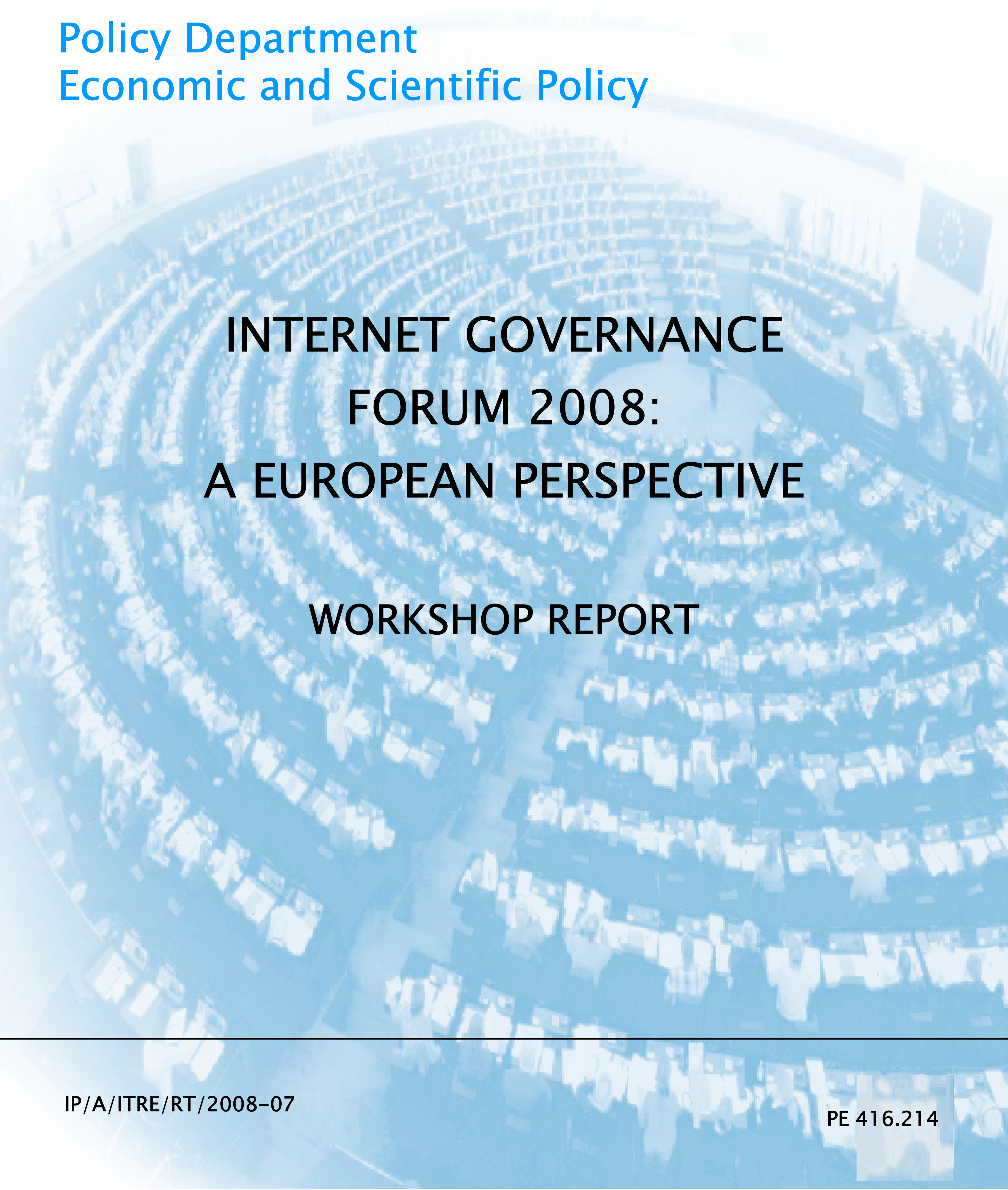
EUROPEAN PARLIAMENT

REPORT

Policy Department
Economic and Scientific Policy



INTERNET GOVERNANCE FORUM 2008: A EUROPEAN PERSPECTIVE

WORKSHOP REPORT

IP/A/ITRE/RT/2008-07

PE 416.214

These Briefing Papers were requested by the European Parliament's Committee on Industry, Research and Energy (ITRE)

Only published in English.

