



International Chamber of Commerce

The world business organization

Department of Policy and Business Practices

ICC informal input on issue papers produced by the Working Group on Internet Governance (WGIG)

Members of ICC's Commission on E-Business, IT and Telecoms (EBITT) are pleased to provide these informal comments and suggestions on several of the draft issue papers that are available for public comment. This input is based on existing ICC members' priorities and positions, but have not received the standard comprehensive consensus building review and comment of all ICC national committees and members due to the short timeframe for public comments on these papers. ICC members look forward to providing the WGIG with additional comments as the drafting process progresses.

“Technical Standards” issue paper:

- Issues section, 4th paragraph: Regulatory requirements should be known at an early stage of standardization so that they can be taken into account. Generally, standards for the world market are consistent with regional standards. Harmonized regulatory requirements from different regions (admittedly not always easy to achieve) are highly desirable in order not to burden a standards-conformant product with diverging features requested by regulations.
- Section 5. Forums:
 - 2nd item: also holds for ETSI
 - 3rd item: in IETF formally only individuals act, however companies delegate a lot of “individuals” to IETF and heavily influence its work and outcome as consistent with their company's priorities.
- Section 6. Governance mechanisms:

Besides radio frequency regulations there are several other fields where national laws or regulations might apply (e.g. emergency communications, lawful interception, disability access etc); the discussion centers around the question: Whether or if technology-neutral regulation/governance should be aimed at? Or, should Internet services be viewed as something not affected by such regulation? Certain important features such as emergency communications and lawful interception will probably sooner or later be requested, irrespective of the technology used, in many countries.



- Suggestion: it may be helpful and appropriate to add a list of recommendations which indicate possible improvements to the current gaps/shortcomings as identified in the paper
For example:
 - establishing a constant and effective information flow between standardizers, regulators, politicians, government people, users where this does not currently exist; and
 - changing the statutes of certain standards development organizations so as to allow direct participation of all stakeholders concerned.
- General Comment: This paper explores “whether there is, and should be, a governance regime applied to the creation and deployment of technical standards for the Internet”:

Currently there are numerous standards organizations developing Internet standards (e.g. W3C, IETF, OASIS, ITU, vertical industry organizations (e.g. health, automotive, financial)), a plethora of successful Internet standards (e.g. TCP/IP, XML) and several types of technology standards (de facto, de jure, proprietary, product, open), all resulting in a high level of interoperability for the Internet and Internet-related technologies, products and services. Their purpose is to promote interoperability, efficiency, increased functionality, productivity and economic growth. Voluntary processes have proven to be the most effective means of fueling innovations through standards. The market-place, responding to consumer demands, is best situated to determining the appropriate timing and substance for the development and promotion of standards. As evidenced by the successful and rapid promulgation of the Internet, suppliers have been able to respond quickly to industry and consumer needs by developing standards that most effectively address interoperability issues and embrace the direction of the market place.

On the other hand, government-mandated standards in the technology industry can often result in a number of unintended consequences. These consequences may include: (i) unnecessarily freezing the development of new technologies and failing to reap fully the benefits of such quickly evolving technologies; (ii) inadvertently disadvantaging certain market competitors; (iii) hindering market acceptance and penetration; and (iv) precluding a multi-faceted competitive environment. The method of development of a standard is not ultimately the critical factor that determines its acceptance. A successful standard is one that solves the problem for which it is intended. Typically, the development of such standards is achieved through a natural and dynamic process that is voluntary and responsive to market demands.

Efforts like the one contemplated to create a central governing regime, will impede technical innovation, stifle competition, and will be severely challenged to remain abreast of market/industry needs and technical developments.



Some corrections to specific statements:

