INTERNET GOVERNANCE: STRENGTHS AND WEAKNESSES FROM A BUSINESS PERSPECTIVE

Ayesha Hassan

This chapter provides an overview of the strengths and weaknesses of the current Internet governance landscape from the perspective of the International Chamber of Commerce (ICC)[1]. In general, business views the current mechanisms that handle Internet related issues to be functioning well. Stability, security and consistency in the functioning and future development of the Internet are critical to business. Coordination, exchange of information and increased participation of all stakeholders from around the world, particularly from developing countries are the key areas that could be strengthened going forward. These areas will require attention and consideration at all levels---international, regional and national---to make progress.

What is Internet Governance?

"The Internet" refers to the global, seamless interconnection of networks using Internet Protocol (IP). Internet Protocol is a network layer protocol that contains the addressing information and some control information that allows packets to be routed. These networks are privately owned and operated, and have many different properties. They are all based on technical protocols, numbering and naming systems that use widely accepted standards to enable the transport of information across many interconnected networks.

Internet users rely on unique and predictable results in domain name resolution anytime and from anywhere in the world, and a high degree of reliability and stability in the operation of the networks themselves. Since the networks that make up the Internet are widely distributed and operated by thousands of different entities, both large and small, the Internet's infrastructure and operation is a collaborative activity[2].

---

[1] More details about the work of ICC's Commission on E-Business, IT & Telecoms can be found at: <http://www.iccwbo.org/policy/ebitt/>

[2] For more detailed information regarding several of the organizations involved in the technical coordination of the Internet, please refer to ICC's "Information Paper on Organizations Involved in Technical Coordination of the Internet," updated version, 2 September 2003 <http://www.iccwbo.org/policy/ebitt/>

At a minimum, "Internet governance" includes the entire set of multi-stakeholder decision-making processes[3] for technical and public policy matters that affect information and communication technology (ICT) infrastructures and networks, Internet communications, and Internet commerce and applications.

"Internet governance" can be understood as comprising the following elements:

- the technical standardization activities that promote interoperability of Internet Protocol (IP) applications as well as network security, reliability and quality for the Internet;
- the technical coordination of the key protocols and addresses and names that underpin the technical functioning of the Internet; and
- the handling of public policy matters.

No single body performs all of these functions. Indeed, different stakeholders are leading, and should continue to lead on different components and sub-issues under each component. In addition, the Internet depends on other infrastructures, e.g. the telecommunications infrastructure to provide an underlying global platform, the energy infrastructure to provide power to operate user and network ICTs, the education infrastructure to educate and train people to use ICTs and their applications and to design, build and operate the Internet.

Technical Standardization and Internet Protocol Standards

Technical standards allow different components of the Internet to inter-operate and to provide secure, reliable and high-quality networks. Besides the Internet Engineering Task Force's (IETF) STD005, which defines the Internet Protocol (IP), the IETF develops many open, voluntary consensus-based interface and protocol standards that facilitate the development of hardware and software capabilities at Open System Interconnection (OSI) layer 3 and above. [4]

The Internet Architecture Board and the Internet Engineering Steering Group provide engineering management and process review functions for the IETF to ensure that the open,

[3] "Multi-stakeholder decision-making processes" here is taken to refer to activities in which governments, business and civil society each actively participate to create normative information. The actual design, deployment, operation, administration and maintenance of ICT networks and their applications by individual network operators and service providers may draw upon information from multi-stakeholder processes, but they are not multi-stakeholder process themselves. Similarly, important activities, such as those performed by the ITU-D, to broadly disseminate information about ICT technologies, standards, and regulations; to provide education and training on ICT, and to provide technical assistance are not viewed as "Internet Governance". These latter functions are discussed throughout the document to complement the discussion of Internet Governance.

[4] For further information regarding the OSI model see <http://www.webopedia.com/quick_ref/OSI_Layers.asp>

voluntary, consensus-based process works properly. The World Wide Web Consortium and specialized forums such as the Session Initiation Protocol Forum provide additional technical specifications for Internet applications and use to meet user needs. The International Telecommunication Union's (ITU) Telecommunication Standardization Sector (ITU-T) and Radiocommunication Sector (ITU-R), as well as other standards development organizations, develop the technical standards for the transport technologies at OSI layer 2 and below for wire line, wireless, cable, fiber optics, satellite, and other facilities. The ITU's Development Sector (ITU-D) assists developing countries by, among other activities, disseminating information on ITU standards, and producing reports on emerging technologies/applications and how they relate to existing infrastructures and services.