Responsible Administrators:

Maya Gadzheva
Policy Department Economy and Science
DG Internal Policies
European Parliament
Rue Wiertz 60 - ATR 00L0xx
B-1047 Brussels
Tel: +32-2-2832858
Fax: +32-2-2846929
E-mail: maya.gadzheva@europarl.europa.eu

Karin Hyldelund
Policy Department A - Economy and Science
Internal Policies Directorate-General
European Parliament
Rue Wiertz 60 - ATR 00 L012
B-1047 Brussels
Tel: +32-2-2832234
Fax: +32-2-2849002
E-mail: karin.hyldelund@europarl.europa.eu

Manuscript completed in January 2009.

The opinions expressed in this document do not necessarily represent the official position of the European Parliament.

E-mail: poldep-esc@europarl.europa.eu.

TABLE OF CONTENTS

ITRE WORKSHOP PROGRAMME

Internet Governance Forum 2008: A European Perspective

Date: 20 November 2008, 09.00 – 12.00

Venue: European Parliament - Strasbourg - Room **Louise Weiss N1.3**

BACKGROUND AND OBJECTIVES

With over a billion users world-wide, the Internet is the most important infrastructure of the information age which influences society, business and technology on the global as well as on the local level. The Internet Governance Forum, one of the main outcomes of the UN World Summit on the Information Society (WSIS), is a multi-stakeholder forum for policy dialogue on issues of internet governance and will have its third meeting in Hyderabad/India in December 2008.

The workshop is intended to stimulate efficient and effective discussion among experts on key topics and to provide expert advice and recommendations to the EP *ad hoc* delegation in order to prepare its input and position vis-à-vis the third IGF meeting. The workshop will provide a forum for invited independent experts and participants to exchange views, analytical research and visions on the political, economic, social and legal issues of Internet governance. The crucial aim is to examine how global governance arrangements are being defined around specific Internet policy issues.

Faced with the convergence of telecommunication, broadcasting and information technologies the workshop looks toward analysing the Internet governance issues within the broader perspective of past development, present trends, and future prospects. All discussions and results from the workshop will be compiled into a report and communicated to all interested MEPs and participants at the workshop.

Workshop Programme

09:00 Welcoming address and opening remarks - MEP Catherine Trautmann, head of the EP *ad hoc* delegation to the third IGF meeting.

SESSION 1: INTERNET GOVERNANCE & DOMAIN NAMES: THE WAY FORWARD

The process of introduction of new generic Top Level Domains (TLDs) and Internationalized Domain Names (IDNs) will open up the Internet turning it into a truly global and multilingual tool, bringing new opportunities for Internet users and providers to develop new services as well as new challenges for existing registries, registrars and ISPs. After years of debate, ICANN reform has made significant progress, but that some key areas need to be further improved in order to complete the transition to an agreed model of multi-stakeholder coordination of the Internet's unique identifiers. This session aims to analyse important aspects of the current debate and to explore different alternatives for managing the DNS namespace.

09:10 Presentation by **Prof. Wolfgang Kleinwächter**

Professor for International Communication Policy and Regulation at the Department for Media and Information Sciences of the University of Aarhus, a former member of the UN Working Group on Internet Governance, a former member of the UN Working Group on Internet Governance (WGIG).

- How the Domain Name System is evolving? Who are the potential actors for the global governance - an extended ICANN, ITU, etc...?
- What are the legal, operational, business and political issues of the ongoing reform? What is the EU position on the three question areas identified in the transition action plan? What is the future of ICANN with the completion of the Joint Project Agreement (JPA)?
- How to achieve broad representation of global Internet communities? How to promote cultural and linguistic diversity on the internet? What are the benefits and new challenges resulting from the creation of new and multilingual top-level domains (TLDs)?
- How to ensure that the security, stability and interoperability of the DNS is maintained? How to minimize the risks of domain name testing, cybersquatting, and consumer confusion?