- Section 1, para 5. For the most part companies do not engage in standards development to gain and/or sustain competitive advantages. They engage to collaborate on developing technical interoperable solutions where necessary (wide-spread adoption of solution may be explicit or implicit). Standards therefore ultimately level the playing field for all participants and foster competition and innovation (on top of the standard).
- Section 3: Term of art and longstanding practice for licensing patents in standards is RAND – reasonable and non-discriminatory. This may or may not include royalties. Licensing copyrights in standards specifications is typically done on royalty-free terms (or for a reasonable fee (to defray operating costs)).
- The categories of Internet standards development in Section 1 are not mutually exclusive. Standards Development Organizations (SDOs) have a number of attributes, e.g. geographic scope, membership criteria, technical scope and expertise.
- In the case of the Internet, interoperability is so critical that standards-based solutions are widely deployed. Therefore, it may be more appropriate to identify “de facto” standards at the end of a list rather than as the first item.
- Cooperation and coordination between standards bodies sometimes is stimulated by national or regional SDOs that work to promote global standards and/or by SDOs that are focusing on technical standards that complement each other, e.g. core network-to-access network interworking, or layered standards.
- The production of technical standards includes the four steps identified, but also has feedback based on implementation experience, technology evolution and the need for additional features that drives a new set of requirements that makes the process a “standards life cycle”.
- Decisions by standards bodies frequently contain many proposals and solutions. So a new standard can favor a variety of parties, including even parties who did not make proposals themselves. The competitiveness and the importance of interoperability within the Internet market lead to a market characterized by standards-based technologies from multiple suppliers rather than de facto standards driven by dominant companies.
- An important point that should be made related to standards is that users benefit from leading-edge technology that address user needs and provide creative capabilities and features. Innovation can be stimulated when innovators benefit from it and thus can afford the research necessary to sustain it. For this reason, the patent policies of many standards bodies includes permitting licensing of patents on a reasonable and non-discriminatory basis.



- The IETF is open to individual participants from all stakeholder groups, not just civil society. Influence within the IETF results from innovative ideas and technical expertise rather than being dependent upon which stakeholder group originates a proposal.
- The membership of the ITU is not open to industry, in general, or to a broad class of non-profit organizations. Its membership is drawn from companies and organizations in the telecom industry.
- Section 6 on “Governance mechanisms” should note that in a dynamic market like that associated with the Internet, technology evolution and innovation is so rapid that standards processes must be fast enough to keep pace so as to address market needs on a timely basis.
- In Section 7, groups such as ATIS can be better described as “complementing and advancing” rather than “coordinating”.
- Also in Section 7 discussion on the relationship between standards development and policy-making, the point should be made that participants in SDOs are looking for practical, implementable solutions based on standards. Therefore, even if they do not explicitly discuss policies, they are informed by the policies and policy implications in the countries of interest to them.

Consumer, User Protection, and Privacy issue paper

- This paper does not represent the full spectrum of views and is extremely weighted towards the views of a specific stakeholder. It needs further revision to reflect a balanced set of view points.
- The third paragraph beginning “User Protection is a narrower issue,” seems to accuse service providers of manipulating factors against the interests of the consumer which is not a fair reflection of the facts. While it may be true that *dishonest or unscrupulous* entities may act fraudulently to the detriment of consumers, this paragraph groups all service providers under the same umbrella and fails to recognize that by and large, service providers have a vested interest in insuring and creating trust in the online environment. We urge the last two sentences of this paragraph to be deleted.
- The definition of “privacy protection” in the following paragraph is overly narrow. Use for which “the purposes the person has allowed” implies that consent is always necessary. This is not the case, for example with publicly available information or under certain other circumstances.



- Not all stakeholders see privacy as a human right. This fact is recognized in the following paragraph. Therefore, the opening clause in the 5th paragraph should be removed. The paragraph should read “Privacy protections must be balanced with the competing and legitimate interests of government and business...” Further, the paragraph seemingly sets the “right” of privacy above all other societal interests and fails to recognize that there are other competing “rights,” i.e. security, that in many instances are in conflict with or may outweigh privacy interests.
- The US-EU Safe Harbor is not an attempt to bridge the differences regarding the status of privacy protection as a human right or not, but rather a compromise between systems that rely on self regulation and government imposed regulation. The relevancy here is also uncertain, as this is a specific agreement that serves a particular purpose for a subset of industry in one country. The paragraph should be deleted.
- Issue section: In the last paragraph in the issue discussion, for clarity, the sentence should conclude with “how long should information about oneself be available on the Internet.” In the penultimate paragraph in the issues section, additional language should be added so as to read “Privacy protection can add to the costs of providing service and content over the Internet, without any resulting benefit to the end user. And in some cases (i.e. mandatory access) may result in the consumer being less secure in their online activities.”
- “Users” of the Internet can include businesses. Discussion related to consumer protection should therefore be limited to “consumers”.
- SWOT analysis section: the second paragraph in the SWOT analysis should be deleted.
- The tone of the non-profit actor discussion should be revised. At the very least, this section should read “the groups sometimes represent divergent interests.”
- Actors section: Privacy enhancing tools (PETs) are a technology, not an actor. This should be removed.
- Governance mechanisms section: in the section on governance mechanisms, it is not correct to say “The objective of governance is to advance consumer protection.” Rather, it would be more appropriate and correct to say “Governments seek to ensure consumer protection and maximize consumer benefit.” Also in this section, it is unbalanced to present consumers as being protected “against the whims of both the government and the retailer.” This sentence should be deleted. Rather, the paragraph could begin “Privacy legislation is usually targeted...”
- The OECD Privacy Guidelines could be cited as a multilateral agreement on privacy, as could the Council of Europe. We suggest deleting specific reference to the EU Directive, especially as a “benchmark”. Likewise, discussion of which countries have and have not met this mark should be deleted.