Each of the entities mentioned above plays an important role in ensuring the interoperability of networks to allow for seamless Internet communications. Business supports each of these organizations maintaining its current role and mandate, and stresses the critical importance of international, open, voluntary, consensus-based development of standards led by the private sector and market forces. As our use of the Internet grows, it is even more important that these organizations cooperate. These entities need to respect each others' expertise and establish mutually agreed-to working relationships[5] that recognize and promote private sector leadership and participation, and are based on a commitment to standards cooperation.

All of the above standards are voluntary, which makes them flexible and able to adapt to a rapidly changing technical environment. An exception is standardization of radio spectrum in ITU-R. Spectrum is a limited resource, so its use is regulated subject to global treaty agreements. The ITU also convenes world treaty conferences to identify, assign and allocate radio spectrum to support the transport infrastructure. The Internet is not a limited resource, and does not need to be regulated in this way.

Technical Coordinator of the Internet Names and Numbers System

Among the key elements that have been broadly discussed within the World Summit on the Information Society (WSIS) and the Working Group on Internet Governance (WGIG) processes is the technical coordination of the Internet names and numbers system. This function is performed by the International Corporation for Assigned Names and Numbers (ICANN), a not for profit global corporation. ICANN exists, first and foremost, because it is essential to ensure the stable functioning of the global Internet. ICANN is a rapidly adaptive

[5] For example, RFC 3356 is the "Internet Engineering Task Force and International Telecommunication Union - Telecommunications Standardization Sector Collaboration Guidelines", August 2002. It was approved by the ITU-Ts Telecommunications Standardization Advisory Group (TSAG) as Supplement 3 to the A-series Recommendations. It is at <http://www.ietf.org/rfc/rfc3356.txt?number=3356>

process that can be responsive to the dynamic nature of Internet growth and evolution in the area of assigned names and numbers, and the system for mapping between them.

The critical parts of this process are:

- the administration, coordination and allocation of IP addresses and the delegation of generic top level domain names;
- the administration and coordination of the root server system;
- the coordination of procedures related to the technical coordination of the Internet;
- the coordination of relationships with other entities, such as the regional addressing registries and the Country Code Top Level Domain (ccTLD) registries;
- promotion of competition within generic top-level domain name space (.com, .org, .net, etc);
- matters related to these functions, such as a system for domain name dispute resolution.

Along with these key responsibilities, ICANN, along with other organizations, has been addressing new challenges, such as introducing multilingual or Internationalized Domain Names (IDN) into the generic TLD domain name system (DNS), and encouraging them in the ccTLDs by issuing guidelines and approving standards for full interoperability between the different languages. Progress in IDN can establish an environment to encourage the development of content in multiple languages and promote greater cultural diversity in Internet content. Other challenges that will need to be addressed in the future are the move to IPv6, the growth of ENUM[6], the maintenance of stability of the core elements of the underlying protocols, names and numbers throughout the upcoming rapid expansion of the Internet's users.

It is important to note that ICANN has a limited mission focused narrowly on the technical coordination of the Internet functions identified above and directly related technical policy areas. ICANN does not take responsibility for general public policy matters related to the Internet.

The Government Advisory Committee (GAC) of ICANN is comprised of members from national governments and intergovernmental organizations such as the ITU, Organization for Economic Cooperation and Development (OECD), and World Intellectual Property Organization (WIPO). It is open to all United Nations member states. The GAC advises on ICANN activities as they relate to concerns of governments, particularly if the issues that are

[6] 'ENUM' refers to the IETF protocol that takes a complete, international telephone number and resolves it to a series of URLs using a Domain Name System-based architecture. (source: <http://www.enum.org>)

being addressed by ICANN would benefit from insights on laws, international agreements or public policy issues. The GAC has a strong role in ICANN, particularly following the ICANN reforms adopted in November 2002. Strengthening the level and geographic range of participation by government representatives in the GAC will be an important evolution.

