|  |
| --- |
|  |
| Geneva, 14-16 May 2013 |
|  **Document WTPF-13/INF/10-E 26 April 2013 English only** |

Information Document

# The Internet’s multi-stakeholder model

Source: Richard Hill, APIG - Member of Informal Expert Group

**1. Introduction**

Since the Internet is unique in some respects, traditional governance mechanisms are not always appropriate, and indeed the governance of the Internet has, to date, been provided by a complex mixture of national actions (some *laissez-faire* and some restrictive), extra-territorial assertions of national powers, collaboration between technologists, and collaboration between commercial interests.

This paper describes the multi-stakeholder model that currently governs most aspects of the Internet, and describes its component entities. The paper points out that not all of the component entities are democratic, so the current model is not fully democratic.

Be that as it may, what is more important is whether the current model has worked well or not. The paper analyses various aspects of today’s Internet and argues that the current governance model has worked well in some respects, but not in other respects.

A separate paper argues that there is a role for traditional governance institutions such as intergovernmental organizations, including the International Telecommunication Union (ITU).

**2. The multi-stakeholder model**

Because the Internet is different from other networks, its governance is not the same as that of other networks. In particular, certain aspects of the Internet are not regulated by governments and they are governed by a variety of private sector organizations which are open to a broad range of participants, including in some cases governments. This situation is often referred to as “the multi-stakeholder model”, which has been defined as engaging “technologists, the private sector and civil society in a bottom-up, consensus driven approach to standards setting, Internet development, and management” [[1]](#footnote-1).

It has been said that that multi-stakeholder model has been an essential component in the success of the Internet. This is reflected in the outcomes of the 2005 World Summit on the Information Society (WSIS) which recognize the following categories of stakeholders (see Annex 1):

1. States/governments
2. Private sector/commercial companies
3. Civil society
4. Intergovernmental organizations
5. International organizations, meaning non-commercial, non-civil society, private sector organizations
6. Academic community
7. Technical community

The WSIS outcomes recognize specific roles and responsibilities for the various stakeholders, in particular stating “Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.” (see Annex 1).

Indeed national governments can and do impose national laws on Internet, in particular copyright, trademark, defamation, prohibitions on sale of controlled/illegal substances, prohibitions on sales of pharmaceutics, prohibitions on gambling, prohibitions on certain types of pornography (in particular child pornography), prohibitions on certain types of political speech (hate speech, negation of genocide, promotion of illegal political parties), etc.

In some cases, it is felt necessary to harmonize to some degree national laws that relate to new technologies (including the Internet), and intergovernmental organizations typically undertake this task, either agreeing “soft law” in the form of declarations or resolutions, or agreeing true international law in the form of treaties. This is recognized in the WSIS outcomes.

The WSIS outcomes (paragraph 29 of the Tunis Agenda) state that “The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations”. Paragraph 61 of the Tunis Agenda also uses the term “democratic”.

Democracy can be defined as “government by the people, exercised either directly or through elected representatives”. But it is not clear how to apply this concept to Internet governance because, to some degree, most of the entities participating in Internet governance are not democratic:

1. For sure most governments at present are elected in some way or another, but not all are elected through universal suffrage, and, even where there is universal suffrage, elections can be marred by corruption, fraud, pressure from economic interests, pressure from extremist parties, pressure from religious groups, etc.
2. Private companies are governed by their owners: the other stakeholders (customers, employees, suppliers) do not usually (at least in most countries) have any direct role in corporate governance.
3. Some civil society organizations are democratic, in the sense that their leadership is elected by their members, but some are not.[[2]](#footnote-2)
4. All intergovernmental organizations are democratic in the sense that they consist of elected/appointed representatives of governments, but, as noted above, not all governments are democratic.
5. Some international organizations are democratic, in the sense that their leadership is directly elected by their members, but some are not.[[3]](#footnote-3)
6. Universities are governed/managed by people appointed by governments (for state-owned universities) or by complex processes that typically do not involve students or non-academic staff.
7. The technical community is mostly composed of people who work for commercial companies. See also the footnote to 5 above.

Thus it cannot be said that key current Internet governance institutions are democratic in the conventional sense of the term.