- Additional Comments section: the additional comments focus negatively on specific perceived situations in one country, the USA. This should be deleted.

E-Commerce issue paper

- Listing “The failure to successfully include many developing countries in the development of overall e-commerce governance initiatives, as well as in action on many of the specific issues...” as a weakness of the current system is perhaps an overstatement. It also contradicts the discussion of international forums working on e-commerce issues which include many global intergovernmental organizations such as the WTO, WIPO and ITU. Moreover, several developing countries participate in APEC, which is listed as a regional organization, and OECD is making a focused and concerted effort to outreach to non-members.
- Threats section: We would question the inclusion of “protectionism”. As this is not one of the main concerns specific to the development of a system to govern e-commerce, it would seem more appropriate to delete it or list it last.
- The threats posed by differing legal, institutional and cultural systems extends beyond content issues. This seems to be the specific issue regarding jurisdiction over content on the internet illegal only in certain countries. Therefore, we suggest deleting the final clause on the last bullet, “particularly in relation to content.”
- UNCITRAL has also developed a Model Law on Electronic Signatures and is in the process of finalizing a Convention on the Use of Electronic Communications in International Contracts. These instruments should also be recognized.
- The section on adequacy against the Declaration of Principles is overly negative, especially regarding “the ideals of transparency and democracy.” It is not clear from the paper why the many fora discussed are not considered transparent or democratic. The first sentence of the section should be deleted and the third paragraph edited to read “The various e-commerce fora differ in the extent to which they can be considered transparent and democratic.”
- While the paper rightly recognizes that “E-commerce is a meta issue that groups a large number of sub-issues...” it seems to imply that there should be a “coordinated governance action at the international level.” The fourth paragraph probably fits better, therefore, under the SWOT analysis. The final phrase in this paragraph should be deleted.



Some suggestions for additions and deletions to strengthen the paper are as follows:

- Bottom of p.1: Suggest that point 1 at the bottom of p. 1 be revised to change the emphasis from physical vs. intangible products, to products and services delivered off-line vs. products and services delivered online. So point 1 would read: **"The extent to which the arrangements and mechanisms that have been developed to govern trade and commerce in products and services delivered off-line should apply [with equal force] to trade and commerce in such products and services when delivered online."**
- The paper lists "trade" as another issue for which the WGIG will provide a paper, but an issue paper has not been made public. Particularly if there is no dedicated trade paper, we recommend adding a fourth governance issue at the bottom of p.1 / top of p.2: **"How to ensure that governments do not impose tariff or non-tariff barriers to trade in products and services delivered online, which would have the effect of preventing domestic firms and consumers from realizing the full benefits of e-commerce."**
- The second full paragraph under point 3 ("SWOT Analysis") lists various mechanisms for governing e-commerce, but fails to mention consumer education and technology tools. Thus, it is recommended that the paragraph be revised to add the following clause at the end of the final sentence: **"including through consumer education efforts and by developing and offering technology tools that empower users to take effective action against unlawful or objectionable e-commerce practices."**
- In the section on "opportunities" enabled by e-commerce, we recommend revising the first bullet point at the top of p. 4 to add, at the end of that sentence: **"including by enabling suppliers in the developing world to deliver products and services to purchasers in foreign markets and to avoid having to use intermediaries to engage in such trade."**
- In the section on "threats" (top of p. 4), revise the first bullet point to add the following language (new text underlined): **"uncontrolled annoyances and criminal activities that undermine consumer acceptance and uptake (e.g., spam, phishing and identity theft, other forms of fraud), and the risk that governments may adopt conflicting approaches to dealing with these problems."**
- Revise the second bullet point in this "threats" section to read: **"protectionism (e.g. concerns in developed countries about outsourcing jobs to developing countries, efforts in both developed and developing countries to protect established industries from online competition from foreign suppliers."**
- Revise the first bullet point under point 6 ("Governance mechanisms") at the top of p. 6 to cover a broader range of treaty obligations beyond just GATS and TRIPS, so that the bullet would read: **"treaty arrangements, including those governing trade in goods, information technology products, government**



procurement, telecommunications and other services, and protecting copyright in digital works"

- Finally, the second and third paragraphs of Section 7 (p. 6) seem to undermine substantially all current e-commerce governance efforts by stating that they fail adequately to take account of the interests of developing countries and consumers. Certainly, steps need to be taken to enhance and improve dialogue on best practices and approaches among all nations, and the forums identified in the paper itself as playing an instrumental role in e-commerce governance (e.g., WTO, UNCTAD, APEC, WIPO, UNCITRAL, ITU) are committed to improving transparency and participation of all stakeholders.

