

DiploFoundation

INTERNET GOVERNANCE RESEARCH PROJECT

**THE PROTECTION OF THE PUBLIC INTEREST
WITH REGARDS TO THE INTERNET**

(Document for Comment)

Research:

Seiiti Arata
Stephanie Psaila

Supervision:

Alex Sceberras Trigona
Andrei Mikheyev
Valentin Katrandzhiev
Vladimir Radunovic

ABSTRACT

The Internet has evolved on a much wider scale than the original project envisaged. It is no longer run and developed by the academic community, as now new stakeholders clash in trying to add their preferences in its future shape. This power struggle has to be dealt with by governance arrangements. Otherwise, the prevailing forces will not be legitimate.

Conflict among the stakeholders will hopefully be substituted by collaboration. The Internet Governance Forum has an important role in this respect, and other lessons from international law are hereby presented for consideration.

1. INTRODUCTION

“The Internet has evolved from a research and academic facility to a global facility available to the public.”

*(Tunis Agenda for the Information Society, par. 30)*¹

Instead of understanding the Internet as a fixed object, a better approach is to follow the Greek philosopher Heraclitus’ aphorism: *panta rhei* (everything flows). For Heraclitus, one can never step in the same river twice, for other waters are continually flowing in. Similarly, the Internet is never the same at two different moments, as it undergoes constant transformation.

We have to accept that the Internet as it is today differs significantly from what it was like in the beginning² and will probably be very different in the near future. As the Internet is a human creation, it is up to those involved in its crafting to decide the shape it will take in the future that will most benefit society, instead of favouring only some privileged parties.

The arrival of new stakeholders raises the possibility of clashes of interests. As the Internet is a global facility available to the public, its governance must be carried out in accordance with the public interest, and not subject to the influence of the most powerful actors.

This research will evaluate how the public interest can be best protected by ongoing Internet governance.

¹ <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

² The Internet started as a military project by the Advanced Research Projects Agency – ARPA, and was further developed by the scientific community. The World Wide Web and the popularity of the personal computer created sufficient network value for spreading the Internet throughout society. Since then, the Internet is much more user-friendly, and text-based and arcane commands are no longer necessary to enjoy most of its applications. However, the increasing concern for security and stability is pushing Internet development towards a new architecture in which some of the freedoms currently enjoyed by users may be curbed. For a brief history of the Internet, the Internet Society’s website is a good starting point: <http://www.isoc.org/internet/history/>.

2. THE PUBLIC INTEREST

2.1 Reaching a Common Definition

Although very easy to understand, the definition of the public interest is a challenging task. The public interest differs according to the “public” referenced. Accordingly, there are contrasting positions between domestic, national, and global public interests.

Due to the global character of the Internet, it is necessary to concentrate on the concept of the global public interest. To reach a worldwide consensus on what constitutes the public interest, a lowest common denominator has to be established.

Such is the practical problem faced in setting up global public interest protection, since most of the time it tends to be set through a lowest common denominator, as the consent of all global players is needed. Examples of issues generally agreed to be combated are war, piracy, terrorism, genocide, massive violations of human rights, and child pornography, among others.

However, for a wide range of interests, such as the freedom of speech and fair use as exceptions to copyright law, and data protection levels, countries’ views differ, and achieving consensus is hard if not impossible unless a lowest common denominator is called for. Unfortunately, this is not always enough to maintain the public interest at an adequate level.

On the other hand, two successful examples of international law achieving an adequate lowest common denominator are the Universal Declaration of Human Rights³ and the UN Convention on the Law of the Sea.⁴ A recent example also to be considered is the Kyoto Protocol to the United Nations Framework Convention on Climate Change⁵ and the adoption of the “Responsibility to Protect” concept on the 60th anniversary of the UNGA Resolution on 15-16 September 2005.⁶ These agreements attracted a considerable number of signatories because prior to consensus, discussions began with a general agreement about a public good that needed to be protected in the public interest.

2.2 Political and Philosophical Considerations

The notion of the public interest is an open and wide-ranging concept, used to evaluate the tendency of policies and institutions to promote the interests of the members of a society considered in their broadest relations; the rights of the public at large that are to be recognised, protected, and advanced.

The public interest is related to other ideas, like “common advantage,” “common good,” “public good,” “public benefit,” and “general will.” For example, a common good is defined as a factor or set of factors (whether a value, concrete operational

³ <http://www.un.org/Overview/rights.html>

⁴ http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm

⁵ http://unfccc.int/essential_background/kyoto_protocol/items/1678.php

⁶ Check, among others, paragraph 113 of: http://www.un.org/ga/president/59/draft_outcome.htm.

objective or the conditions for realising a value or attaining an objective) that would direct a person's collaboration with others and would likewise, from their point of view, direct their collaboration with each other and with himself. Thus, public benefits/goods must be protected in the public interest and for the common good. The public interest can also mean more generally what is considered beneficial to the public.

From the political and philosophical realms, there are three major traditional concepts that can be highlighted: Utilitarianism,⁷ Civic Republicanism,⁸ and Rousseau's "general will."⁹ Furthermore, there are modern concepts derived from these traditional doctrines, such as the economic notion of non-rival goods¹⁰ and the free-rider problem,¹¹ among others. However, going deeper into these concepts is not the aim of the current research. A pragmatic and practical approach is necessary to identify actions for the protection of the public interest.

2.3 WSIS and the Public Interest with Regards to the Internet

The identification of public interest issues with regards to the Information Society and particularly in connection with the Internet was achieved during the World Summit on the Information Society – WSIS¹².

As explained on the WSIS website,¹³ like all UN summits, WSIS was basically an intergovernmental process and final decisions were taken by states, since only government delegations had the right to vote. However, WSIS also included a multistakeholder¹⁴ process in which UN bodies and other international organisations, non-governmental organisations, the private sector, civil society, and media were welcomed to participate in the discussions, providing more transparency and legitimacy to the process.

The evolutionary expansion of the Internet into a global communication facility has posed considerable technical, financial, political, and cultural challenges to its governance. There is a certain push from the majority of sovereign states, with the exception of the US and a few other developed countries, which constitute the norm-setting actors in the WSIS, to centralise the existing decentralised system of Internet Governance.

There is a growing concern in the Internet-based industry and technical community that such a move would destroy the delicate balance between the private and the public interest in the Internet's functioning. In order to minimise the possibility of

⁷ <http://en.wikipedia.org/wiki/Utilitarianism>

⁸ http://en.wikipedia.org/wiki/Republicanism#Civic_humanism

⁹ http://en.wikipedia.org/wiki/General_will

¹⁰ <http://en.wikipedia.org/wiki/Rivalrous>

¹¹ http://en.wikipedia.org/wiki/Free_rider_problem

¹² WSIS was a series of UN-sponsored conferences about information and communication. Additional information can be obtained at the official website (www.itu.int/wsis), and in the Wikipedia (<http://en.wikipedia.org/wiki/WSIS>), among other sources.

¹³ <http://www.itu.int/wsis/participation/index.html>

¹⁴ <http://www.itu.int/wsis/basic/multistakeholders.html>

such a scenario, the Geneva WSIS Declaration of Principles calls for a multistakeholder approach to Internet Governance.

The document identifies governments and, respectively, intergovernmental organisations, the business sector, civil society, and international organisations, as the key Internet governance stakeholders, empowered to guarantee in a democratic, multilateral, and transparent manner, the “equitable distribution of resources, facilitate access for all, and ensure a stable and secure functioning of the Internet” (article 48, Declaration of Principles).