And it cannot be said that a multi-stakeholder model is “democratic”. Rather, a multi-stakeholder model dilutes the influence of the more “democratic” instutitions (governments and intergovernmental organizations) in favor of institutions that are rather more elitist[[4]](#footnote-4).

Of course this may be desirable: a long line of thinkers, starting with Plato, has suggested that rule by a well-informed elite may be preferable to democracy. And, as noted above, important and effective institutions such as private companies and universities are not democracies (nor are armies or organized religions).

Some of the component institutions of the multi-stakeholder model are open in the sense that anybody can contribute to the discussions (but this may be difficult for participants from developing countries[[5]](#footnote-5)), but some are, at least at times, influenced by commercial interests[[6]](#footnote-6). Thus, in a multi-stakeholder model private companies are able to intervene at multiple levels: within some components of the multi-stakeholder model (including goverments) and directly as private companies. Thus it is not surprising that most private companies favor the multi-stakeholder model.

Recent research regarding multi-stakehoderism in the field of enforcement of intellectual property rights suggests that it does not work well for making decisions about public policies prior to those made by the appropriate public decision-making bodies, even if those decisions are non-binding.[[7]](#footnote-7) Such a finding may or may not be relevant for Internet governance in general.

**3. Results of the current Internet model**

But the question is not whether or not the current system of Internet governance is or is not democratic. The question is whether or not that system has worked well.

It has undoubtely worked very well in some respects: in particular the Internet has become a pervasive data transport network, and that this network is used to provide innovative services and applications, such as:

1. A wealth of information
2. Search engines that allow rapid and easy access to that information
3. New business models based on the world-wide-web, such as discount airlines, web-based book sales, etc.

However, the underlying protocols were designed for private networks, not for public networks. Consequently:

1. They did not provide adequate security features[[8]](#footnote-8)
2. It has proven very difficult to add security features subsequently[[9]](#footnote-9)
3. There are no global naming standards
4. There are no agreed accounting/billing standards other than zero-cost peering agreements[[10]](#footnote-10)
5. The domain name system is not compatible with well-established trademark customs and laws[[11]](#footnote-11)
6. The US government continues to have at least nominal control over the domain name system through its contracts with the Internet Assigned Names Authority (IANA) and Versign.[[12]](#footnote-12)

Because of the inherent security weaknesses of the Internet protocols combined with the inherent security weaknesses of the PCs typically used by end-users, and because of the hands-off attitude taken by national governments in the wake of the general trends towards privatization and liberalization of the telecommunications sector, the following have emerged and are considered undesirable by at least some people:

1. Spam and phishing
2. Viruses, botnets, etc.
3. Possible access by minors to extremely hard forms of pornography[[13]](#footnote-13)
4. Use of the network to organize illegal activities such as pedophilia
5. Abuse of domain names, in the sense of cybersquatting[[14]](#footnote-14)
6. Unequal and inequitable distribution of naming and addressing resources, at least historically
7. Regulation of the naming and addressing resources that is heavily influenced by the providers of names and addresses, and whose policies are not always seen to take into account the public good in a meaningful manner[[15]](#footnote-15)
8. Monopoly rents derived from ownership of large blocks of names and addresses, without a clear policy regarding the return of such profits to the public[[16]](#footnote-16)

Various issues can be categorized under two overarching issues: security and financial arrangements.

## *3.1 Security*

There is an important trade-off between safety and security and other public policy goals such as innovation and competition. For example, there would be much more innovation in the pharmaceutical market if safety and effectiveness requirements were relaxed. But policy makers have decided that certain safety standards are mandatory, even if this does hinder innovation. The same holds for many other industries, such as air transport, automobiles, electrical appliances, etc.

The lack of mandatory security and safety standards for the Internet surely encourages positive innovation (such as new business models for the retail sale of books or discount airlines) but it also encourages less desirable innovations (such as web sites offering illegal products or services and free pornographic web sites that do not even display an entry page asking whether users are adults). And it is not disputed that the Internet is being used to wage cyberwar, even though there are conflicting views regarding who is most active in that respect[[17]](#footnote-17).