09:30 Questions and answers session

SESSION 2: TRANSITION FROM IPV4 TO IPV6: SUCCESS & CHALLENGES

IPv6 (Internet Protocol, version 6) is the next version of the Internet Protocol, capable of eliminating the risks and limitations associated with the current version of the IPv4 protocol and better addressing the emerging needs of the information society characterised by a proliferation of new networked devices. This session will explore the level of IPv6 take-up in Europe and the ways to achieve interoperability for the period of co-existence between IPv4 and IPv6 as well as to identify the remaining challenges, bottlenecks and security implications of IPv6 deployment. The crucial aim is to provide appropriate strategic recommendations suggesting the way forward and the actions to be initiated by the various stakeholders - regulators, standardisation bodies, ICT industries and end-users - to stimulate IPv6 connectivity.

09:45 Presentation by **Prof. Rolf Weber**

Director of the European Law Institute and of the Centre for Information and Communication Law, Faculty of Law, University of Zürich

- How long we will have enough IPv4 addresses? How to better allocate the remaining IPv4 address space and better re-use allocated address space?
- What are the drivers and challenges for transitioning to IPv6 through a dual IPv4/IPv6 environment? Is there a risk to split the Internet into two address spaces?
- What are the drivers and challenges of IPv6 deployment? What is the current status of IPv6 deployment? What lessons could be learned from successes and barriers that have been identified in IPv6 implementations to-date?
- How to accelerate the transition from IPv4 to IPv6? What is the role of different stakeholders in the transition to IPv6? Are Internet-poor countries ready in upgrading themselves to IPv6? Is there a need for an EU initiative on this technology?

10:05 Questions and answers session

SESSION 3: THE INTERNET OF THE FUTURE: ACHIEVING TRANSPARENCY, PLURALISM AND DEMOCRACY

User generated content, Web 2.0, RFID, Internet of things are no more buzzwords only, but have already started to challenge the way some of us currently lead our lives and expect to live them in the future. Recognising the Internet as a key infrastructure in addressing mainstream policy challenges (e.g. ageing, health, environment, globalisation…), this session will present different approaches and perspectives on the scope and implications of the future Internet governance debate. It will identify the priority issues which should be addressed in the near future as well as bring into focus emerging issues which could be of importance to the future agenda of the IGF.

10:20 Presentation by **Prof. Yves Poullet**

Director, Research Centre on IT and Law (CRID), University of Namur, Belgium

- How to address the vulnerability issues (security, privacy, etc.)? What is the relationship between security, privacy and openness? Are there new rights in cyberspace? Is there a need for an Internet Bill of Rights?
- What are the public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, stability and development of the Internet?
- How to ensure the interaction between the Future Internet and the Internet of Things towards a new “post-Internet” network? What concrete actions should the European Union take at international level?

10:40 Questions and answers session

SESSION 4: EUROPEAN INTERNET GOVERNANCE APPROACH: OVERVIEW BY THE EUROPEAN COMMISSION

This session provides an opportunity for interactive discussion on the EU policy and activities in relation to internet governance.

10:55 Presentation by **Michael Niebel**

Head of Unit, Internet; Network and Information Security, European Commission

- What are the key challenges of internet governance at European level?
- What is the role of EU regarding internet governance? What are the policy orientations and activities of the European Commission?
- What does European business expect from internet governance? Do we need more regulation for the Internet? What should a new policy framework look like?
- How can the EU increase its impact and build a stronger presence of Europe in the design of the Internet? How can Europe ensure that its impact on defining internet governance will be felt?

GENERAL DEBATE

11:15 Debate with all the panellists - Which of the many issues involved in Internet governance should be given priority in the near-term?

CONCLUSIONS: PRIORITY-SETTING AND WRAP-UP

11:50 Closing remarks – MEP Catherine Trautmann

The Workshop is organised by the Policy Department A and the ITRE Secretariat

BRIEFING PAPER PROF. WOLGANG KLEINWÄCHTER: INTERNET GOVERNANCE & DOMAIN NAMES

1. BACKGROUND

The Internet "Domain Name System" (DNS), which is also called the "Territory of Cyberspace", was invented in the early 1980s and described in various so called "Request of Comments" (RFC)[1] by Paul Mockapetris und Jon Postel. They created a layered system with two main categories at the top: generic Top Level Domains (gTLDs like .com, .gov or .net) and country code Top Level Domains (ccTLDs like .de, .uk or .nl). The basic idea behind the DNS was to give IP numbers, which interconnect the computers, a "human face" by translating the "number" of the computer into a "name" of the person or institution behind the computer. The DNS system was hierarchically designed but decentrally organized. The TLD zone files were kept in one database, in the authoritative root, while the Secondary Level Domains (SLDs) were managed by the assigned manager of a TLD registry.