The public interest is enshrined in the phrase “Internet-related public policy issues,” which should be the responsibility and right of all states. According to the Internet researchers and analysts, there is a consensus that public policy affecting the Internet includes normative work of the governments on regulating the communication infrastructure, including rules on privacy, security, fraud, etc.

The technical and economic spheres of Internet Governance are left to the business/industry sector, while civil society could contribute to development and Internet awareness at the community level. International organisations (more precisely Internet-governing ones, such as ICANN) still have an important role to play in the creation of technical standards and appropriate policies for the network.

Four important documents resulting from the WSIS process have to be taken into consideration in the identification of the public interest. These documents were endorsed by more than 170 countries and supported by the key stakeholders involved:¹⁵

- Geneva Declaration of Principles¹⁶
- Geneva Plan of Action¹⁷
- Tunis Commitment¹⁸
- Tunis Agenda for the Information Society¹⁹

The WSIS documents reaffirm the universal values related to the public interest, such as the principles of the Charter of the United Nations, international law and multilateralism, the Universal Declaration of Human Rights and the Millennium Development Goals.²⁰

Furthermore, values such as “the universality, indivisibility, interdependence, and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration” were also reaffirmed, alongside with “democracy, sustainable development, and respect for human rights and fundamental freedoms, as well as good governance at all levels.”

¹⁵ Statistics on the Geneva and Tunis Phases can be found respectively at:
<http://www.itu.int/wsis/geneva/newsroom/index.html> and
<http://www.itu.int/wsis/tunis/newsroom/index.html>.

¹⁶ http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=11610

¹⁷ http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=11600

¹⁸ http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=22660

¹⁹ http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=22670

²⁰ Paragraph 2 of the Tunis Commitment: <http://www.itu.int/wsis/docs2/tunis/off/7.html>.

The principles supported by the WSIS documents constitute a valuable and practical definition of the public interest for our purposes.

2.3.1 The Internet, ICTs, and NGNs

A noteworthy positive feature of the public interest as agreed in the WSIS documentation is that reference is made to ICTs in general, and not only to the Internet. This has two main consequences:

First, notwithstanding the current status of the Internet as the most important global network of networks, new networks may emerge in the future, either sharing the current Internet informational space or creating a separate environment.

The Next Generation Networking (NGN)²¹ is a general term to encompass the emerging computer network architectures and technologies. As NGNs are ICTs, the WSIS documents will be applicable to these new networking architectures as well.²²

Second, it has already been noticed by some analysts²³ that in case regulatory protection is only targeted on maintaining the current features of openness and transparency of the network, the changes to the informational environment will shift to the edges, the devices attached to the networks. Accordingly, not only the Internet (or any NGN) should observe the WSIS values, but every ICT should be developed and employed in accordance with the public interest as defined in the WSIS documents.

²¹ <http://en.wikipedia.org/wiki/NGN>

²² The Tunis Commitment, paragraph 28 reaffirmed the desire to build ICT networks and develop applications based on open or interoperable standards that are affordable and accessible to all, available anywhere and anytime, to anyone, on any device. This tends to reject support for NGNs that are not compatible with the Internet or even a segmentation of the current Internet into a two-tiered system as reported by Michael Geist at: <http://news.bbc.co.uk/1/hi/technology/4552138.stm>.

²³ See, for example, Jonathan Zittrain, *The Generative Internet*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=847124.

3. A RESEARCH AND ACADEMIC FACILITY

As argued in the Introduction, the Internet is constantly shifting. As the Tunis Agenda stated, “The Internet has evolved from a research and academic facility to a global facility available to the public.”

Even during the times when the Internet was a research and academic facility, many changes took place. Just to illustrate such an affirmation, two historical examples will be used: (i) the transition from NCP to TCP/IP; and (ii) the discussion between X.25 and TCP/IP.

3.1 From NCP to TCP/IP

The Internet connects computer networks that transmit data using a technique called *packet switching*. Basically, information to be sent along the network is broken into small pieces (*packets*) and header information containing the sender and receiver addresses is added. Since more than one packet may be needed for transmitting the information, and such packets may arrive in a different order, they are also numbered so that the receiving machine is able to re-assemble the content. All these processes are carried out using a series of *protocols*, agreed processes involving software instructions.

In the 70s, the preceding network was called ARPANET and, under supervision of the US military, data was transmitted using a protocol called NCP (Network Control Program).²⁴ Although NCP was a functional solution for the ARPANET, it was rejected by scientist Robert Kahn who had the task of implementing a form of connecting different and independent networks together. NCP was not a technical solution for Kahn’s proposal since control of transmission errors was not good enough. A new protocol suite would better suit this challenge, to be known as TCP/IP (Transmission Control Protocol / Internet Protocol).²⁵

Making the transition from NCP to TCP/IP would not be a simple task. The push for substituting the protocols came from the new ARPANET operator, the Defense Communications Agency – DCA. The DCA agenda had plans to reorient the network to military applications and reduce its research origins. One of the main concerns of DCA managers was that the academic use of the network could expose it to hacker attacks. To protect military computers, a segmentation of the network was carried out, MILNET would be dedicated to military operations, while the TCP/IP ARPANET would continue to develop new technologies.

The transition from NCP to TCP/IP did not result in a significant social change, though. Basically, the network architecture remained the same, with similar social values.

²⁴ http://en.wikipedia.org/wiki/Network_Control_Program

²⁵ <http://en.wikipedia.org/wiki/TCP/IP>

3.2 The X.25 and TCP/IP Debate

The second example, though, involved a greater clash of interests: the X.25 and TCP/IP dispute. As in the '70s the computer vendors had very strong power in the market, their proprietary standards were used to secure their market positions.

In *Silent Theft: The Private Plunder of Our Common Wealth*, David Bollier identifies a connection between standards and the Internet commons, in a section entitled Open Standards as the Basis for an Internet Commons:

“Technological standards are typically designed by companies to advance their strategic competitive interests. That is one reason why IBM so dominated computing in the 1960s and 1970s; its technical protocols were pervasive and proprietary. Other computer companies – Xerox, Digital Equipment, Burroughs, Honeywell, and others – sought to promote their own standards to compete in the market, with varying degrees of success. As this suggests, technical standards are a form of politics and power. That is why they are generally designed to advance a company’s market interests and not necessarily the public interest. What made the advent of the Internet so significant was that it established a common base of technical protocols that belonged to everyone, as a commons. This prevented any single company from ‘owning’ the Internet or any of its key components. Equally important, the technical standards of the Internet did not vest the most power with either computer companies or telephone carriers, who were the chief disputants over technical standards, but with the end users themselves.

“There is nothing intrinsic to computer networking that requires it to function as a commons. The Internet’s architecture is the result of deliberate ARPANET choices that are now embedded in the very design of networking hardware and software. The Internet could just as easily be designed to regulate and control individual behaviour. It could be designed to facilitate the interception of e-mail or the monitoring of suspect citizens. It could be structured to allow anonymity or to require online identification. It could be structured to restrict access in selective ways (such as banning Nazi-related websites, as the French have done) or to entice users to stay within proprietary spaces (as Microsoft and AOL are seeking to do).”

Since the telephone carriers did not want to be imprisoned in using equipment from certain vendors like IBM, they made a joint effort at the Consultative Committee on International Telegraphy and Telephony – CCITT (currently, ITU-T)²⁶ to agree on a common standard for networking, called X.25.

X.25 basically could free the national telephone carriers from buying certain equipment from vendors that dominated the market with their private networking protocols. The X.25 protocol put much control power in the hands of the network operator, based on the model that the network would be designed to maximise transportation technique levels and request little effort from the computing edges.