Business supports each of the organizations identified in prior sections maintaining its current role and mandate, and the importance of private sector leadership in the technical management and development of the Internet. Business and the ICC in particular do not support the transfer to an intergovernmental body of any of the functions performed by private sector led organizations, or organizations that function as a partnership between the private sector and users.

Public Policy Issues

Public policy matters are the responsibility of governments. However, policy discussions must include the active participation of business and other stakeholders and should be motivated by broad national public objectives, e.g.:

- Promoting economic/infrastructure growth and development
- Attracting capital and encourage investment
- Stimulating innovation and creativity

While a public policy deliberation can result in governments regulating a particular activity, refraining from regulation, promoting a competitive environment or allowing business to self-regulate can increase user choice and reduce costs. Therefore, a public policy might be to forbear from regulating where it is not essential. Business believes forbearance to be a wise strategy in an area of rapid change and technological development to avoid constraining regulations that inhibit the use and deployment of technologies.

Public policy matters related to the information society include:

- privacy
- trade
- security
- education
- spam
- intellectual property protection

There are several other Internet related public policy issues, such as telecommunications infrastructure-related matters, and consumer confidence/empowerment and others which are not elaborated in this chapter for reasons of space, but that are important.

Many of these issues can benefit from *international cooperation and action*. There are international bodies such as WIPO and the World Trade Organization (WTO) with authority and jurisdiction for some of these issues. Other issues require *international coordination of national policy*. A number of bodies exist such as the OECD, Asian Pacific Economic Cooperation (APEC), and Inter-American Telecommunication Commission (CITEL) where these issues can be discussed and coordinated.

Strengthening the coordination and exchange of information amongst the bodies that are discussing these issues and developing important guidelines and best practices will be important. In addition, creating ways to ensure greater participation of all stakeholders, as relevant, from all geographies, will ensure a deepening of involvement in these bodies and enrich the outputs.

Capacity building is a critical element that needs particular attention in the immediate future to ensure that the Internet and the information society is truly people centered. This is related to Internet governance as without this element greater participation by all stakeholders from around the world will not be achievable.

Education

Throughout the WSIS and WGIG processes over the past four years, business advocated the importance of a sound education system as a fundamental building block to the creation of a truly global information society. Education is essential to derive sustainable benefit from the information society. Without the requisite education, including basic tools such as literacy and more targeted tools such as computer literacy, citizens will not be able to use the deployed infrastructure and equipment to access the Internet. Governments should ensure a framework that will develop the requisite skills to engage in an information society, through appropriate public/private partnerships.

Such a framework includes providing basic education, equipping young people with ICT knowledge and skills, recognizing the importance of lifelong learning in ensuring that the workforce skills do not become obsolete, and promoting private sector investment in training and development, which is important to retaining skilled workers and preventing 'brain drain'. Governments should also build a culture that promotes entrepreneurship.

Governments, along with other stakeholders, should also ensure that opportunities exist to obtain the specialized skills necessary to design, build, and operate ICT infrastructures to support the critical national needs for these capabilities.

Speech and Content

The Internet is a vibrant and growing medium for communicating, sharing information and knowledge, and doing business. Excessive regulation of Internet content will inhibit its flow and diminish the benefits of the Internet. Business proposes the following recommendations to governments on Internet speech and content:

- allow self-regulation to demonstrate its efficacy---filtering, labeling and self-regulation should be carefully considered as alternatives to legislation;
- regulation, when necessary, should be kept to a minimum and only deal with specific, observed abuses, taking account of existing technologies;
- laws and regulations should be clear, precise and narrowly tailored;
- legislation should not place additional costs and burdens on business beyond those born by users and government;
- jurisdiction and applicable law mechanisms should not expose business to unexpected risks that they are subject to laws and judgments in other countries;
- provisions dealing with liability should limit the liability of technical service providers in a manner that balances the interests of all stakeholders.

Privacy

The protection of personal data is an essential element of building confidence in the use of information and communication technologies and the Internet.