The database of the DNS was managed by just one man, Jon Postel himself, who worked at the Information Science Institute (ISI) at the University of Southern California (USC) in Marina del Rey, and his assistant. Postel assigned IP number blocks to Regional Internet Registries (RIRs) and delegated the management of ccTLD registries according to the ISO 3166 list by "handshake" to people he trusted. No government and no parliament was involved in the ccTLD delegation process in the 1980 and 1990s.

In 1988, the US government, which funded the Internet research first via its "Defence Advanced Research Project Agency" (DARPA) and later via the "National Science Foundation" (NSF), proposed Jon Postel to institutionalize the management of the database. The new "Internet Assigned Numbers Authority" (IANA), Postels one-man-organisation, became an institutional part of the ISI and entered into a ten year contract with the National Telecommunication and Information Administration (NTIA) of the US Department of Commerce (DOC). The contract terminated in 1998.

The terminology "Internet Governance" emerged only in the 1990s and was used first by the Harvard Information Infrastructure Project (HIIP) at the "JFK School of Government" at Harvard University. The project analyzed primarily the implications of the "National Information Infrastructure Initiative" (NII) of the Clinton Administration which was inspired by the concept of private sector leadership. The term "Internet Governance" described a new model of key resource management by private sector led self regulation. The general understanding was that governmental intervention into the management of Internet resources should be avoided. The concept was "Governance without Government".

After the invention of the World Wide Web in the early 1990s, Jon Postel realized that the DNS and its management need further development and institutional stability. Various efforts to "enhance and internationalize" IANA since 1992 via the Internet Society (ISOC) and a so-called "Interim Ad Hoc Committee" (IAHC), where the IANA, ISOC, the Internet Architecture Board (IAB/home of the IETF), ITU, WIPO and the International Trademark Association (INTA) were involved, did not produce broadly accepted results.

[1] A RFC is a Internet Standard which is adopted after a bottom up open and transparent consultation process. The methodology was introduced in the early 1970s. Today, there are more than 4000 RFC standards which are now managed by the Internet Engineering Task Force (IETF).

In June 1997 - against the background of the expiration of the contract between ISI and DOC - the US government launched a process towards the privatization and internationalization of the DNS.

The first “Green Paper” (January 1998) was widely discussed and also criticized by the European Commission as too US centric. Based on the comments, the “White Paper” from June 1998 paved the way for the establishment of the “Internet Corporation for Assigned Names and Numbers” (ICANN) in October 1998.

ICANN was incorporated as a private non-for-profit corporation under Californian law and entered into a Memorandum of Understanding” (MoU) with the US Department of Commerce. ICANN got the backing from various governments, including the EU, Canada and Australia. However, countries like China, Russia, Brazil or India were not involved in the making of ICANN. All governments were invited to join ICANNs “Governmental Advisory Committee” (GAC) which was also open, by invitation, to intergovernmental organizations and so-called recognized territories as Taiwan. The MoU between ICANN and the US government was laid out for two years. When it expired in October 2000, it was several times enlarged and finally substituted in 2006 by a “Joint Project Agreement” (JPA) which expires in October 2009.

During the UN World Summit on the Information Society (WSIS) [2], the government of the Peoples Republic of China – supported by a large number of developing countries - argued that private sector leadership for the Internet was good for one million Internet users but with more than one billion Internet users the time had come for governmental leadership in Internet Governance. China proposed either to establish a new intergovernmental UN Internet organization or to transfer ICANNs responsibilities to the existing intergovernmental ITU, an agency of the UN system.

To bridge the controversy 'private sector leadership vs. governmental leadership' or 'ICANN vs. ITU', the Geneva Summit decided in 2003 to ask UN Secretary General Kofi Annan to establish a 'Working Group on Internet Governance' (WGIG) with the mandate, inter alia, to define 'Internet Governance', to identify the public policy components of Internet Governance and to clear the role of the various stakeholders. WGIG proposed a broad definition and the concept of 'Multistakeholderism' instead of 'single stakeholder leadership'. The Internet should not be governed by a single unit or a single stakeholder. There should be no singular Internet Governance Model.

