspective. Such principles can then be used in the process of governance. This may not be a simple notion nor an easily practicable process and many national and international political processes will shy away from this issue, preferring to deal with more observable manifestations such as problems with spam or cybercrime. To a certain extent, the Internet is a victim of its own success, having expanded so much and having become a locus of so many social and economic activities that Governments can no longer leave it alone. Society is moving online and with it its need to organize and govern.

Accepting that the need to govern the Internet is a given, a political fact of life, the question that follows is: how to go about it? A first and unavoidable step is to advance the dialogue between the technological and the political communities. This should be done at the national and international levels. Governments, in particularly those of developing and transition economies, should spare no effort to engage their scientific and academic communities, in particular those members that specialize in electronic and digital communications, and institutionalize a permanent dialogue on Internet governance issues. The learning process would be a two-way street. As much as policymakers may be unfamiliar with, say, the functions of various protocols residing in the transport layer, technologists may need to learn about issues of legitimacy, economic externalities and utilities above and beyond the concepts of technical functionality, effectiveness and efficiency. Such processes need to be reinforced at the level of international policy and the IGF needs to be challenged and supported in bringing the political and technological communities together in the Internet governance debate.

A further step for the IGF would be to formulate a key set of principles to serve as guidelines for Internet governance policy and regulation. This chapter proposes the layers principle because it reduces many other proposed principles to two arguments: does proposed policy require one layer to differentiate the handling of data based on information available in another layer, and does the proposed policy minimize the distance between the layer at which it is implemented and the layer where the outcomes are expected? However, many policymakers and technologists may choose instead, or in addition, the end-to-end principle or the network neutrality principle. They may also choose to develop a new principle from scratch or a derivative of existing notions. Whatever the case, this chapter suggest that policymakers should develop Internet governance policy based on a set of debated and agreed principles.

Finally, there will always be questions as to how far to go in codifying any of the proposed principles. The conventional wisdom is that activities that result only in a certain loss should be regulated. Does *not codifying* the Internet present society with situations of certain and unambiguous loss without any upside or possible benefits? This is a serious issue that will require much debate. At this point in time it would be safe to say that policymakers should consider the full spectrum of policy tools, including education, awareness and capacity building, economic incentives and self-regulation, before considering regulation.

Finally, the international community needs to extend the opportunity for technical cooperation on Internet governance issues to developing and transition economy countries and in particular to least developed countries. This will ensure that they fully benefit from the development opportunities provided by the Internet. It would also improve their ability to make a valuable contribution to the IGF and other international processes dealing with Internet governance in the post-WSIS era.

Annex I

A selective overview of protocols that make up the Internet protocol suite

Acronym	Description	Layer level
ARP	The Address Resolution Protocol (ARP) is the method for finding a host's hardware address when only its Internet Protocol address is known.	Network
ATM	Asynchronous Transfer Mode (ATM) is a cell relay network protocol that encodes data traffic into small fixed-sized cells, instead of variable-sized packets as used in the Internet Protocol or Ethernet.	Link
BitTorrent	BitTorrent is a file sharing protocol designed to widely distribute large amounts of data without the corresponding large consumption in server and bandwidth resources.	Application
DCCP	The Datagram Congestion Control Protocol is a transport layer protocol used by applications with timing constraints on data delivery, such as streaming media and Internet telephony.	Transport
DNS	The domain name system/server translates domain names to IP addresses and thus provides a global redirection service for the Internet, and thus is essential for its use.	Application
Ethernet	Ethernet is a networking technology for local area networks that has been standardized as IEEE 802.3.	Link
Frame Relay	Frame relay is an efficient data transmission technique. While IP-based networks have gradually begun to displace frame relay, in areas lacking DSL and cable modem services frame relay "always-on" connections provide a possibility for high-speed access.	Link
FTP	File transfer protocol is used for exchanging files over any network that supports the TCP/IP protocol, such as the Internet or an intranet.	Application
HTTP	Hypertext Transfer Protocol is used to transfer information on the World Wide Web by providing a standard for publishing and reading HTML pages.	Application
ICMP	The Internet Control Message Protocol is used to send error messages, indicating, for example, that a requested service is not available or that a host cannot be reached.	Network
IGMP	The Internet Group Management Protocol is used to manage multicast groups. It is used for online video and gaming.	Network
IMAP	The Internet Message Access allows a local client to access e-mail on a remote server.	Application
IP	Internet Protocol provides the service of communicable unique global addressing amongst computers. It is encapsulated in a data link layer protocol (e.g. Ethernet) and this relieves the data link layer of the need to provide this service.	Network
IRC	Internet Relay Chat provides instant communication over the Internet and was designed for discussion forums or one-on-one exchanges.	Application
NNTP	The Network News Transfer Protocol is used to read and post Usenet articles and to transfer news among news servers.	Application
POP3	The Post Office Protocol version 3 is used by subscribers to Internet-based e-mail accounts to access their e-mail on their local computers.	Application
PPP	The Point-to-Point Protocol establishes a direct connection between two nodes and many Internet service providers use PPP to give customers dial-up or DSL access to the Internet.	Link
RTP	The Real-time Transport Protocol (or RTP) defines a standardized packet format for delivering audio and video over the Internet.	Application
RUDP	The Reliable User Datagram Protocol is a transport layer protocol designed as an extended functionality UDP protocol that can provide guaranteed-order packet delivery.	Transport
SCTP	SCTP can transport multiple message-streams and operates on whole messages instead of single bytes.	Transport
SIP	Session Initiation Protocol enables initiating, modifying and terminating Internet connections for multimedia applications such as audio, video, instant messaging, online games and virtual reality.	Application
SMTP	Simple Mail Transfer Protocol is the standard for e-mail and Internet fax transmissions across the Internet.	Application