²⁶ <http://www.itu.int/ITU-T/>

This view, also called the Bellhead view,²⁷ was the opposite from the Nethead view, which was, parallel to the disputes between the computer vendors and telephone carriers, collaboratively developing the TCP/IP protocol, which was ignored by the Bellheads at CCITT defining how to win the battle against the private protocols from the vendors.

Once X.25 was successfully implemented by many national networks, the wait began to see which network protocol would prevail: TCP/IP or X.25. For some, X.25 and the Bellhead view were wrong in having an “intelligent” network in which control was left in the hands of the telephone carriers. For the telephone engineers, this was the only feasible solution, since it would be too dreamy to imagine that the edges of the network would one day be empowered with sufficient computing capacities to have a simpler network. For others, a “stupid network” would provide a better alternative in which the computing ends would do most of the communication tasks, and the computers inside the network would only forward the data packets.²⁸

Different from the NCP to TCP/IP move, this dispute was basically about control. Stanford professor Lawrence Lessig has eloquently argued that the design and ownership of the Internet’s architecture is a key factor in determining how control will be exercised over people and the flow of information. That is why we should be concerned about preserving open standards on the Internet. They are an affirmative means by which ordinary people can assert their civic, cultural, and economic interests over and against those of government and business, which have their own distinct interests in how the Internet architecture should be designed.

By the end of the day, a new understanding of networking came about from the International Standardisation Organisation – ISO, called Open Systems Interconnection – OSI. The OSI layered model of networking made it easier to understand that X.25 and TCP/IP were not competing models, but rather complementary systems.²⁹ And TCP/IP was thus used as a network protocol paradigm for years, under the Nethead view that the network should be as simple as possible and the computer ends would run the applications. This later became known as the *end-to-end* architectural principle.³⁰

3.3 Names and Numbers

Another legacy from the time when the Internet was a research and academic facility is the Domain Name System – DNS.

²⁷ For one article on the Bellhead v. Nethead views, see:
<http://www.wired.com/wired/archive/4.10/atm.html>.

²⁸ For more information on this, check David Isenberg’s *The Rise of the Stupid Network*,
<http://www.isen.com/stupid.html>.

²⁹ In 1982, ARPA neutralised X.25 as a rival networking model by putting a *translation gateway* into work providing an interface between a TCP/IP Internet and a X.25 Telnet. In the combined system, Telnet computers would run TCP/IP over X.25, which was placed at a lower level. The OSI model helped in such interpretation of the ARPA networking system.

³⁰ The 1981 paper *End-to-End Arguments in System Design* by Saltzer, Clark and Reed is a turning point in adding this view to the networking architecture discussion:
<http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf>.

Every computer connected to the Internet has a unique numeric IP address used to route packets of data, allowing e-mail, web pages and other data to reach a desired destination. Since IP numbers need to be unique, the processes of allocation must be transparent and equitable, otherwise commercial and political issues may arise.³¹

By the mid-1980s, a system had been designed to translate numeric IP addresses into human readable names, the Domain Name System – DNS. Since the earliest days of the Internet, someone has had to keep track of IP addresses, to make sure that a given numeric address is assigned to only one computer connected to the Internet.

With the introduction of the DNS, it also became necessary to create and maintain name-to-number lists to translate the domain names used by humans into the numeric IP addresses used by Internet routers. The computers that maintain these translation tables for the top-level are known as root name servers. There were originally 13 of them, located in countries throughout the world and operated by various organisations. A server in the US, known as the “A root,” maintains the authoritative root database and sends changes to the other root servers on a daily basis. Without a set of consistent roots and subsidiary name servers for each TLD, messages on the Internet addressed to a human readable domain name could not be sent to the intended recipients.

The problem reported by Jonathan Zittrain is that by 1997, “the Internet’s supply of ‘good’ names was thought to be drying up. Worse, certain good names were thought to be in the wrong hands. As a Web presence became a near-necessity for large businesses, the realisation that corporate marquee names, such as *avis.com* and *mcdonalds.com* already had been reserved, ‘first-come, first-served’ by cybersquatters, severe consternation was caused among trademark holders. Commercial interests did not desire to expand the name space, and the problem proved to go much beyond the technical level.

ICANN was created in the middle of this economic and political battle, which involves intricate details, such as the agreements granted by the National Science Foundation to Network Solutions, Inc., the composition of the International Ad Hoc Committee and the gTLD MoU deposited at ITU, the National Telecommunications and Information Administration White Paper and much more.

The history of ICANN is seen by many as a dynamic process of institutionalisation of the DNS. Initially, the scientist Jonathan Postel dealt with the DNS through the Internet Assigned Names Authority – IANA. As the necessity for a more elaborate system was identified, a tentative aggregation of IANA was reached, the Internet Society, the Internet Architecture Board, International Telecommunications Union (ITU), the World Intellectual Property Organisation, and the International Trademark Association, through a memorandum of understanding with the ITU as its depository. However, the document was not taken into consideration by the US government, which later created ICANN and a series of steps to internationalise it, but subject to many criticisms, both as a model of the roles and responsibilities of stakeholders and the timing to implementation of these changes.

³¹ One example is the recent negotiation with the ICM Registry for the .xxx domain name.

Further, the US government currently has approval power over ICANN decisions, which means, according to Kenneth Cukier,³² that, in theory, it could act according to its sole interests without outside hindrance.

The names and numbers issue is another example of a system that, while in the early phase when the Internet was a research and academic facility, governance levels were adequate. It was a geek Internet run by geeks. However, as commercial interests, concerns from civil society and attention from national governments on security issues, to name a few, become increasingly prevalent as the Internet turned into a global facility available to the public, a higher level of governance was needed.

3.4 Challenges Brought About by New Stakeholders

There is a cultural change to be noticed when the Internet moved from a research and academic community to a global facility available to the public. For Marjory Blumenthal and David Clark,³³ in *Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World*,³⁴ the Internet was originally a small scientific community with great affinity and common trust under the supervision of academic institutions and governmental bodies prohibiting commercial use of the network. This made it easier for decisions to be taken since there was this sense of community³⁵ and the stakes were not high.

As new stakeholders joined the Net, expectations were modified, causing a change in the architecture of the network to conform to the new interests.

³² Multilateral Control of Internet Infrastructure and its Impact on US Sovereignty: <http://www.cukier.com/writings/cukier-netgov-TPRC04.pdf>.

³³ Also worth to check *The Rise of the Middle and the Future of End to End* slides from James Kempf and Rob Austein at: <http://www3.ietf.org/proceedings/03mar/slides/plenary-18.pdf>.

³⁴ <http://itc.mit.edu/itel/docs/jun00/TPRC-Clark-Blumenthal.pdf>

³⁵ Supporting this is Dave Clark's famous phrase "We reject kings, presidents and voting. We believe in rough consensus and running code."

4. A GLOBAL FACILITY AVAILABLE TO THE PUBLIC

As the Internet has expanded more stakeholders must now be involved in its governance. It is important to explore how clashes between public and private interests were resolved domestically with different equations and balances, as this is a very important Internet analogy in this research.

4.1 Global Public Goods

Global public goods play an important role in meeting the public interest. According to Kaul, Grunberg, and Stern, public goods' benefits reach across borders, generations, and population groups. The authors state that most recently the World Bank's Global Development Finance Programme has further distinguished between the core and complementary activities associated with the provision of global public goods.