The management of the internet was described as a 'Multilayer Multiplayer Mechanism' (M3) where the various stakeholders and governmental and non-governmental organizations are involved according to their specific roles and carry special responsibilities for their specific terrain. Government, private sector, civil society, the technical and the academic community should work together and enhance their communication, coordination and cooperation (C3).

In November 2005 the 2nd World Summit on the Information Society (WSIS) in Tunis accepted the WGIG proposal in principle by:

- Agreeing on a framework of basic Internet Governance principles (openess, transparency, multilingualism, multistakeholderism, equal rights, sovereingty etc.) for Internet Governance;
- Creating the Internet Governance Forum (IGF) as a space for discussion of cross cutting issues;

[2] WSIS 2005 in Tunis, see http://newsbreaks.infotoday.com/nbreader.asp?ArticleID=16066.

- Launching a process of “enhanced cooperation” among stakeholders and governments to promote the security, stability, robustness and interoperability of the Internet.

The new established Internet Governance Forum” (IGF) was not a new UN Intergovernmental Internet Organisation but a multistakeholder discussion platform without decision making capacity. The idea of the IGF is to bring the various stakeholders on a high level and on equal footing together, to discuss cross cutting key issues and to enable them to understand better the general environment of their own activities. The “messages” of the IGF are embedded in their proceedings and in the chairs conclusions. The fact that there is no need to negotiate an agreed text at the end of the IGF has liberated the discussion and promoted an open, frank and critical atmosphere for the interaction among the various stakeholders.

The IGF started 2006 in Athens, continued 2007 in Rio de Janeiro and is followed now by the 3rd meeting in Hyderabad in December 2008. In Rio there were nearly 2000 participants from all stakeholders. Meanwhile the IGF is seen by many as 'the Davos of the Internet'. Further IGFs are planned for 2009 (Egypt) and 2010 (Vilnjus or Baku). In 2010 the UN Secretary General, who is the convener of the IGF, has to decide, based on consultations with all stakeholders, how to continue.

In the meantime, ICANNs JPA terminates in October 2009 and ICANN is preparing for a transition period in a post JPA future. The ITU is going to organize a 'World Telecommunication Policy Forum' (WTPF) in April 2009 in Lisbon to discuss Internet issues, including also the management of critical internet resources and is planning for its next Plenipotentiary Conference in Mexico City in 2010.

During the recent ICANN meeting in Cairo (October 2008) ITU Secretary General Hamadoun Toure had his first official meeting with the ICANN community, its Board of Directors and the Governmental Advisory Committee (GAC). He offered an improved cooperation among ICANN and ITU but was rather sceptical with regard to the efficiency of the multistakeholder model.

2. QUESTIONS PUT FORWARD BY THE EUROPEAN PARLIAMENT

2.1 How the Domain Name System is evolving?

DNS has proofed its efficiency. It was able to accommodate an incredible quantative growth from several thousands to nearly 200 million registered domain names without bigger problems. In the largest registries - .com with more than 70 million, .cn and .de with 12 million – it is meanwhile difficult to register a name because nearly all words are already taken. There is no technical barrier for broadening the domain name space, that is to introduce new TLDs and to “create new land in cyberspace”.

We are now at the eve of a qualitative growth with new generic and multilingual TLDs. On the one hand ICANN has opened the door for the introduction of hundreds of new gTLDs. On the other hand we will see soon the introduction of internationalized Domain Names (iDNs) where all parts of a web- or e-mail address can use non ASCII scripts with Chinese, Cyrillic or Arabic characters.

2.2 Potential actors for the global governance: an extended ICANN, ITU or something else?

ICANN has a limited technical mandate but the technical issues, managed by ICANN, have unavoidable public policy implications. ICANN reflects this challenge by its multistakeholder model which is meanwhile widely accepted as a workable and efficient form to handle the complexity of the management of the critical Internet resources (CIR). The open and transparent bottom up policy development process (PDP) allows the involvement of all stakeholders from the very beginning of the discussion of a new issue.