Annex I *(continued)*

SNMP	The simple network management protocol is used by network management systems for monitoring network devices for occurrences that require administrative attention.	Application
SSH	Secure SHell allows the establishment of a secure connection between two remote computers using public-key cryptography for authentication as well as confidentiality and data integrity.	Application
TCP	The Transmission Control Protocol is, together with the IP, a core protocol enabling exchange of data packets. It provides for reliable and in-order delivery, and enables multiple, concurrent applications to send data at the same time.	Transport
TELNET	The Telephone Network protocol provides a general, two-way communications facility and was designed to emulate a single terminal attached to the other computer using a telephone network.	Application
TLS/SSL	Transport Layer Security and Secure Socket Layer are cryptographic protocols for secure communications on the Internet. The protocols allow applications to communicate while decreasing the risk of eavesdropping, tampering and message forgery.	Application
UDP	The User Datagram Protocol allows programs on networked computers to send short messages, but it does not provide the reliability and ordering guarantees that TCP does. While packets may arrive out of order or go missing, UDP can be more efficient than TCP for time-sensitive applications.	Transport
Wi-Fi	Wi-Fi is a protocol enabling wireless local area networks (WLAN) based on the IEEE 802.11 specifications. Wi-Fi also allows connectivity in peer-to-peer mode; this makes it useful in consumer electronics and gaming applications.	Link

Annex II

The ISO/IEC Open Systems Interconnection model (OSI) is a framework describing how messages should be transmitted between any two points in a telecommunication network. It divides a telecommunications network into seven layers. When data pass only through a computer, on their way to a final destination, only the lower three layers — up to the network layer — are used. The OSI is a modular system that divides a complex set of functions into manageable and self-contained layers. In theory, this allows communication systems to independently develop and innovate applications at the various layers without a global redesign being mandated. The seven layers are:

Layer 1: The physical layer conveys the bit stream through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier.

Layer 2: The data-link layer provides synchronization for the physical level and furnishes transmission protocol knowledge and management.

Layer 3: The network layer handles the routing and forwarding of the data. This means sending data in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level.

Layer 4: The transport layer manages the end-to-end control — for example, determining whether all packets have arrived — and error-checking. It ensures complete data transfer.

Layer 5: The session layer sets up, coordinates and terminates conversations, exchanges and dialogues between the applications at each end. It deals with session and connection coordination.

Layer 6: The presentation layer is usually part of an operating system which converts incoming and outgoing data from one presentation format to another. It is sometimes called the syntax layer.

Layer 7: The application layer is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.

OSI represents a design paradigm for packet-switched network architecture and reflects the increasing level of use of such technologies. From a practical perspective, while extensive effort was invested in its promotion, OSI did not become a popular implementation, as it was not accepted by the communications industry, which favoured the TCP/IP suite.