Cybersecurity and Cybercrime issue paper

- In general, this paper is US-centric. These papers are supposed to be evaluating and discussing the issues as they relate to global internet governance systems, rather than specific countries' treatment. Although this appears throughout the paper, references to and quotes from the "Report of the President's Working Group on Unlawful Content" should be removed. Similarly, the section on the role of the government in this paper should be revised to be more representative of the global information society. And the fact that the U.S. is likely to ratify the Council of Europe (COE) Convention is not likely to be relevant to the discussion of this Convention in the paper's section on international organizations, if leaving this discussion in the paper is considered appropriate (although this is highly questionable), the paper should not include unsubstantiated statements that the Convention will be harmful to privacy.
- Some actions included as examples of cybercrime under the discussion of the issue are not necessarily cybercrime. For example, while child pornography is a crime under the Council of Europe Convention, the storage of pornographic material is not. "Illegal distribution of racist or sexually explicit materials" is very vague and may not be a criminal offence in all countries. For example, this could be seen as conflicting with the US First Amendment. Furthermore, the paragraph should be revised for clarity and not to refer to a report of unknown origin. Perhaps a simple list of different types or categories of cybercrimes would be more clear.
- The 10th paragraph on the section on assessment of risks, beginning "The matter of regulation of the internet" could be viewed as incorrect. Comparative levels of privacy protection between the US and the EU is a highly debated subject. Moreover, the relevancy of this comparison in this paper is uncertain, as ID theft is not primarily a cybersecurity problem and privacy is not a cybersecurity problem at all. We urge deletion of the paragraph as a whole.
- The final paragraph in the section discussing governments' roles should be revised. While it is true that countries and stakeholders differ in the preferred degree of participation of the private sector, it is a fairly universally accepted view that there must be a holistic approach to cybersecurity. Indeed, the OECD Information



Security Guidelines promote a “Culture of Security” in which all stakeholders have a role.

- The paper’s listing of “stakeholders” for 10 different spheres of security issues (page 6) underestimates the role of the private sector. The private sector should be added to each of the following sections: Crafting laws, Regulation, Consumer protection, and Public awareness.

Unlawful Content and Access Protection issue paper

- In the opening “Issue” section’s discussion of labeling, it’s the “methods” which have been found to be fallible, not the “systems”.
- In the SWOT analysis, the weakness section should be further elaborated. The application of differing laws with regard to legal content is more than confusing to content providers. Moreover, to effectively enforce their laws on the internet, such laws would have to be applied on an extraterritorial basis. In the context of the internet, this is often impossible for content providers to comply with. It is also confusing and often technically impossible for service providers, as some countries also seek to put the burden of enforcement on ISPs, despite obvious extra-territorial implications for both services and content.
- Threats section: the objection to compulsory filters under the threats section should be left to national law if this is referring to filters imposed by certain governments. Also under threats, the reference to “extra judicial” should likely be “stakeholder direct action (which itself may be outside the scope of legal proceedings)”.
- Actors section: The government role in partial (and extra-territorial) denial of access is key, but the section should not imply that ISP installation of filters is effective to the government end. ISPs may attempt to install filters or implement other technical measures to give effect to a governmental decree, and while these attempts do create cross-border denial of access and service issues, they frequently do not effectively achieve the desired government ends.
- In the SWOT analysis, the weakness section should be further elaborated. The application of differing laws with regard to legal content is more than confusing to content providers. Moreover, to effectively enforce their laws on the internet, such laws would have to be applied on an extraterritorial basis. In the context of the internet, this is often impossible for content providers to comply with. Some countries may also seek to put the burden of enforcement on ISPs.
- Threats section: the objection to compulsory filters under the threats section should be left to national law if this is referring to filters imposed by certain governments. At the same time, it is unnecessary to block the flow of content in order to achieve access protection goals. And it is vastly preferable, given the design of the Internet, to empower users with technical tools that enable them to



control their choice of content. This approach is the most consistent with the WSIS Declaration of Principles, which notes that the right to seek, receive and impart information and ideas through any media and regardless of frontiers is central to the Information Society.