The ICANN process offers a space for collaboration of relevant organisations like the Regional Internet Registries (RIRs) and its Number Resource Organisation (NRO), the Internet Engineering Task Force (IETF), the various regional organisations of ccTLD Registries, ISPs, Internet users and others. The GAC allows also a broad interaction among the non-governmental and governmental stakeholders on ICANN related public policy issues.

However, there are still various gaps to use the full potential of multistakholderism in the ICANN process.

On the agenda for a future ICANN development are, inter alia

- a reconsideration of the relationship between the ICANN Board and the GAC;
- a greater role for the At Large community (Internet Users) in the ICANN processes¨;
- a more decentralized management of various components of names and numbers.

ITUs constitutional mandate is to manage the frequency spectrum, to coordinate telecommunication standardization and to promote telecommunication infrastructure development, in particular in developing countries. The ITU is an intergovernmental organisation of the UN system which is not based on the principle of multistakeholderism.

However the ITU Plenipotentiary Conference in Kyodo in 1992 introduced a special status for private sector companies allowing them to become non-voting members under the ITU constitution. WSIS gave ITU also a special mandate to promote infrastructure development (WSIS C3) and cyber security (WSIS C5).

While the Internet management is not under the mandate of the ITU, in some areas ITU activities overlap with the ICANN mandate (ENUM, IP and ccTLD/iDN management). Since 1998 (Minneapolis) the ITU Plenipotentiary Conferences have adopted resolutions on Internet management (Marrakesh 2002, Antalaya 2006).

On the agenda for an extended ITU could be, inter alia:

- an enhanced communication, coordination and collaboration with ICANN and the IGF to avoid duplication and waste of resources;
- a reconsideration of the relationship between voting governments and non-voting sector members within the ITU;
- the inclusion of Civil Society as an ITU unit member;
- to strengthen open, transparent and bottom up elements in ITUs policy development processes.

In this context, the Internet Governance Forum (IGF) could become something like a "clearinghouse" or a "watchdog" for Internet Governance, where issues of common interest are discussed among the various involved stakeholders. The relevant governmental and non-governmental organisations (ITU, UN, UNESCO, COE, EU, ICANN, IETF, W3C, NRO etc.), which have according to their legal mandate a decision making capacity for individual Internet related issues, are encouraged to enhance their bi- and multilateral communication and collaboration to improve their own decision making processes by taking into account interest, values and comments from other constituencies outside their own membership. Such a complex mechanism could serve best the interest of the whole global internet community.

2.3 What are the legal, operational, business and political issues of the ongoing ICANN reform?

ICANNs legal status, in particular its incorporation under Californian law, is an ongoing subject for discussion. There are various plans, discussed in ICANNs Presidential Strategy Committee (PSC), to consider the launch of a second legal unit in the form of an "ICANN International Inc." which would be incorporated, eventually, under Swiss law in Geneva. Another option is to give ICANN the legal status of an independent international organisation with semi-diplomatic immunities based on a contract with the host country.

Changes in the legal status of ICANN have to be drafted carefully and have to take into consideration the hundreds of private contracts ICANN has with various private partners (TLD registries, Registrars UDRP Service Providers) which could be affected if ICANN changes its legal status.

The main political issue in ICANNs ongoing reform is the forthcoming termination of the Joint Project Agreement (JPA) with the US government in October 2009. The US Department of Commerce had launched a mid-term review of the JPA in 2007 and ICANN itself has launched a plan for transition into a post JPA future.

The majority of the milestones, defined in the JPA, are implemented. Broad parts of the community expect a termination of the contract.However, other parts of the community, mainly the US private sector, is also supportive for a continuation of a special contractual arrangement between ICANN and the US government to avoid one sided capture by ICANN staff, individual interests, commercial groups or other governments. It is too early to speculate how the new Obama Administration will position itself with regard to Internet Governance. In this context the future role of the GAC should be reconsidered.

2.4 What is the EU position on the question identified in ICANNs transition action plan?

In ICANNs transition plan five key issues are identified for further discussion. For the EU each of the five issues is important. Priority could have the following points:

1. To address freedom from capture
   - Avoid commercial capture by market dominance (competition and anti-trust law);
   - Avoid governmental capture by some government;
   - Avoid Staff Capture.