References

Benkler Y (2000). From consumers to users: Shifting deeper structures of regulation toward sustainable commons and user access, *Federal Communications Law Journal* , vol. 52, no. 3.
http://www.law.indiana.edu/fclj/pubs/v52/no3/benkler1.pdf

Cerf V (2006). Network neutrality, presented at the hearing of the US Senate Committee on Commerce, Science, and Transportation.
http://commerce.senate.gov/pdf/cerf-020706.pdf

DiLorenzo TJ (1996). The myth of the natural monopoly, *Review of Austrian Economics,* vol. 9, no. 2.
http://www.mises.org/journals/rae/pdf/rae9_2_3.pdf

Drake W (2004). Reframing Internet governance discourse: Fifteen baseline propositions, Memo #2 for the Social Science Research Council's Research Network on IT and Governance.
http://www.ssrc.org/programs/itic/publications/Drake2.pdf

Drake W, ed. (2005). Reforming Internet governance: Perspectives from the WGIG, United Nations Task Force Series 12.
http://www.wgig.org/docs/book/WGIG_book.pdf

Interent Society (2003). A brief history of the Internet.
http://www.isoc.org/internet/history/brief.shtml

Isenberg D (1997). Rise of the stupid network: Why the intelligent network was once a good idea, but isn't anymore, Computer Telephony.
http://www.hyperorg.com/misc/stupidnet.html

Kruse H, Yurcik W, Lessig L (2000). The InterNAT: Policy Implications of the Internet Architecture Debate, Telecommunications Policy Research Conference - Agenda 2000.
http://www.tprc.org/abstracts00/internatpap.pdf

Lessig L (1999). *Code and Other Laws of Cyberspace*, Basic Books.

Lessig L (2001). *The Future of Ideas: The Fate of the Commons in a Connected World*, Vintage Books.

MacLean D, ed. (2004). Internet governance: A grand collaboration, United Nations Task Force Series 5.
http://www.epol-net.org/pport/pdf/465794058.pdf

Mitchell WJ (1995). City of Bits: Space, Place, and the Infobahn. MIT Press.

Peake A (2004). Internet governance and the World Summit on the Information Society (WSIS), Association for Progressive Communications (APC).
http://rights.apc.org/documents/governance.pdf

Saltzer JH, Reed DP and Clark DD (1981). End-to-end arguments in system design, *ACM Transactions in Computer Systems* vol. 2, no. 4, November 1984.
http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.txt

Saltzer JH, Reed DP and Clark DD (1998). Active networking and end-to-end Arguments, IEEE Network vol. 12, no. 3, May/June.
http://web.mit.edu/Saltzer/www/publications/endtoend/ANe2ecomment.html

Solum B and Chung M (2003). The layers principle: Internet architecture and the Law, Public Law and Legal Theory Research Paper 55, University of San Diego School of Law, California.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416263

Tanenbaum AS (1996). Computer Networks (3rd Ed), Prentice-Hall Inc.

UNCTAD (2002). *E-Commerce and Development Report 2002*, UNCTAD/SDTE/ECB/2.
http://r0.unctad.org/ecommerce/ecommerce_en/edr02_en.htm

UNCTAD (2003). *E-Commerce and Development Report 2003*, UNCTAD/SDTE/ECB/2003/1.
http://r0.unctad.org/ecommerce/docs/edr03_en/ecdr03.htm

UNCTAD (2005). *Information Economy Report 2005*: *E-commerce and development*, UNCTAD/SDTE/ ECB/2005/1.
http://www.unctad.org/en/docs/sdteecb20051_en.pdf

UNDP-APDIP (2005). *Internet Governance: Asia-Pacific perspectives,* Elsevier.
http://www.apdip.net/publications/ict4d/igovperspectives.pdf

Werbach K (2004). Breaking the ice: Rethinking telecommunications law for the digital age, *Journal on Telecommunications and High-Tech Law*, 2005.
http://werbach.com/docs/breaking_the_ice.pdf

Werbach K (2002). A layered model for Internet policy, *Journal on Telecommunications and High-Tech Law*, vol. 1, no. 37.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=648581

WGIG (2005a). Report of the Working Group on Internet Governance.
http://www.wgig.org/docs/WGIGREPORT.pdf or
http://www.wgig.org/docs/WGIGREPORT.odt

WGIG (2005b). Background report of the Working Group on Internet Governance.
http://www.wgig.org/docs/BackgroundReport.pdf or
http://www.wgig.org/docs/Background-Report.htm

Wu T (2005). Network neutrality, broadband discrimination, *Journal of Telecommunications and High Technology Law*, vol. 2.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

Yoo CS (2004). Would mandating broadband network neutrality help or hurt competition? A comment on the end-to-end debate, Vanderbilt University Law School Law & Economics Working Paper Number 04-04.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=495502

Notes

1. See Drake (2004).

2. Mobile telephony is a typical example: providers will have a licence for a specified type of service, such as GPRS or 3G, in a particular region or country, and will use identifiable infrastructure.