- The paper highlights a specific filtering software tool developed by the Internet Content Rating Association (“ICRA”). ICRA’s primary contribution is not filtering software, but that it has developed a vocabulary for labeling content through an international process of expert input. Though ICRA has also developed filtering software based on this vocabulary, there is a variety of filtering software alternatives available as well. The objection that “there is no critical mass of sites labeling their content” applies both to the ICRA labeling vocabulary and to other systems; accordingly, the point should be made more generally, without reference to a specific organization.
- It is not entirely accurate to say that there are no multilateral agreements governing illegal content. With regard to IP, the World Intellectual Property Organization has concluded two important Internet treaties that update international copyright law so that it applies to digital works.
- Also, there is an optional protocol to the Council of Europe Cybercrime Convention (which is not specifically mentioned) on Acts of a racist or xenophobic nature committed through computer systems which is a multilateral agreement on harmful content, including hate-speech.
- There appears to be a floating sentence at the end of the paper, currently under the additional comment heading. Without context, its meaning is unclear.
- The paper correctly observes that in some sectors, self-help efforts have been undertaken in order to remove illegal content from the stream of commerce. But the paper inaccurately presumes that such efforts always prevent an objective evaluation of the legality of the content. Given that online piracy and Internet-related fraud are already prevalent and increasing at an alarming rate, such self-help actions are needed. Industry “notice and takedown” systems, for example, can play a role in alerting governments and/or ISPs to the presence of illegal content. Such efforts should be carried out in a manner that includes an effective evaluation of the legality of the content.
- The Opportunities section might note that there are incentives for such “best practices” to be developed. As markets converge, and the scope of global commerce increases, content providers and distributors are likely to seek ways to improve their ability to sell content in a variety of new markets. This might include self-regulatory efforts to develop effective content labeling and filtering tools. A wide variety of industries, including television, movies, and computer games, already self-regulate by providing ratings labels indicating the age-appropriateness of certain content.



Social Dimensions issue paper

- The important role that the private sector plays in bringing ICTs to the world so that they can be used as tools for economic and social development should be included more clearly in this paper. There is no mention of the importance of private sector investment and the enabling environment that attracts investment, and promotes entrepreneurship and innovation. These are key factors in fully utilizing ICTs and the Internet for economic growth and social development.
- The paper seems to imply that projects and money can solve the issue of access to ICTs. Without investment and the environment that draws it, money and projects alone cannot accomplish the objectives of integrating and fully using ICTs.
- Section 3 should highlight that the Internet and ICTs are important tools/enablers in helping the Information Society expand and promote the social dimension and inclusion.
- The third bullet of Section 3 should highlight that sustainable investment is required for development of basic ICT infrastructure and application, and other Information Society capabilities. An enabling environment is critical to promote such investment.
- Section 3 could mention that programmes have been established and have been successful in assisting special populations/groups or in achieving objectives with respect to participation by those populations/groups in general programmes.
- Business entities are among the organizations who are working to promote the social dimension and inclusion.
- Section 5 should note that partnerships between governments, business entities, civil society groups and international organizations can provide alternatives to broad-based forums in developing and implementing programs that address social dimension and inclusion. The partners can successfully work together on an on-going basis complementing each others capabilities and taking advantage of synergies toward this end drawing upon other resources as appropriate.
- Section 7 should be clear that a wide variety of user appliances and applications are needed recognizing that users have a wide variation in literacy and other skills and capabilities. Addressing the needs of the largest possible population of users by making information in all its possible modes and forms accessible including with the ability to create, process and apply it will promote inclusion.



Administration of Internet Names and IP Addresses issue paper

- We support the approach that the existing system should be improved rather than replaced.
- On page 12 in the list of negatives:
 1. It is unclear what the first bullet means. This needs to be clarified.
 2. Regarding outreach on the IANA functions, ICANN is making efforts to do more in this regard.
 3. It is important to note that the MOU is temporary and that NTIA is working with ICANN to terminate its oversight pursuant to the MOU.
 4. Governments can participate in the technical bodies and therefore can voice their views regarding public policy concerns.
- On page 13 under threats:
 1. It is unclear that it is necessary or appropriate to discuss spam here since it is a problem that cuts across so many forums and stakeholders – the toolkit approach.
- Suggested additions:

The new version of the Internet Protocol, IPv6, will enable new capabilities beyond IPv4, including providing greatly increased availability of IP addresses.