2. To strengthen ICANN's accountability to its community
   - Bring more transparency in the "last mile" of the PDP;
   - Strengthen the ongoing review process;
   - Strengthen the role of the Ombudsman.
3. To internationalize ICANN
   - Exploring the option of an "ICANN International";
   - Broadening regional presence of ICANN;
   - Finding ways to bridge conflicting jurisdictions (Whois, competition law).
4. To Ensure Financial and Operational Security
   - Broadening of income sources but keeping the non-commercial public benefit nature;
   - Bring full transparency into the financial mechanisms of the new gTLD process;
   - Exploring the feasibility of a DNS Solidarity Fund, financed by the new gTLD process.
5. To Maintain Secure and Stable operations
   - Avoid political experimentation with oversight;
   - Implementing DNSSec[3];
   - Developing the contingency plan.

2.5 What is the future of ICANN with the completion of the Joint Project Agreement?

The Joint Project Agreement (JPA) does not constitute a hard regulatory framework for oversight. It is an agreement about a "joint project". It is aimed to improve ICANNs performance through enhanced cooperation. The JPA is mainly about "reporting" and "consultation". ICANNs day to day operations are not subject of the JPA. ICANNs decisions on new gTLD or iDNs do not need formal approval by the DOC however comments by the US government are well taken by the ICANN Board as the cases of .net re-delegation or the rejection of the .xxx application have indicated.

To a high degree the JPA is symbolic. An ICANN without a JPA would not fundamentally change the landscape but ICANN would get broader recognition and legitimacy by the global Internet community. The JPA is still seen by many constituencies as an instrument of the US government to control ICANN.

[3] The Domain Name System Security Extensions (DNSSEC) are a suite of IETF specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers): Origin authentication of DNS data; Data integrity (but not availability or confidentiality) and Authenticated denial of existence. It is widely believed that securing the DNS is critically important for securing the Internet as a whole, but deployment of DNSSEC specifically has been hampered by the difficulty of; 1) Devising a backward-compatible standard that can scale to the size of the Internet; 2) Preventing "zone enumeration" where desired, 3) Deploying DNSSEC implementations across a wide variety of DNS servers and resolvers (clients); 4) Disagreement among key players over who should own the .com (etc) root keys; and 5) Overcoming the perceived complexity of DNSSEC and DNSSEC deployment.

On the other hand, the call for ICANNs "independence" is a double edged sword. If the JPA terminates, a stable and secure system for accountability needs to be installed. ICANN has to be accountable to the global Internet community and to all relevant stakeholders, including the governments. One option could be to have a JPA similar arrangement between the ICANN Board and the GAC, probably in the form of enhanced procedures for interaction through an amendment to ICANNs bylaws.

Furthermore there is a general need to strengthen transparency and openness in all bottom-up policy development processes (PDP). This needs a more intensive interaction among all stakeholders already in an early stage of the start of a PDP. Improved and transparent procedures for interaction among stakeholders – in particular between the ICANN Board and the GAC but also between the ICANN Board and the other Supporting Organisations (SOs) and Advisory Committees (ACs), including the ALAC[4] – are needed if ICANN wants to become accountable and enhance the efficiency and improve stability of its processes.

It is also important to note, that the IANA contract, which gives the US government the role to authorize the publication of TLD Zone Files in the Hidden Root Server, is not part of the JPA and does not terminate in October 2009.

2.6 How to achieve broad representation of global Internet communities?

For ICANNs future it is important to strengthen in particular the "weak" constituencies like the At Large Membership, the Non Commercial GNSO constituency and the various stakeholder groups from developing countries. ICANN will get full acceptance as a global multistakeholder organisation only, if all stakeholders are indeed included as equal partners and on equal footing in their specific roles in the process. This includes active participation both in the online discussion as well as in the offline F2F meetings. An important element could be the further development of the Fellowship Programme[5] which could be financed, inter alia, by income from the new gTLD programme.

It is also important to create more political awareness among governments both in developed and developing countries. Internet Governance deals with the most critical infrastructure of the global information society. However, in many societies and for many governments both in developed and developing countries the issue is still low on the priority list.

Broader representation of the global internet community can be reached also by speeding up the fast track for the introduction of iDNs, in particular on the country code level. Another step is the strengthening of regional bodies of ICANN constituencies like regional organisations for TLDs, IP Addresses, ISP and Internet Users. In this context, regional ICANN offices could be very useful.