4.2 Commons

Also to meet expectations of the public interest, another concept of interest comes into play: the commons. The commons is an absence of legal exclusionary norms. It therefore does not have direct consequences for human actions that are equivalent to those arising as a result of the existence and enforcement of property rights. The development of the commons will be addressed in this research, but will not constitute the focus of our analysis.

John Cahir states that the commons is not a redundant concept in legal theory. Contrary to James Harris' contention that the concept of common property is redundant until the instantiation of a private property regime, and that therefore the commons is the negative of property, it is not property, Cahir states that parallel to the relationship between "being" and "nothingness" (their priority against each other remains unresolved), or parallel to saying that darkness is not light and light is not darkness, one can invert the logical relationship and say that property is the negation of the commons, property is not the commons.

4.3 The Common Heritage of Mankind

The concepts raised so far are intertwined and derive from the same underlying general concept of the public interest. Since the common interest requires states to refrain from giving their individual interests precedence over that of mankind, the concept of the Common Heritage of Mankind is the application of the regimes related to the commons (such as *res communis*) to areas made accessible by new technologies, such as the deep seabed and outer space.

The Common Heritage of Mankind principle can be found in some experiences from international law, which will be briefly examined for illustration purposes and with a wrap-up of the principles related to it. For effectiveness, however, it is mandatory that the global character and relevancy of the object to be protected is clearly identified.

Since identifying mankind's interests, where the CHM is involved, is a real analytical problem, Kemal Baslar³⁶ suggests that such decisions should be carried out by a Common Heritage Authority, which will take into account the benefits of present and future generations in analysing whether a resource should be declared as the CHM.

4.4 Zones of Public Interest with Regards to the Internet

Internet Standards – They can be regarded as common public goods and the public at large will benefit if future standards remain open and not the property of any corporate interests.

Open Source Software – End-users, who also make up part of the public interest, will benefit from a wider choice of software.

Freedom of Access to Critical Information – While any future IG regime has to take into account the protection of property rights of intangible products distributed through ICTs, the public interest will benefit if critical information (health, education, etc., and related issues) is made available to the public in a balanced format.

Privacy/Data Protection vs. Surveillance (Cryptography) – While in most democratic societies there is a general interest in the disclosure of documents of public authorities, the right to public access is and should be limited to exceptions of privacy and data protection. The disclosure of private data is only allowed when the principles of the right to information and of proportionality are in play.

The Internet as a Social Phenomenon and Pool of Knowledge – The traditional education model is based on face-to-face contact between the trainer and the learner, which is changing with ICTs. E-learning models have been introduced in the educational systems of many countries (especially those with good levels of ICT capacity and Internet awareness). The model creates virtual e-learning collaborative environments, where knowledge is generated and passed on through flexible web-based platforms for information sharing. Thus, the Internet has been rapidly evolving into an education medium that provides socialisation and social advancement. It is firmly in the public interest to further develop the Internet as an instrument/platform for education and dissemination of knowledge. Vast amounts of e-knowledge, created and pooled through e-mail exchanges, blog postings, discussion groups, and other forms of Internet-based interactivity, is a global public good and should not be commercialised or privatised for the benefit of the few. Access to this information and data must be unimpeded and free.

Content – This involves the issue of pornographic images and text over the Internet. While safeguarding the basic right of freedom of expression over the Internet, the spread of publicly unacceptable information over the Internet, which is difficult to define from a legal and social point of view, should be curbed. Different cultural systems treat the issue of Internet-based content differently. China, for example, is imposing new regulations to control content on its news websites. Sites should only post news on current events and politics. It did not define what would be acceptable

³⁶ The Concept of the Common Heritage of Mankind in International Law.

under those categories. The sites are prohibited from spreading news and information that goes against state security and public interests. In an ongoing effort to curb potential dissent, thousands of cybercafés, the main entry to the Web for many Chinese unable to afford a computer or Internet access, have been closed. Authorities in Shanghai³⁷ have installed surveillance cameras and began requiring visitors to Internet cafés to register using their official identity cards to keep tabs on who's seeing and saying what online. The government also threatened to shut down unregistered websites and blogs. Moreover, Google has offered a censored Chinese search.³⁸

Terrorism – The possibility of instantaneous and reliable communication makes the Internet a unique instrument for the planning and the execution of a whole set of human activities. The Internet could have a devastating effect if used by terrorist networks for the mobilisation of their supporters across the globe, in the planning and the coordination of their deadly actions. It is fully in the public interest to develop effective safeguards to protect the Internet from such practices. However, it remains very difficult to do so, because many governments take drastic measures and adopt policies aimed at the ongoing monitoring of e-mails, and the tracking of privately or commercially sensitive information. This violates basic human freedoms (enshrined in various international human rights conventions). The opponents find the policing of the Internet, in other words, eavesdropping on e-communication, not a viable option.

4.5 Areas that Call for Attention

The attached table (Annex) indicates which zones from the ones mentioned above are already regulated, at both the regional and the international level.

The table clearly shows that it is the zone on Internet standards which remains unregulated other than by ICANN. This zone links other areas, including the Internet as a social phenomenon, pool of knowledge, and technological development. Therefore, apparently it is the Internet standards zone that calls for regulation the most. Regulation should be mapped out by always keeping the public interest (as opposed to private ownership, economic advantages, politics, etc.) as a priority.

There is increasing attention to the possibility of the politicisation of Internet resources, “manipulated for national economic gain by developing countries, but with increased costs to genuine users of resources and that this is more likely in a multinational, intergovernmental setting than under the current framework of Internet management,” according to Kenneth Cukier.

Another feature regarding the Internet that must be observed is its flexibility and dynamism, existing since the time of the ARPANET. New naming schemes may be developed in the near future. But no matter whether the DNS is maintained or new systems developed, the public interest must be observed and not only business-driven design and dispute resolution approaches or politics of control without harmony to the global public interest.

³⁷ <http://news.designtechnica.com/>

³⁸ Check *Google.cn Filtering: How It Works*: <http://ice.citizenlab.org/?p=178>.

4.6 Protecting the Public Interest

As pointed out above, there are public interest features that need protection, such as:

- (i) protection against layer violation regulations, which, in order to regulate problems identified in a certain layer, target another layer and thus hurt non-infringing users;
- (ii) adequate, legitimate, accountable, and democratic control of the root's extra-territorial manifestations, in case there should be only one authoritative root zone system "owned" by one state and managed by its licensee, while at the same time stimulate research for alternative roots and their impact on the Internet;
- (iii) establishment of an international mechanism to be resorted to and adjudicated at the appellate stage after regional arbitration has been exhausted, when conflicting national public interests cannot be resolved through self-regulation;
- (iv) establish criteria to assess when and to what degree the local courts or local arbitration, and ultimately the international mechanism, should impose state responsibility when other stakeholders are damaged and propose criteria for states to grant varying degrees of immunities as appropriate to specified Internet operators whilst engaged in the course of their Internet-related duties, and also exercise oversight over such bodies as ICANN, W3C, and the IETF;
- (v) protection of an enabling environment for innovation, by keeping the Internet protocols within the public domain;
- (vi) promote recourse to regional arbitration mechanisms to resolve disputes efficiently, cheaply, transparently, and without undue legalese.

All these actions must be carefully carried out under the precautionary principle, because by applying public interest regimes the dynamism of the Internet may be negatively impacted.