The benefits of IPv6 include:

- The number of IP addresses available with IPv6 is enormous - 3.4×10^{38} (i.e. 10 to the power of 38) – and will not be exhausted in the foreseeable future.
- IPv6 improves the efficiency of the Internet. Simplified packet header information allows for more straightforward and efficient routing of Internet packets. Shorter routing tables are possible because most Internet service providers can receive address space in adjacent blocks, offering greater convenience to their clients and also allowing for a more efficient structure in the Internet's core routing tables.
- IPv6 creates opportunities for new types of services that prioritize Internet traffic flows. It is 'auto-configurable', meaning devices like laptops, PDAs and mobile phones can be given their own unique IP addresses easily and without delay. This will simplify the installation and maintenance of home, vehicle and small office networks.
- IPv6 improves security by facilitating network-level security. It has security services at the IP-layer as a 'native' feature (i.e. IPSec includes the following capabilities: data origin authentication, rejection of replayed packets, and encryption). Also, allowing each communications device to have its own unique IP number facilitates 'end-to-end security', meaning that an entire communication session can be conducted securely rather than just the parts that use a virtual private network.
- IPv6 provides the basis for continued technical innovation in communications technologies.



Challenges in IPv6 deployment

As with the upgrade of any network, computer or related technology, deploying IPv6 generates costs, interoperability and resource issues for Internet stakeholders.

- Network routing and related Internet architecture equipment will need to be upgraded or modified to accommodate IPv6 128 bit addressing (as compared to 32 bit for IPv4).
- Although the number of IPv6-enabled Internet applications is constantly increasing, not all applications are presently engineered to work in an IPv6 environment.
- Having both protocols coexist in Internet architecture as IPv6 continues to be deployed generates integration and interoperability costs and challenges.

These issues may require Internet stakeholders to prioritize and concentrate their continued IPv6 implementation where it is most needed and will have the greatest benefit.

Network and Information Security issue paper

- The 'Introduction': needs to be either reworked or discarded. While the first two sentences are clear and the statements defensible, the remainder of the section is not. It uses terms, analogies and references that are questionable or wholly inappropriate. For instance, what is a "merit good" as used in the second paragraph? Further, use of "education and health-care" as an analogy to how security creates "externalities to the Society as a whole bringing benefits" is wrong; it defeats what basic message there is regarding individual action/greater good. In paragraph three, what "type of goods" is the author(s) referring to? And importantly, it can only be assumed that by "the new regulatory framework", the author(s) is referring to the European Union. But whatever their merits, this framework and "liberalization" in the telecom sector generally do not belong in the "introduction" to a paper on network security.
- Issue section: there is a paragraph beginning "Availability and security". These terms need definition and scope in order for the paragraph to have substantive meaning – "availability of what/whom" and "physical/logical security" must be understood in order for the misplaced "3 minute" statistic to have any relevance. Given the next paragraph, remove this paragraph as redundant. Although the 1-10 "challenges" that follow are essentially good, they generally are not well introduced by the opening paragraphs.
- Forums section: beginning at page 5, there are numerous problems stemming from both the headings used and the nature of the list/functional descriptions of organizations. A suggestion would be to simply list the organizations without titling

their input (e.g., “governance”, “domain name”) or describing their function – for two reasons: a) the paper should be brief, and b) it would alleviate the politics of offending an organization by an incomplete summary. For instance, the Section presently lists key “Governance Actors” as the UN (ITU and WIPO) and other solely European entities. Although each of these entities play a key role in IG issues, only the ITU-T/SG2 and OECD have made significant/effective contributions to the globalization of Network Security. Further, the description of ICANN is both wholly inadequate and misplaced under the sole heading “domain name bodies”.