Thus it would appear reasonable to conduct discussions regarding what, if any, additional security standards should be adopted for Internet and to discuss the extent (if any) to which those standards should be harmonized around the world.[[18]](#footnote-18)

And indeed this has already been done to some extent, for example with the widespread implementation of HTTPS and calls for widespread implementation of DNSSEC and IPsec[[19]](#footnote-19).

## *3.2 Financial arrangements*

At present, it is disputed whether the current financial arrangements for the Internet will result in sufficient return on investments to finance the rollout of sufficient new infrastructure[[20]](#footnote-20).

As noted above, the Internet is based on a “receiver pays” model. This model applies at two levels: at the level of the end-user, and at the level of the international interconnection.

There is general agreement that it is logical for an end-user to pay for something that he or she asked for, for example a video; but there is some question regarding whether the provider of the content should also pay, for example if it wishes to ensure the speed of transmission of its content (this is the “net neutrality debate”).

But “receiver pays” also applies to international interconnections at the wholesale level, and developing countries have long taken the view that it penalizes them, because these countries produce little content and access much content, so they use proportionately more international bandwidth.[[21]](#footnote-21)

Fundamentally, it is obvious that, in a “receiver pays” system, a relatively poor country will obtain less information than a relatively rich country, simply because the relatively poor country has less money to spend.

One might take the view that there is nothing wrong with this: after all, nobody thinks that everybody should drive luxury cars.

On the other hand, one might take the view that access to what is undoubtely the world’s fundamental communication and information system (the “free and open Internet”) should be made available to all at prices they can afford.

So the question becomes how to address the fact that (1) for people in developing countries Internet access is relatively less affordable than it is for people in developed countries; and (2) people in developing countries have relatively less access to Internet than they do to mobile telephones, again when compare to people in developed countries[[22]](#footnote-22). That is, how can we make Internet as available as voice services provided by mobile phones?

Some take the view that liberalization will achieve this goal[[23]](#footnote-23).

Others point out that liberalization has not had the desired effects in some countries[[24]](#footnote-24).

It is not disputed that developing countries have questions and legitimate concerns[[25]](#footnote-25). And it cannot be disputed that discussions on the topics outlined above should continue.

Thus the question is: in which forums should the discussions take place?

**Annex 1: Excerpts of WSIS outcomes**

The Tunis Agenda recognized in paragraphs 29, 35 and 61 various stakeholders and their respective roles:

29. We reaffirm the principlesenunciated in the Geneva phase of the WSIS, in December 2003,thatthe Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.

…

35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

a) Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.

b) The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.

c) Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role.

d) Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.

e) International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

…

61. We are convinced that there is a need to initiate, and reinforce, as appropriate, a transparent, democratic, and multilateral process, with the participation of governments, private sector, civil society and international organizations, in their respective roles. This process could envisage creation of a suitable framework or mechanisms, where justified, thus spurring the ongoing and active evolution of the current arrangements in order to synergize the efforts in this regard.

The contribution of the multi-stakeholder model to the success of the Internet is recognized paragraph 36:

36. We recognize the valuable contribution by the academic and technical communities within those stakeholder groups mentioned in paragraph 35 to the evolution, functioning and development of the Internet.

But additional stakeholders are recognized elsewhere in the Tunis agenda:

73. The Internet Governance Forum, in its working and function, will be multilateral, multi-stakeholder, democratic and transparent. To that end, the proposed IGF could:

a) Build on the existing structures of Internet governance, with special emphasis on the complementarity between all stakeholders involved in this process – governments, business entities, civil society and intergovernmental organizations.

b) Have a lightweight and decentralized structure that would be subject to periodic review.

c) Meet periodically, as required. IGF meetings, in principle, may be held in parallel with major relevant UN conferences, inter alia, to use logistical support."