A strong counter-argument to protection (by shielding the Internet against unwanted changes) is the Internet's dynamism. From the early days of the ARPANET to the current Internet so much has changed. We do not know what will come next. Is the so called "balkanisation," the fragmentation of the Internet into new Internets, which may or may not be compatible something absolutely bad, to be feared, and avoided? Or should we just let things be and let things sort themselves out? These are very difficult, however mandatory, questions that need to be addressed. The WSIS documents, however, indicate that the public interest would seek a ubiquitous Internet.

It is important to have in mind that the mechanisms aimed at the protection of the public interest should not impact the flexibility of the Internet. Janet Abbate states that "the key to the Internet's success was a commitment to flexibility and diversity, both in technical design and in organisational culture. No one could predict the specific changes that would revolutionise the computing and communications industries at the end of the 20th century. A network architecture designed to accommodate a variety of

computing technologies, combined with an informal and inclusive management style, gave the Internet system the ability to adapt to an unpredictable environment.” The analogies with the Law of the Sea, outer space, common heritage, etc., in general, tend to fix the object of protection against unwanted changes. However, this should be counterbalanced against the dynamism of the Internet.

4.7 The Internet Governance Forum

The new Internet Governance Forum – IGF³⁹ is expected to be the most appropriate mechanism to discuss several issues related to Internet Governance, including standards-setting. The current groups involved with producing protocols and *de facto* standards, such as the Internet Engineering Task Force – IETF lack a high governance level.

The definition of technical standards is historically an issue that did not raise much attention, since efforts have been centralised on ICANN and the names and numbers governance. Many other issues should receive more public attention and many of these should be related to standards-setting. We note that in many cases self-regulation by the market may not be enough to avoid abuses and if certain protocols benefiting some actors are implemented, the end users will have difficulty in making a choice.

The IETF is described⁴⁰ as a group of people that organised spontaneously with an interest of contributing to the engineering and evolution of new technologies for the Internet. It is the main group engaged in developing new Internet features and specifications. It is not a legal entity, nor does it have a board of directors.

Openness and meritocracy are core principles of the IETF and the famous phrase from David Clark reflects this: “We reject kings, presidents and voting. We believe in rough consensus and running code.” Decisions at the IETF are taken by discussions held online and the final results consolidated in the form of Requests for Comments. As these sometimes tend to become too philosophical, in the case of the development of the World Wide Web, Tim Berners-Lee decided to bypass the IETF and constitute the World Wide Web Consortium.⁴¹

Similarly, other stakeholders are today not obliged to conduct their discussions and submit proposals for new technologies through the IETF process. This is somehow positive, since by having a mandatory body for standards-setting, the chances of influence by private interests of such a body would be higher.

Independently of which body shall continue leading the development of new protocols and standards-setting, such organisations shall work together with the IGF to increase legitimacy in their decisions. It is important to stress that among the IGF

³⁹ So far, the IGF envisaged by the Tunis Agenda has not been established, and its first meeting is expected to occur in Athens. The IGF website is located at: <http://www.intgovforum.org>.

⁴⁰ RFC 3160 – The Tao of IETF: A Novice’s Guide to the Internet Engineering Task Force: <http://www.ietf.org/tao.html>.

⁴¹ See Tim Berners-Lee, *Weaving the Web*.

competencies, recommendations can be made and the IGF can process opinions on proposed standards and technologies.

4.8 The Need for an International Agreement

The Internet Governance Project paper *Quo Vadis? IGP's Response to the WGIG Report*⁴² states that despite the governance/oversight models proposed by WGIG, global governance must be based on authoritative agreements between governments. Furthermore, authoritative agreements not only have to be legitimate, they also have to be justiciable. In international law, justiciable agreements are those that are included in conventions or legally-binding international treaties. Thus, if Internet Governance is to be obtained, it must be treaty-based, and the treaties must have universal adherence in order to be fully effective.

The Internet Governance Project acknowledged the widespread reluctance of almost all parties in this process to take up the burden of a new international convention. “We realise that everyone is looking for short cuts. We are convinced that short cuts don’t really exist and won’t work. They will simply defer the day of reckoning and prolong the current state of tension and lack of resolution of outstanding governance problems.”

While some conventions already exist that affect isolated issues related to the Internet, like intellectual property, elements of telecommunications policy, organised crime, or child pornography, there are currently none that affect the Internet as a channel or the management of Internet resources. The Internet Governance Project strongly advocates a framework convention:

“Something must be done. The definition of Internet Governance proposed by the WGIG suggests a sequence in which agreements must be made. First, there must be a definition of the principles and norms on which governance is to be based. If the first stage is to agree authoritatively on principles and norms, the negotiation of a framework convention is clearly a reasonable, practical, and feasible mechanism.”

Framework conventions in areas like climate change have allowed states, with the input of non-state actors, to reach agreements that will provide a legally-binding context for subsequent efforts to deal with issues. Negotiating a framework convention would provide a focus for policy analysis and discussion through a new multistakeholder forum, but would also provide a specific objective for the discussions.

Negotiation of international conventions can either take place within an existing institution, or if one cannot be agreed, can take place on an *ad hoc* basis, reporting to a more general intergovernmental body, like the United Nations General Assembly or the Economic and Social Council. Eventually, a convention would have to be adopted by the General Assembly, the only universal body whose competence covers all of the elements of Internet Governance – prior to signature, ratification, and entry-into-force. Secretariat support for the negotiations, including monitoring and facilitating the

⁴² <http://dcc.syr.edu/miscarticles/IGP-quovadis.pdf>

forum as part of the process, could be provided by an existing organisational unit, or by an *ad hoc* unit attached to an existing organisation, much as was done with WGIG. This would keep the financial implications of the negotiation process to a minimum.

Once a framework convention has entered into force, its periodic meetings of states parties would constitute a general intergovernmental body in which issues could be resolved. This would provide intergovernmental oversight to the Internet without the creation of a more complex and definitive structure, unless, as rules and procedures were worked out in subsequent negotiations, a more formal institutional structure was found necessary at some future time.

The Internet Governance Project paper *Framework Convention: An Institutional Option for Internet Governance*⁴³ suggests that a United Nations Framework Convention on Internet Governance seems to be a reasonable option for states to consider.

First, the framework convention should define clearly what the governance problem is, and its boundaries. Like the United Nations Framework Convention on Climate Change, it should have agreed definitions for key Internet concepts, including the Internet itself and who is concerned with its governance. In working out those issues, the principle of subsidiarity, which advocates cross-border legislative solutions only when it is considered more effective than action taken at national, regional, or local levels, is an appropriate starting point for discussion. Many issues may be better resolved at a regional or national level than at the international level. For example, some content related issues (hate speech, pornography, gambling) involve cultural differences that may be difficult to resolve at a global level beyond the acceptance of general principles. These should then form part of an international framework.

Second, a framework convention should clearly establish the norms that should be applied to governance. This could include such elements as maintaining the openness and freedom of the Internet as a communication channel and ensuring unimpeded global access. Norms could also be defined to address issues that are considered misuses of the channel, such as spam. A framework convention should indicate those areas in which further agreements need to be reached, particularly in terms of conflicting regimes (like intellectual property and freedom of expression). The norms should clearly define and legitimise the role of civil society and private sector organisations, which have been critical to the development and maintenance of the Internet, will play in the formal governance process.

Third, it should establish agreements on when negotiations should take place – a kind of trigger mechanism based on disputes in other areas, or with the functioning of the Internet. It could establish the concept that when additional legal agreements are needed, these can be in the form of protocols to the convention.

Fourth, it should empower the meetings of states parties to the convention to act as a kind of overseer of that limited set of Internet-related issues that are deemed appropriate for governance. It is important that the states party set the basis for vigorous participation of civil society in this function.