- The paper does not so much provide an overview of the topic as a perspective on one way the future of the field might develop based upon certain unstated assumptions. It is difficult to suggest spot-fixes as a result. For example, the paper promotes a regulatory non-competitive model (*e.g.* telecoms regulation) as desirable because it would promote increased resiliency, perhaps because of the European focus of the text. But the paper does not provide evidence that regulatory models promote resiliency and ignores evidence that unregulated Internet may be more stable than the regulated telecoms system (*e.g.* the aftermath of the 9/11 terrorist attacks in New York). The paper will have to explore the facts; generalizations may be impossible.
- The last sentence of the software section (page 2) referencing the “monoculture argument” should be removed both because it is polemic and because it is unsupported by evidence both in the paper and in the real world.
- The paper lists “closed versus open standards” as an issue requiring balance (page 4). It is always necessary to be cautious when discussing standards: the fact that a standard is open does not *ipso facto* make it better than a closed one, or vice versa. It is difficult to know what the paper intends by this inclusion, because the paper does not provide a position as to whether closed standards are too prevalent or not prevalent enough.
- The section on “governance actors” (page 5) seems to focus on government and international NGOs and does not consider the work of industry groups like USISPA and EuroISPA to promote more secure practices.
- The paragraph on authentication and interoperability is confusing and needs to be reworked. Even if it makes sense to treat authentication and privacy on an international basis (and the paper leads no actual evidence in this regard), for practical reasons it is unlikely that solutions like a one-world regime for PKI will ever be adopted. It would be better to replace the infrastructures portion of this section as follows: “A diversity of authentication mechanisms, used for different purposes, is likely. Proposed solutions, whether based on infrastructure or distributed mechanisms, will need to address issues of cost and benefit, interoperability, scalability, and maintenance.”
- Finally, the final sections on “governance mechanisms”, “adequacy measured” and “other comments” miss what should be the focus of the closing analysis. The current focus is exclusively on standard setting, particularly the IETF. These



sections should not focus solely on the work of the IETF and its related organizations. Instead, it should seek to discuss how current standard-setting is both national and regional, whereas network security threat and response coordination must continue to be local (at the operational) level while further developing regional and international coordination.

International Internet Connections issue paper

- Background section: While the body of the paper outlines various arguments as to the difference between the circuit-switched and packet switched models, the complexity of the issue, lack of market power etc., are not covered in the background section. The result is that the background section is unbalanced.
- Strengths section (first bullet): The landscape of Internet backbone operators is a bit more complex than this bullet indicates. Tier 1 providers only peer (i.e., pay no transit). Other operators may peer regionally (or even locally) but then do pay transit for some of their traffic.
- Weaknesses section (fourth bullet): The bullet should be revised for clarity. While it begins with saying the non-regulated layer, it goes on to discuss the settlements process, which is the circuit-switched regulated layer. While it is true that the settlement charges were not cost based, this relates to the regulated circuit-switched telephony model.

Voice over Internet Protocol (VoIP) issue paper

- The paper is insufficiently precise in using the term “VoIP.” We suggest that it is important to an understanding of the issues to distinguish between IP-enabled transport and applications that use such transport, for example. It is also important to distinguish between applications that have the capability of substituting for traditional phone service, and those that do not, e.g., adding a voice capability to a multiplayer online gaming experience.
- Issue section: add a comment in this section that many, including telecommunications regulators, have agreed that we cannot simply transpose traditional telephony regulation to the VoIP space, and that governments should apply a light touch approach to regulation in this area.
- SWOT analysis section: it is worth noting that there is an opportunity to address the appropriate regulatory treatment of VoIP carefully and over time. Relative to traditional telephone networks, the level of international voice traffic carried over the Internet remains modest.
- It is important that the concept of “technological neutrality” not be misused. Where competitive conditions differ, regulation should differ. Where network technologies differ in many respects, as do IP-enabled and analog networks,



regulation should account for those differences. Neutrality does not mean treating different things exactly alike, particularly if such treatment creates disparate harms for one and not the other.

- Other Issue Section (2nd bullet): The PSTN is also susceptible to cyber attacks (although perhaps not denial of service attacks).

Competition Policy, liberalization, privatization and regulations issue paper

- Introduction (3rd para): This paragraph reads as if the ITU and the WTO both negotiate policy for telecoms. This should be modified.
- SWOT Weaknesses section: The second sentence is unclear. If members are not required to be signatories then why is it inconsistent that they remain sovereign when implementing them?
- Content of principles, norms and rules: The first sentence should be clarified to indicate that the Reference Paper only applies to basic telecom. Similarly, the second paragraph on licensing is applicable to basic telecom but not necessarily Internet services.

Telecommunications Infrastructure, Broadband Access and Convergence with NGN issue paper

- In the issue section, it is important to note that while the *incremental* cost of carrying voice on the Internet or over “Next Generation Networks” (NGN) is close to zero, the total cost (and the average cost) is not. Indeed, high-speed internet access networks involve significant up-front costs. And, as the paper notes later on, a poor regulatory environment can stifle investment in these networks.
- The development of NGNs does create a variety of issues for the ITU accounting rate system. But it is important to note that issues have arisen before, for example, due to the rise of mobile telephony. Incumbent telephone providers have, in the past, expressed concern about the impact on revenue and infrastructure deployment from the creation of competitive markets for long distance, or the deregulation of handsets and equipment markets. It is important to examine the facts before expressing alarm.
- The paper presumes that regulation of IT networks is a good way to promote their development and focuses on what kind of regulation, thereby skipping the logically anterior step of whether regulation is required or desirable at all. See for example the discussion of “Transforming policy and regulation” (page 2), which focuses on how to transform current regulatory regimes to a world of converged networks but does not ask whether these regimes are a good idea in the first place.