1. Sally Wentworth, “Testimony”, *5 February 2013 Hearing: Fighting for Internet Freedom, Dubai and Beyond, U.S. House of Representatives Committee on Energy and Commerce’s Subcommittee on Communications and Technology*, available at: <http://docs.house.gov/meetings/IF/IF16/20130205/100221/HHRG-113-IF16-Wstate-ShipmanWentworthS-20130205.pdf> [↑](#footnote-ref-1)
2. ISOC has a rather complex process for selecting the members of its governing body, the Board of Trustees: “ISOC By-Laws and Policies call for the Trustees on its Board of Trustees to be elected or selected by various constituencies, namely Organizational Members, Chapters, the ISOC standards organization embodied by the Internet Architecture Board (IAB) and Individual Members. The Board of Trustees itself is empowered to appoint a limited number of Trustees over and above the constituency-based Trustees”, see:
<http://www.internetsociety.org/who-we-are/board-trustees/policies-and-procedures/selection> [↑](#footnote-ref-2)
3. For example, ICANN has no membership, so its Board cannot be elected in a conventional manner. Half of the members of the ICANN Board are selected by a Nominating Committee, the other half are selected by various other committees, see the ICANN Bylaws.
IETF does not have a formal membership. The selection process for the IESG, the body that makes formal decisions regarding IETF standards, is complex, involving a nominating committee and the ISOC Board of Trustees, see RFC 2727. [↑](#footnote-ref-3)
4. A very good detailed analysis of the shortcomings of the current multi-stakeholder model is given in Olivier Crispin (2013) “What Happened at WCIT in December 2012”, p. 25
<http://fr.slideshare.net/ocl999/what-happened-at-wcit-in-december-2012> accessed 31 March 2013. [↑](#footnote-ref-4)
5. Crespin-Leblond, *ibid.* [↑](#footnote-ref-5)
6. Crespin-Leblond, *ibid.* [↑](#footnote-ref-6)
7. Chistopher Plaum, “Globalization of Law Enforcement: A Study of Trans-National Public-Private Partnerships Against Intellectual Property Crimes, Doctoral Thesis, University of Bremen (2012) p. 230, available at:
 <http://elib.suub.uni-bremen.de/edocs/00103026-1.pdf> ;
a summary can be found in Christopher Plaum, “Global Public-Private Partnerships Against IP Crimes: How Interpol Avoided the Failures of WCO and WHO”, *Intellectual Property Watch* (24 April 2013), available at:
 <http://www.ip-watch.org/2013/04/24/global-public-private-partnerships-against-ip-crimes-how-interpol-avoided-the-failures-of-wco-and-who/> [↑](#footnote-ref-7)
8. See David Talbot, “The Internet is broken”(2006) *MIT Technology Review* (December 2005/January 2006), p. 62
<<http://www.technologyreview.com/news/405318/the-internet-is-broken/>> [↑](#footnote-ref-8)
9. See Talbot, *op. cit.* The situation is substantially the same today as when the cited article was written. [↑](#footnote-ref-9)
10. See Dennis Weller and Bill Woodcock, “Internet Traffic Exchange”, available at
 <http://www.oecd-ilibrary.org/science-and-technology/internet-traffic-exchange_5k918gpt130q-en> [↑](#footnote-ref-10)
11. ICANN’s Uniform Dispute Resolution Process (UDRP) and related activities are measures that were taken to compensate (or to attempt to compensate) for this incompatibility. [↑](#footnote-ref-11)
12. In May 2012, the US Congress resolved that US authorities “should continue working to implement the position of the United States on Internet governance that clearly articulates the consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multistakeholder model that governs the Internet today”. Presumably this resolution refers only to keeping the Internet free from the control of governments other than that of the United States, because the US continued to maintain its control over the Internet Assigned Names and Addresses (IANA) function and of course continued to enforce various measure such as its ban on online gambling. [↑](#footnote-ref-12)
13. Pornography is freely available on the Internet in many countries, which is not the case for other broadcast media. Major free porn sites do not even have an entry page, so the user is immediately presented explicit material. The videos that are available for free are full hard-core videos, of the type that, in the past, could only be purchased in sex shops. In 2012, it was reported that the largest such site had about 4.4 billion page views per month, that is, on average, more than one view per month per Internet user (but of course most Internet users do not access such sites at all, so some users must access them frequently). According to one source these free porn sites account for something like 30% of Internet traffic, see