The general functions of privacy policies are as follows:

- *Identification:* identification includes analyzing technological trends, isolating threats to consumers, and suggesting how consumers might be protected from those harms. This can be done by businesses themselves, central authorities, regulatory agencies within their scope of responsibilities, legislative committees and academic research centres.
- *Education:* Consumers need to be educated about the uses of information, benefits those uses create, risks, and consumer rights and responsibilities. This education is the responsibility of government, business, consumer organizations, non-governmental organizations and even the media.
- *Implementation:* Implementation of privacy protection principles can be done directly, through legislation on either a sectoral or omnibus basis, as appropriate, and ensuring maximum clarity and flexibility, or through self regulation, use of appropriate technology or other 'bottom up' processes including sectoral and/or company codes of conduct, corporate rules and individual customer empowerment.
- *Enforcement:* There are numerous ways to ensure that privacy protections are enforced, for example, through self-regulatory initiatives, legislation, regulation, or other forms of third party oversight. The most important part of enforcement is not the type of organization, but that it promotes trust in the data protection regime.

Business advocates a privacy protection regime that offers sufficient protection to citizens while allowing the economy to flourish and thrive. Governments, business and other groups should agree on a solid core of privacy principles and then enable business to meet these requirements in a flexible manner that allows for cultural and business practice variations that are part of a thriving, competitive economy. The OECD adopted Privacy Guidelines[7] in 1980 that represent an international consensus on such a core set of principles. In November 2004, APEC adopted a Privacy Framework consisting of a set of principles, guidance for domestic implementation and a future work programme for cross border implementation.

With this background, business has recommended the following items for government actions to strengthen privacy frameworks.

- Adopt a set of principles to ensure adequate data protection, such as that included in this document, and in so doing, not exceed the principles set forth in the 1980 OECD Guidelines.
- Adopt a flexible and responsive approach to the protection of personal information, including the acceptance of self-regulatory solutions and technological innovations that empower the user, determining where specific laws are needed to protect consumers from harm and enact those laws in the most targeted fashion possible.
- Educate the public about privacy protection and the use of privacy-enhancing technologies.
- Cooperate internationally to ensure a seamless environment for different privacy regimes. In assessing the level of protection provided to personal information in other jurisdictions, the criterion should be the objective level of protection afforded by the system as actually used in practice within that jurisdiction.
- Avoid developing laws, policies and practices that create obstacles to crossborder flows of personal data.
- Endorse model contracts, codes of conduct, seal programmes, and other self-regulatory mechanisms prepared by the private sector in order to promote the free and secure flow of information within and between companies, and across borders.

Security

Business, and ICC in particular, strongly supports a global culture of security consistent with the OECD Guidelines for the Security of Information Systems and Networks, and United Nations General Assembly Resolution on this issue. ICC and the Business and Industry Advisory Committee to the OECD (BIAC), have developed "*Information Security Assurance for Executives*", a guide to help the global business community in fulfilling its role in the global culture of security. ICC and BIAC have also developed "*Information security issues and resources for*

[7] Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* 1981 <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>

small and entrepreneurial companies, A business companion to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security". This second application of the OECD security guidelines is directed especially at companies that do not have a dedicated ICT function or expertise.

Appropriate laws are necessary to address cybercrime, but laws are not necessary to mandate particular levels of security. Some laws and regulations could undermine security by offering hackers information as to the security measures deployed pursuant to such laws/regulations. Moreover, different sectors and different types of information and communication require different levels of security, making a flexible approach to security the most effective.

ICC proposes the following actions at the national level for governments:

- take steps to secure government networks and infrastructures;
- support private sector leadership in the development and deployment of technology solutions and services, and information-sharing mechanisms;
- remove controls on cryptographic technologies and applications; and
- educate all stakeholders on issues related to security.

Spam

Business is a victim of and a partner in the fight against spam, i.e. "fraudulent and unsolicited harmful e-mail". Spam is detrimental to consumers and business, as both are users of information and communication technologies. Governments should distinguish between fraudulent and untargeted commercial communications and legitimate commercial email, prohibiting the first two, while recognizing that the third plays a significant role in the emergence and growth of electronic commerce.

- *Education and cooperation:* Stakeholders must work together in public/private partnership to educate users in the fight against spam.
- *Technology:* Industry should continue to develop technological solutions to spam, working with governments and consumers to promote awareness of technological approaches.
- *Industry's role in fighting spam:* Anti-spam measures should distinguish between legitimate commercial e-mail and spam. Business can best manage legitimate unsolicited commercial e-mail with industry codes of conduct and other self-regulatory tools, while government enforcement is needed to combat spam.
- *Government Regulation/Enforcement:* Governments should ensure that existing legislation covers spam and is effectively enforced. New legislation or amendments, where needed, should focus on preventing illegitimate, fraudulent, or harmful messages.