- The paper presumes that the “public good” obligations placed on telecoms companies are appropriate. Perhaps in a time when telecoms companies were national monopolies, insisting upon such obligations was an acceptable way to offset the monopoly. The paper then seems to conclude that NGNs and other non-traditional telecoms companies are receiving an unfair advantage by not being subjected to these same obligations, rather than questioning whether the obligations are appropriate in a non-monopoly context. It also does not consider that in some countries NGNs have accepted “public good” obligations such as 911 service, and that it may not be appropriate to require NGNs to contribute to infrastructure such as wire lines that they do not require for their services.
- The paper’s definition of “telecommunications infrastructure” excludes various items that are necessary for an IP-based network such as DNS and servers. This is significant because even today virtually all “traditional network proficers” are using IP-based background and many are offering advanced IP services such as VoIP or DLS.
- The paper’s discussion of trade associations does not note how incumbent providers and their sunken investments in technologies may impact upon the ability of NGNs to develop new technologies, nor does it focus on the well-known theory that regulated industries often tend to “capture” their regulators.
- The following sentence should be removed because it is inflammatory and reflects one opinion or view point and is arguably not true (page 7): “The power of OECD influence, US supremacy and private sector preferences is likely to combine and ensure that decisions are not reached or are made consistent with their preferences.” Besides being inflammatory, it is arguably not true.
- The document may unintentionally create confusion in saying, so starkly, that “Internet governance institutions... fall short of the high standards set by WSIS.” (page 8). It might be helpful to clarify this by adding that it is possible that the needed reforms could be achieved without creating new [multilateral] organizations.
- There is no real or lasting distinction between a traditional network provider and a NGN provider; they increasingly all use IP backbones and want to offer IP services. In many cases, the greatest threat to the revenues of traditional network providers are those traditional providers who have upgraded their networks to embrace an IP world.
- There is also an assumption that it must be the traditional network providers and not NGNs that develop and extend national infrastructure. Given the success of competitive wireless operators bypassing legacy networks to provide useful and affordable services to underserved areas, this assumption is tenuous at best.
- The paper presumes that regulation of IT networks is a good way to promote their development and focuses on what kind of regulation, thereby skipping the logically anterior step of whether regulation is required or desirable at all. See for example



the discussion of “Transforming policy and regulation” (page 2), which focuses on how to transform current regulatory regimes to a world of converged networks but does not ask whether these regimes are a good idea in the first place.

SPAM issue paper

- Overall, the tone calling for a multi-faceted approach that includes legislation, enforcement, technology, public/private sector collaboration, and consumer awareness is appropriate.
- It would be helpful if the paper emphasized a bit more strongly the importance of an effective legislative infrastructure with resources for enforcement (perhaps with reference to recent enforcement activities and the likely impact of sustained enforcement over time). The private sector can provide exceptional support to government enforcement initiatives and should not be overlooked as the global government approach is assembled.
- Ideally, the piece on legislation would be a bit more developed with recommendations on core elements. And while it is appreciated that legislative approaches have varied widely and some issues are particularly controversial (e.g., opt in v. opt out), it would be helpful to at least call out the need for meaningful, deterrent penalties (whether criminal liability in some cases or significant monetary penalties). It would also be helpful to have a reference to the value of giving standing to private sector actors to take enforcement action under spam laws (this would be a tough sell given that a number of legal systems do not allow for this).
- Suggest adding reference to APEC as another multilateral group that is active in this area.
- Finally, the last paragraph in the SWOT analysis states that “in the absence of effective governance, it is possible that a number of different, privately controlled proprietary anti-spam solution will emerge, thereby threatening the integrity of the Internet...” To speak of blocking and filtering technologies as a “threat to the Internet,” particularly in the spam context, misses the mark. Technological solutions are blocking more spam than any government regulation or enforcement action. And to de-emphasize or pejoritize their effectiveness is inappropriate. This paragraph should be deleted.



About ICC

ICC is the world business organization, the only representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world. ICC promotes an open international trade and investment system and the market economy. Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment, e-business, IT and telecoms policy as well as on vital technical and sectoral subjects. ICC was founded in 1919 and today it groups thousands of member companies and associations from over 130 countries.

* * * * *