 <http://www.extremetech.com/computing/123929-just-how-big-are-porn-sites> .
Children and adolescents can easily access these sites, including from their smartphones, and that may have led to a banalization of certain sexual practices, such as sodomy and multiple-partners: in the past, it was difficult for children and adolescents to have access to images of such sexual practices. [↑](#footnote-ref-13)
14. As noted above, this is alleviated by the UDRP and related mechanisms [↑](#footnote-ref-14)
15. See for example the well-informed account at: <http://news.dot-nxt.com/2012/10/12/sickening-nomcom-must-be-refor>. ICANN received some 340 million dollars in 2012 in connection with applications for new gTLDs. [↑](#footnote-ref-15)
16. There are various government initiatives to encourage the adoption of IPv6, when large amounts of allocated IPv4 addresses are unused, and governments take no actions to reclaim those unused addresses. That is, governments are inciting private companies to make additional investments, and to incur additional costs, instead of taking measures to improve efficiency by reclaiming what can reasonably be held to be unused critical infrastructure resources.
ICANN's operating budget for 2001-2002 was approximately US$ 5 million for a staff of 21 full-time equivalents. ICANN’s operating expenses in 2012 were about 70 million US dollars, and in 2013 about 140 million dollars. Revenues in 2012 were projected to be some 230 million dollars. Staff was 158 people in 2012, planned to grow to 189 in 2013.
That is, ICANN’s operating expenses grew by 30% per year during the 10 years from 2001 to 2011, and planned to grow 100% from 2012 to 2013. Staff grew by 22% per year during the 10 years from 2001 to 2011, and was planned to increase by 20% from 2012 to 2013.
This is of course far higher than the growth rates of the economies of most countries, and far higher than the growth rate of most areas of economic activity. [↑](#footnote-ref-16)
17. Not surprisingly, the USA accuses China and Russia of actively engaging in cyber-warfare or at least in commercial cyber-espionage. However, it is generally accepted that the USA and Israel conducted an apparently successful secret cyber-attack on Iranian nuclear facilities, through the Stuxnet virus. And Chinese government researchers have published in the open literature accounts of some of their work. See Richard Stone, “A Call to Cyber Arms”, *Science*, vol. 339, p. 1026 (1 March 2013) [↑](#footnote-ref-17)
18. For a good discussion of a particular issue security-related issue (anonymity and defamation), see Anna Vamialis, “Online defamation: confronting anonymity”, *International Journal of Law and Information Technology*, vol. 21, no. 1, spring 2013, p. 31 ff. [↑](#footnote-ref-18)
19. All three of which rely on the public key encryption scheme formalized in Recommendation ITU-T X.509. [↑](#footnote-ref-19)
20. See AT Kearney, *“A Viable Future Model for the Internet”*, available at: <http://www.atkearney.com/index.php/Publications/a-viable-future-model-for-the-internet.html> ; and, conversely, Dennis Weller and Bill Woodcock, “Internet Traffic Exchange”, available at
 <http://www.oecd-ilibrary.org/science-and-technology/internet-traffic-exchange_5k918gpt130q-en> [↑](#footnote-ref-20)
21. See for example <http://www.itu.int/ITU-T/studygroups/com03/iic/index.html>
and <http://www.itu.int/ITU-T/worksem/apportionment/201201/index.html> [↑](#footnote-ref-21)
22. Broadband and Internet penetration rates are markedly higher in developed countries than they are in developing countries, while the differences with respect to mobile cellular penetration are smaller. In most of the developing world, 2.5G and 3G mobile has grown far faster than fixed Internet. See the ITU Secretary-General’s Report to the 2013 World Telecommunication Policy Forum. [↑](#footnote-ref-22)
23. See Weller and Woodcock, *op. cit.* [↑](#footnote-ref-23)
24. See Susan Crawford, Captive Audience: The Telecom Industry and Monopoly in the New Guilded Age, Yale University Press (2013). A summary is available at:
<http://business.time.com/2013/01/09/is-broadband-internet-access-a-public-utility/?goback=%2Egde_65453_member_204153607> [↑](#footnote-ref-24)
25. Sally Wentworth, “Testimony”, *5 February 2013 Hearing: Fighting for Internet Freedom, Dubai and Beyond, U.S. House of Representatives Committee on Energy and Commerce’s Subcommittee on Communications and Technology*, available at: <http://docs.house.gov/meetings/IF/IF16/20130205/100221/HHRG-113-IF16-Wstate-ShipmanWentworthS-20130205.pdf> [↑](#footnote-ref-25)