3. See http://www.isoc.org/internet/history/brief.shtml .

4. In June 2005, an Interactive Advertising Bureau and PricewaterhouseCoopers survey estimated that Internet advertising totalled over $2.8 billion for the first quarter of 2005; this made it the highest reported quarter in nine consecutive growth quarters and represented a 26 per cent increase over the first quarter of 2004 (http://www.iab.net/news/pr_2005_6_6.asp). For a more detailed discussion of online advertising see "Online Advertising Landscape, Europe" and "The Decade in Online Advertising, 1994-2004"; http://www.doubleclick.com/us/knowledge_central/ .

5. The diagram is derived from a graphic presenting the OSI reference model. The original was produced by Josef Sábl for Wikipedia and is available under the GNU Public Licence at http://en.wikipedia.org/wiki/Image:Rm-osi_parallel.png .

6. The full specification can be accessed at http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip.

7. DiLorenzo (1996) argues that monopolies in the telephony sector were created through government regulation instead of being a result of market failure.

8. See UNCTAD (2002), chapter 2, "The domain name system and issues for developing countries".

9. See http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html, http://www.copyright.gov/legislation/dmca.pdf , and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

10. See http://news.com.com/2102-1028_3-6058223.html .

11. This is not entirely correct. Data travelling on the Internet have origin and destination IP addresses associated with it; thus one can see where data come from, as the IP numbers give at least an approximate indication of where users may be located. However, the Internet uses these data only to manage the routing and transporting of the data. It is the applications that the data reach that then choose to interpret and use the data from a geographical perspective. For example, Apple iTunes refuses to sell music downloads to users not residing in the same domicile as the regional portal. Therefore, only French residents can do business with iTunes.fr. However, while the iTunes.fr website is an Internet-enabled e-commerce application, it is not strictly speaking the Internet — it merely uses the Internet. It is up to the website manager or programmer to choose to consider IP number information. The Internet itself does not do this other than in respect of routing and transporting data.

12. Lessig (1991, p. 5) ascribes the "code is law" notion to Mitchell (1995).

13. See Solum and Chung (2003, p. 13).

14. More specifically, Saltzer et al. (1998) state that "building complex function into a network implicitly optimizes the network for one set of uses while substantially increasing the cost of a set of potentially valuable uses that may be unknown or unpredictable at design time. A case in point: had the original Internet design… Preserving low-cost options to innovate outside the network, while keeping the core network services and functions simple and cheap, has been shown to have very substantial value."

15. See http://search.news.com/search?q=internet+neutrality .

16. See Solum and Chung (2003, p. 32, second para.).

17. WGIG (2005a, p. 6, para. 20).

18. The WSIS Second phase Prepcom-3 was the locus for developing the Internet governance debate in between the Geneva and Tunis summits; see http://www.itu.int/wsis/preparatory2/pc3/index.html .

19. For comprehensive documentation see the WSIS portal at http://www.itu.int/wsis/.

20. See Annex 3: Geneva Declaration of Principles, article 49.1.

21. In November 2004, Secretary-General Kofi Annan appointed 40 individuals from government, the private sector and civil society to the WGIG. However, many more people attended the WGIG consultations in Geneva, contributing their views and knowledge. Lists of participants, and papers and presentations submitted, are available at the WGIG website at http://www.wgig.org .

22. See WGIG Background Report at http://www.wgig.org/.

23. See WGIG Final Report at http://www.wgig.org/.

24. See WGIG (2005a), page 3, para. 6.

25. See http://rights.apc.org.au/wsis/2005/03/report_wsis_prepcom2.php , http://news.com.com/U.N.+says+its+plans+are+misunderstood/2008-1028_3-5959117.html , http://www.infotoday.com/newsbreaks/nb051121-1.shtml , or http://www.worldsummit2005.de/en/web/796.htm. Also see the Memorandum of Understanding Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.ntia.doc.gov/ntiahome/domainname/icann.htm .

26. See the Internet Society's "DNS root name servers explained for non-experts" at http://www.isoc.org/briefings/019/ as well as Root-servers.org for a complete list of server locations at http://www.root-servers.org/.

27. Anycast is a network technology that routes data traffic to the "nearest" or "best" destination in accordance with the routing topology. It can be used to provide redundancy and load sharing for particular Internet functions, such as DNS root servers; see http://www.net.cmu.edu/pres/anycast/.

28. An excellent description of United States policy can be found in Ambassador David A. Gross' testimony before the Senate Committee on Commerce, Science, and Transportation; see http://www.state.gov/e/eb/rls/rm/36700.htm .

29. See UNCTAD (2003) for a detailed analysis of the free software phenomenon.