⁴³ <http://dcc.syr.edu/miscarticles/igp-FC.pdf>

4.9 Analogies with Other Conventions

Before going further with analogies, it is important to understand that the deep seas, some celestial bodies, and the Antarctic, have mineral resources of great economic interest. Apart from the material benefits, the states obtaining footholds in these places would also benefit strategically in many political and military aspects. Therefore, first possession regimes benefit the wealthy and powerful parties.

The situation is very similar to that which was faced in dealing with climate change in the 1980s. In that case, the first step taken to deal with the problem was to first agree that the problem existed and to agree on its dimensions. The second step was to agree on the norms that should be applied.

Climate Control – The Framework Convention on Climate Change was one of two binding treaties opened for signature at the United Nations Conference on Environment and Development (UNCED) in 1992. The treaty, also known as the Climate Convention, addresses potential human-induced global warming by pledging countries to seek “stabilisation of greenhouse gas concentrations in the atmosphere at a level that would prevent dangerous anthropogenic interference with the climate system.” Though stated only in general terms, the Climate Convention parties agreed to attempt to limit emissions of greenhouse gases, mainly carbon dioxide (CO₂) and methane (CH₄).

Although signed at UNCED, the Climate Convention was negotiated through a separate process under the Intergovernmental Negotiating Committee (INC) for the Framework Convention on Climate Change. The text was adopted at New York on 9 May 1992, opened for signature at Rio de Janeiro from 4-14 June 1992, and thereafter at United Nations Headquarters from 20 June 1992 to 19 June 1993. By that date, the Convention had already received 166 signatures.

In 1997, governments agreed to an addition to the treaty, called the Kyoto Protocol, which has more powerful (and legally binding) measures. The protocol is expected to take effect soon. And, since 1988, an Intergovernmental Panel on Climate Change has reviewed scientific research and provided governments with summaries and advice on climate problems.

The compliance regime consists of a Compliance Committee made up of two branches: a Facilitative Branch and an Enforcement Branch. As their names suggest, the facilitative branch aims to provide advice and assistance to parties in order to promote compliance, whereas the enforcement branch has the power to determine consequences for parties not meeting their commitments. Both branches are composed of 10 members, including one representative from each of the five official UN regions (Africa, Asia, Latin America and the Caribbean, Central and Eastern Europe, as well as Western Europe and Others), one from the small island developing states, and two each from Annex I and non-Annex I parties. Decisions of the Facilitative Branch may be taken by a three-quarters majority, but decisions of the Enforcement Branch require, in addition, a double majority of both Annex I and non-Annex I parties. The committee also meets in a plenary, composed of members of both branches. A bureau, made up of the chair and vice-chair of each branch, supports its work.

Similar to Internet Governance, a large number of national actors and different international organisations were involved in climate change issues (the World Meteorological Organisation, the United Nations Environment Programme, UNESCO, to name a few), and there was significant interest by non-governmental organisations, too. It was recognised that any regime, in order to deal with the issue, would have to have a sound basis in international law, and therefore an international convention would be needed. Rather than seeking to solve all of the problems of climate change in a single convention, a method that risked getting bogged down in contentious detail and taking considerable time, the concerned governments and organisations decided instead to pursue what they called a “framework convention.” This convention would establish the principles and norms under which international action would proceed, and set up a procedure for negotiating the more detailed arrangements that would be necessary to deal with climate change. The conference of states party to the convention would become the oversight body and negotiating forum, while its secretariat would provide the necessary studies.

The United Nations Framework Convention on Climate Change (UNFCCC) has provided a basis for subsequent negotiation that has led to progress in dealing with the issue. Almost all states (189 in total) are parties to the convention, although not to all of its protocols. The situation with regard to Internet Governance is remarkably similar. A large number of national governments are involved, as are a number of international organisations (ITU, WIPO, WTO, UNESCO, and the United Nations itself, to name a few), as are many civil society organisations. Any effort to deal with Internet Governance will have to be firmly grounded in international law, suggesting a convention as a means of providing the necessary standing. The time is ripe for agreement not only on principles and norms, but also on procedures for dealing with future issues as they arise. Therefore, the UN Framework Convention on Climate Change, rather than seeking to solve all of the problems in a single treaty, pursued a “framework convention,” which first established the principles and norms under which international action would proceed. It also set up a procedure for future negotiations over more detailed arrangements. A similar approach for Internet Governance is suggested.

UN Convention on the Law of the Sea – The UN Convention on the Law of the Sea is the main international legal instrument that regulates the world’s high seas.

The origins of the convention date from November 1967 when Ambassador Arvid Pardo addressed the General Assembly of the United Nations and called for “an effective international regime over the seabed and the ocean floor beyond a clearly defined national jurisdiction.” This led to the convening of the Third United Nations Conference on the Law of the Sea in 1973. After nine years of negotiations, the conference adopted the Convention in December 1982. It entered into force 12 years later.

The convention establishes a comprehensive legal framework to regulate all ocean space, its uses, and resources. It contains, among other things, provisions relating to the territorial sea, the contiguous zone, the continental shelf, the exclusive economic zone, and the high seas. It also provides for the protection and preservation of the marine environment, for marine scientific research, and for the development and transfer of marine technology. One of the most important parts of the convention

concerns the exploration and exploitation of the resources of the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction. The convention declares the area and its resources to be “the common heritage of mankind.” The International Seabed Authority, established by the convention, administers the resources of the area.

One of the Internet framework’s aims would be to remove Internet jurisdiction disputes from the realm of national jurisdictions and assign them to a supra-national authority to judge them according to the harmonised laws of the convention.

The convention would also allow technological studies and progress by private parties in the name of a declared commons or public good.

Part XV of the UN Convention lays down a comprehensive system for the settlement of disputes that might arise with respect to the interpretation and application of the convention. It requires state parties to settle their disputes concerning the interpretation or application of the convention by peaceful means indicated in the Charter of the United Nations. However, if parties to a dispute fail to reach a settlement by peaceful means of their own choice, they are obliged to resort to the compulsory dispute settlement procedures entailing binding decisions, subject to the limitations and exceptions contained in the convention. The mechanism established by the convention provides four alternative means for the settlement of disputes: the International Tribunal for the Law of the Sea, the International Court of Justice, an arbitral tribunal constituted in accordance with Annex VII to the Convention, and a special arbitral tribunal constituted in accordance with Annex VIII to the Convention. If the parties to a dispute have not accepted the same settlement procedure, the dispute may be submitted only to arbitration in accordance with Annex VII, unless the parties otherwise agree.

In Internet cases, it is doubtful whether states can arrive at settlement by peaceful means of their own choice. Asserting (or declaring that a court lacks jurisdiction) involves a myriad of issues and interests, especially since every court would be more than willing to protect its own nationals from foreigners.

The high seas are described both as *mare liberum* and as the common heritage of mankind.

In the late sixteenth and early seventeenth century, the great voyages of discovery and the resulting sea-borne empires in Europe necessitated internationally accepted rules on rights to the use of the ocean. There were already negotiations on freedom of the high seas and on the Grotian principle of *mare liberum*. Grotius had noted that “the sea, since it is incapable of being seized as air, cannot have been attached to the possessions of any particular nation.”

Later on, the Preamble of the Outer Space Treaty of 1967, stated that “inspired by the great prospects opening up before mankind as a result of man’s entry into outer space, and recognising the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes, the exploration and use of outer space should be carried on for the benefit of all peoples irrespective of the degree of their economic or scientific development, and that the treaty parties wanted to contribute to

broad international co-operation in the scientific as well as the legal aspects of the exploration and use of outer space for peaceful purposes.”