The fight against cross-border spam is largely a matter of law enforcement cooperation. The OECD recommendations on cross-border fraud provide guidance on these issues[8]. Other international efforts are being made by the London Action Plan and through bilateral and multilateral memorandums of understanding to increase efforts to facilitate cross-border cooperation on enforcement actions against spammers. Concrete government actions, like active facilitation of international enforcement actions, are essential in fighting spam.

The ICC recently launched a Global Online Spam Resource, a global spam-fighting resource to help Internet users reduce their exposure to unwanted email[9]. The resource is an evolving project that contains practical information on how to opt out of unsolicited commercial email and spam in over 30 countries. It lists data protection authorities, direct marketing associations or other public and private organizations to which email users can report spammers and lodge complaints about privacy infringements.

Legal Frameworks

Intellectual Property Protection

It is essential to recognize that the existing international intellectual property system represents a delicate balance between the needs of the creator and the user, and is designed to promote innovation and creativity to benefit society as a whole. Intellectual property rights (IPRs) contribute to society by helping competition, encouraging the production and dissemination of a wide range of quality goods and services, underpinning economic growth and employment, sustaining innovation and creation (including the stimulation of local content), promoting technological and cultural advances and expression, and enriching the pool of public knowledge and art.

Strong intellectual property protection promotes economic and social development by stimulating innovation and investment. Business urges national governments to put into place the necessary measures to allow the intellectual property protection system to fulfill its potential as a tool for development, growth and progress. Any further discussions about intellectual property in the information society should be conducted within the United Nations specialized agency, the WIPO.

Fraud, Cybercrime and Law Enforcement Cooperation

Business strongly supports efforts to combat fraud on the Internet. Fraud undermines the commercial viability of the Internet for legitimate businesses. Therefore, business is eager to

[8] see <http://www.oecd.org/document/50/0,2340,en_2649_34267_2514994_1_1_1_1,00.html>

[9] see <http://www.iccwbo.org/policy/ebitt/id2399/index.html >

work with governments to identify mechanisms to combat fraud on the Internet. International cooperation is vital.

A key element to combating this problem is effective law enforcement cooperation. Every government should ensure that it has the tools to cooperate with law enforcement agencies from other countries. In this regard, business will cooperate with law enforcement in a manner consistent with business realities. The OECD recently adopted Guidelines on Cross-border Fraud. These Guidelines are a model for such cooperation.

The Council of Europe adopted its Convention on Cybercrime in November 2002. This Convention is open to signature by non-member Governments through a political process. As governments begin to implement the convention, ICC encourages them to consider the following factors:

- preventing conflicting privacy and security obligations;
- limiting service provider liability in a manner that balances the interests of all parties including copyright owners, service providers and users;
- adopting clear procedural safeguards;
- providing reimbursement for costs of compliance;
- identifying the appropriate circumstances for corporate liability;
- maintaining criminalization of copyright infringements;
- ensuring consistency between the misuse of devices provisions of the convention and existing law concerning anti-circumvention.

Technological Neutrality with Respect to User Choice

To promote innovation, increase access and foster diversity of choice, governments should adopt a policy framework that maximizes competition and allows users of technology to choose the technology that best meets their specific needs based on considerations such as performance, quality, reliability, security and life-cycle cost.

Government policies that limit choice, or that promote one form of technology over another, can deprive users, including governments themselves, of the best solutions and the full benefits of available technologies. This can stifle both competition and innovation, and potentially impair economic development, productivity and growth.

Conclusion

The Internet governance structures and mechanisms work well today. Business supports the existing organizations maintaining their current roles and mandate, and the importance of private sector leadership in the technical management and development of the Internet.

Business views the evolution, development and improvement of these structures as keys to unleashing the full potential of the Internet for all. The free flow of information, access, and full integration of ICTs and the Internet as tools for economic growth and social development will be enhanced by national level multistakeholder action, coordination and exchange of information at the national, regional and international levels, and increased participation of all stakeholders from around the world, particularly from developing countries.