Therefore, the Grotian principle of *mare liberum* resulted in the concept of *res communis*. These goods are characterised by their freedom of exploitation. They belong to all and, in principle no limits are set on their use. The common heritage of mankind concept emerged in 1967 when Ambassador Arvid Pardo from Malta pleaded in the UN General Assembly for an exploitation of the deep seabed resources in the general interest under supervision of an international body.

Both *res communis* and the common heritage of mankind have in common that goods in one of these categories are not under the sovereignty of any one state and that national appropriation is not possible.

But, *res communis* is aimed at making it possible for all countries to use the goods. This means that there should be freedom of access, exploration, and exploitation for all states. States have to avoid obstructing the use of *res communis* by other states. States have the right to appropriate the products of exploration/exploitation of the *res communis*. In contrast, the concept of the common heritage of mankind is rather aimed at the preservation of the goods. For this kind of public good, a governing mechanism will regulate the access, exploration, and exploitation. States will only have rights on the products of exploitation in accordance with the treaties. These treaties mostly use criteria of equity to divide the gains of exploitation. Two global public goods are recognised in international agreements as the common heritage of mankind, namely the deep seabed and the moon and its natural resources.

The Internet should belong to the common heritage category. Access, exploration, and exploitation should be governed by an international treaty, under the supervision of an international body. Governance of the Internet should not run amok.

The Internet is different in the sense that there are no direct material benefits to be shared. However, similarly as in the situation in which the developing states would not benefit from the exploration that would be only carried out by the developed states due to technological advantage, there are several stakeholders that currently do not have the capacity to participate in the legal and technological regulation of the Internet.

Outer Space Treaty – The Outer Space Treaty was considered by the Legal Subcommittee on the Peaceful Uses of Outer Space (COPUOS) in 1966 and agreement was reached in the General Assembly in the same year (resolution 2222 (XXI)). The Treaty was largely based on the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space. The declaration stated that:

1. The exploration and use of outer space shall be carried out for the benefit and in the interests of all mankind.
2. Outer space and celestial bodies are free for exploration and use by all states on a basis of equality and in accordance with international law.

3. Outer space and celestial bodies are not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.

The declaration was adopted by the General Assembly in resolution 1962 (XVIII) in 1963, but added a few new provisions. The treaty was opened for signature by the three depository governments (the Soviet Union, the United Kingdom and the United States of America) in January 1967, and it entered into force in October 1967.

State parties are obliged to settle by peaceful means their disputes concerning the interpretation or application of the convention. Disputes can be submitted to the International Tribunal for the Law of the Sea established under the convention, to the International Court of Justice, or to arbitration. Conciliation is also available and, in certain circumstances, submission to it would be compulsory. The tribunal has exclusive jurisdiction over deep seabed mining disputes.

The Antarctic Treaty – A total of 12 nations signed the Antarctic Treaty on 1 December 1959 in Washington, D.C. The treaty entered into force on 23 June 1961; the 12 signatories became the original 12 consultative nations. To date, there are 45 Antarctic Treaty nations, representing about two-thirds of the world's human population.

Consultative meetings have been held approximately every other year since the treaty entered into force, but since 1993 they have been held more frequently. Each meeting has generated recommendations regarding operation of the treaty that, when ratified by the participating governments, become binding on the parties to the treaty.

Additional meetings within the Antarctic Treaty system have produced agreements on conservation of seals, conservation of living resources, and comprehensive environmental protection.

The Antarctic Treaty designated the Antarctic continent as a sanctuary for peaceful use for the benefit of all mankind, prohibiting “any measures of a military nature,” which includes the establishment of military bases and fortifications, carrying out military manoeuvres, and testing any type of weapons.

Regarding jurisdiction claims, Article VIII of the Treaty states that:

1. In order to facilitate the exercise of their functions under the present treaty, and without prejudice to the respective positions of the contracting parties relating to jurisdiction over all other persons in Antarctica, observers designated under paragraph 1 of Article VII and scientific personnel exchanged under subparagraph 1(b) of Article III of the Treaty, and members of the staffs accompanying any such persons, shall be subject only to the jurisdiction of the contracting party of which they are nationals in respect to all acts or omissions occurring while they are in Antarctica for the purpose of exercising their functions.

2. Without prejudice to the provisions of paragraph 1 of this article, and pending the adoption of measures in pursuance of subparagraph 1(e) of Article IX, the contracting parties concerned in any case of dispute with regard to the exercise of jurisdiction in

Antarctica shall immediately consult together with a view to reaching a mutually acceptable solution.

The treaty also provides for the parties to meet periodically to discuss measures to further the objectives of the treaty and puts in place a dispute settlement procedure and a mechanism by which the treaty can be modified. Article XI in fact states that:

1. If any dispute arises between two or more of the contracting parties concerning the interpretation or application of the present treaty, those contracting parties shall consult among themselves with a view to having the dispute resolved by negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement, or other peaceful means of their own choice.

2. Any dispute of this character not so resolved shall, with the consent, in each case, of all parties to the dispute, be referred to the International Court of Justice for settlement; but failure to reach agreement on reference to the International Court shall not absolve parties to the dispute from the responsibility of continuing to seek to resolve it by any of the various peaceful means referred to in paragraph 1 of this article.

5. CONCLUSION

As the peoples of the world have the possibility of using ICTs for many purposes, such as sharing knowledge and participating in collaborative initiatives regardless of geographical boundaries, leading to higher levels of development and enhancing the innovation process, the Internet plays an essential role as the most important facility for internetworking.

Considering these and many other important aspects brought by the Internet, the WSIS documents have highlighted the need for the protection of the public interest with regard to the Internet by calling for international Internet Governance with the full involvement of all stakeholders.

At a global level, the current debate on Internet Governance, public interest, control of the root servers, and most other topics, which entail some sort of governance, seems to take the form of a tug of war between the US on the one hand, and the rest of the stakeholders who have an interest in the subject on the other. Evidently enough, the US is unwilling to lessen its control over ICANN, the institution that manages the Internet resources, attributing this unwillingness to the fact that “the current Internet system is working (well)” and for the benefit of security and stability. It has also expressed the view that existing institutions are appropriate forums, such as WIPO for intellectual property rights, and the Council of Europe Cybercrime Convention for cybercrime.

On the other hand, the majority of other stakeholders view the US position as exceeding its role of control and ICANN as having strayed from the principles specified in its Memorandum of Understanding.

A global framework may be one of the best ways to secure the protection of the public interest on the Internet. Although some authors oppose a global framework because it is a “fatal flaw” to empower an international body to govern the Internet since the Internet is not a single thing, but rather a multitude of technologies, networks, applications, and users subject to many different rules and regulators, other authors believe a framework could be drafted even though there is still a long way to go. This is because there are already many rules being created and enforced within the digital communities. These common norms include social pressure where the offender is reprimanded by the group or community as opposed to an outside force. Behaviour is also being controlled by contract between users and commercial services in which the offender is punished by cancellation of services. While there may be consensus as to the current methods of enforcement on the Internet, there is no consensus as to whether new legislation should be imposed on network communities by any nation state. Despite the lack of cohesive thought regarding the need for new law, consensus building takes place regularly within online communities. This is apparent from the informal creation of rules and enforcement of penalties. Such consensus building within the network is the fundament of any future legal regime or regimes. Furthermore, given that a degree of consensus required for a global convention on jurisdiction and recognition can be acquired, this can only be achieved if its scope is modest and its provisions tolerant to differences in practices and values.

Many observers have warned of the risk of the balkanisation of the Internet and even of the establishment of a second far-reaching global network. However, the scope of the Internet is to have as many computers as possible connected to one network. A second network would defeat the scope of both. Secondly, according to the statement issued by the US on August 15 in reply to the WGIG Report, the US has showed that continued internationalisation of the Internet is evidenced by the recent creation of Regional Internet Registries for Latin America and Africa and enhanced efforts of the Internet community to work towards an equitable distribution of IP addresses. Nonetheless, it is true that the US dominance may lead to political unrest. It is feared that the US' aggressive assertions of control over ICANN only increases the possibility that other nations will support policies that will deglobalise and territorialise authority over the Internet.

It is worth mentioning that even though other internetworking approaches may be possible in the future, the WSIS documents specifically address the Internet as a system that deserves global attention and therefore an international public interest seems to justify an enhancement in the governance level of the Internet, contrary to claims that the historical leading role of the United States must be maintained. While this leading role has been essential in achieving the current value of the Internet, it is uncertain whether the *status quo* should remain unchanged for the benefit of the public at large.

By understanding the historical dynamism of the Internet, one can be convinced that its architectural design is the product of many different sources of influence (to name a few, the US military, the academic community, trademark rights holders, Internet domain name registrars and registries, telephone carriers, computer equipment manufacturers, international organisations, and so on). As the Internet has connected different networks all over the world, the network value has increased and a new "player" arisen: the public interest.

It is important to understand the historical development of the Internet leading to its current architectural structure. The lesson learned is that the Internet should not be taken for granted, as it is a human creation. And it can therefore be modified by the players with sufficient technical, political, and economic power. These power struggles have always been a natural feature of Internet development (such as the domain name wars, the substitution of NCP for TCP/IP, or the X.25 and TCP/IP debate) and these decisions were rarely made democratically or with regard to the global public interest, especially because at that time the Internet was mostly a domestic experiment and there was no need for a public interest regime. The Internet was a "research and academic facility."

In this sense it is possible to make some analogy to the notion of "governance" from a concept generally more familiar to the general public than "Internet Governance": in "corporate governance," "governance" arrangements are become necessary as the corporation and the base of shareholders grow, which gives rise to the establishment of transparent rules of how to conduct the company's business. At the time when the corporation is a small shop, there is no need for disclosure of financial information or an independent board, because the administrator is often the owner of the shop. However, as more interests are involved, governance becomes necessary. One can say that a similar process has happened to the once "techie" dominated Internet, which

has observed the coming of intellectual property lawyers and large corporations. The Internet is now a “global facility available to the public.”

As the Information Society is now an enshrined concept resulting from the WSIS process, the public interest has reached sufficient potential to bring to negotiations the concrete argument that institutional processes that define how Internet names and numbers dealt with by ICANN can no longer run without a reform addressing the criticism currently discussed. Not only ICANN, but also standardisation bodies, such as the IETF and W3C must more and more enhance their governance processes of board composition, transparency, accountability, fiscal control, and openness.

Meanwhile, the Internet Governance Forum is about to conduct its first meeting. However, unless the stakeholders agree on basic principles and norms, there can be no agreement on rules, organisations, and decision-making procedures.

A starting point would be to agree on an applicable regime for the Internet, which could benefit from the experiences related to the moon, the high seas, the seabed, and outer space. These international spaces were first argued to be *res nullius*, or entities belonging to no one. This idea was disputed and the idea of *res communis*, or a common thing, won out, as is the case with many Internet components. However, an agreement has not yet been reached.

Considerable further research still needs to be conducted. The conclusions of the Working Group on Internet Governance can form part of that investigation, as can the work of members of civil society and of governments. This is a great opportunity to both protect and promote the Internet as one of the world’s most important global services and to innovate in the creation of the institutions that will be needed for that purpose.

ANNEX

AREAS WHICH ARE ALREADY REGULATED BY TREATIES/AGREEMENTS/DECLARATIONS <i>compiled by Stephanie Psaila</i>			
INTERNET ISSUE AREA	INTERNET AREA	EU/REGIONAL	INTERNATIONAL
Commerce	Trade/ E-Commerce	Brussels Regulation	Doha Ministerial Declaration of WTO (2001)
			UNCITRAL Model Law
			Hague Conference's Proposed Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Law
	Consumer Protection	Brussels Regulation	2000 OECD Guidelines for Consumer Protection in the Context of E-Commerce
			2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders
			APEC Voluntary Guidelines for the Online Environment
	Taxation		OECD Technical Advisory Group on Tax
Competition		ICANN Registry-registrar split	
		ICANN registry contract EU competition authority review of ISP mergers	
Intellectual Property Rights	Copyright	Council of Europe Cybercrime Convention	WTO Trade-Related Aspects of Intellectual Property (TRIPS)
			WIPO Copyright Treaty (WCT) 1996
			WIPO Performances and Phonograms Treaty (WPPT) 1996
	Trademarks		WIPO Joint Recommendation Concerning the Protection of Marks, and Other Industrial Property Rights in Signs on the Internet

			ICANN-WIPO UDRP for domain name trademark conflicts
			US Anti-cybersquatting Consumer Protection Act
	<i>Patents</i>		WIPO Substantive Patent Law Treaty
<i>Crimes</i>	<i>Hacking (Illegal access/interference/misuse of computer data and systems, computer fraud)/ Network and IS Security</i>	Council of Europe Cybercrime Convention	2002 OECD Guidelines on the Security of Information Systems and Networks
			UN General Assembly Resolution 58/199 on a Global Culture of Security
			ITU Plenipotentiary 2002 Resolution 130
			UN Convention on Organised Crime
	<i>Child Pornography</i>	Council of Europe Cybercrime Convention	Optional Protocol to the Convention on the Rights of the Child (2002)
	<i>Terrorism</i>	Council of Europe Cybercrime Convention	G8 Lyon Group 2001 Recommendations; G8 Justice and Interior Ministers 2002 Statement on Data Availability to Protect Public Safety
<i>Spam</i>	EU Spam Directive	General consensus that SPAM is bad; ASTA, OECD, ITU conferences and studies	
<i>Human Rights</i>	<i>Privacy/Data Protection</i>	EU Directive on Protection of Personal Data (1995)	ICANN Registrar Accreditation contract (regarding Whois database)
			General Assembly resolution 45/95, December, 1990: Guidelines for the Regulation of Computerised Personal Data Files
			OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (1980)
	<i>Authentication and Identity</i>	Council of Europe Declaration on Freedom of Communication on the Internet	DNS Whois database accuracy (ICANN)
Model Law on Electronic Signatures Resolution 56/80			
IETF DNSSEC standard RIRs securing access to IP address Whois information. Secure BGP			

			ITU PKI Standards UN Convention on Organised Crime
	<i>Freedom of Expression</i>		Durban Declaration of the World Conference Against Racism (2001)
			Commission on Human Rights Resolution 2003/42
			ICANN and WIPO Uniform Domain Name
			Dispute Resolution Policy (UDRP)
			Internet Content Rating Association
<i>Operational Policies for the Internet</i>	<i>Global Resource Management</i>		E.164 code assignment and .int TLD administration (ITU)
			DNS root server administration (ICANN, ISC, others); BIND software
			Country code TLD administration
			IP address administration (ICANN, RIRs)
			Internationalised Domain Names IDN technical standard (IETF)
	<i>Interconnection</i>		ITU Recommendation D.50
			ITU standards for PSTN – Internet interoperability