[4] ALAC stands for At Large Advisory Committee. The Committee is the space for the individual Internet users and civil society within the ICANN community. ALAC has 15 members. 10 are elected by five regional At Large Organisations (RALOS), five members are nominated by ICANNs Nomination Committee (NomCom). A RALO has so called At Large Structures (ALS) as members. ALSs needs the recognition of the ALAC. The European Regional At Large Organisation (EURALO) is still a weak body with not more than 25 members, representing various NGOs and civil society organisations from about 10 European countries.

[5] An ICANN fellowship is a one-time grant of support which is awarded to enable individuals from stakeholder groups around the world to attend ICANN meetings, see http://www.icann.org/en/fellowships/.

2.7 How to promote cultural & linguistic diversity on the internet?

First priority at this stage has ICANNs ccTLD IDN Fast Track. To enable millions of Internet users to use their own language and local characters when writing web- or e-mail addresses will remove a great barrier and bring much more opportunities to the next billion Internet users.

Internet content is not ICANNs mandate, but the experiences with the .cat TLD – where the availability of a TLD for the cultural and language community of the Catalans has triggered the production of an enormous amount of new websites in Catalan – shows the interdependence between new opportunities in the DNS and the growth of cultural and linguistic diversity.

Another challenge for ICANN is to broaden its language base. While English, in the author's opinion, should continue to be the "lingua franca" of the global Internet community and remain the main working language for subgroups and taskforces, ICANN plenary assemblies, public fora and other key meetings should be translated and all policy and corporate documents should be available in the major languages.

ICANN could also make more use of its three annual meetings to do outreach into the local Internet community by organizing special events for the local academic, technical, business and user community as integral part of its meetings which take place on a rotation basis in the five ICANN regions.

2.8 New generic & multilingual Top Level Domains (TLDs): Benefits & Challenges?

The introduction of new gTLD is the subject of discussion since the early 1990s when the invention of the World Wide Web opened the door for a new wave of Internet innovation. Already in 1994 Jon Postel wanted to introduce 150 new gTLDs under the umbrella of ISOC. In 1997 the IAHC proposed the introduction of seven new TLDs. Both efforts failed.

The broadening of the DNS was one of the main driving ideas behind the establishment of ICANN in 1998. ICANNs first application round for new TLDs – in the year 2000 - produced nearly one hundred proposals. Only seven were accepted. In a second round – between 2003 and 2007 - another seven new TLDs ware recognized.

There is no technical barrier for the broadening of the domain name space via the introduction of new gTLDs. However, there is a need to have a sound process and guarantees for financial, organizational and technical capabilities from applicants to avoid that the introduction of new gTLDs could affect in a negative way the stability and security of the Internet.

The main benefits of new TLDs are:

- Removing of language/script barriers
- More choice for consumer;
- New business opportunities;
- Opportunity for a more systematic ordering of new domain name spaces.

The main challenges linked to new TLDs are:

- Avoiding confusion;
- Guaranteeing Consumer Protection;
- Finding procedures to settle conflicts around disputed TLD strings;
- Enhancing security (eliminating Phishing opportunities).

The recently proposed procedure for the new gTLD application process got broad support by global Internet community but has raised also some additional questions.

One concern emerged from the proposed fee structure (about $180.000.00 application fee and $70.000.00 annual fee): The question is whether public entities, representing local or regional authorities and applying for so-called GEO-TLDS (for cities and regions) should be treated in the same way like purely commercial TLDs (.web, .shop or .xyz) or so-called corporation TLDs (like .nokia, .siemens or .sheraton).

The GAC expressed some concerns with regard the use of city and region names or other geographical or cultural names in TLDs. Another concern was expressed by the US government which invited ICANN first to study more in depth the DNS market development implication, in particular for broader and more efficient competition, before launching a great number of new TLDs.

A disputed issue is also the proposed procedure for dealing with conflicts if the proposed TLD string as a special meaning with regard to moral and public order and is challenged by a third party.

2.9 How to ensure that the security, stability and interoperability of the DNS is maintained?

The main elements to ensure the security, stability and interoperability of the DNS are, inter alia:

- Avoid risky experimentation with oversight (if it is not broken, don't fix it);
- Enhance security at the Root & Name Server Level (DNSSec);
- Reduce incentives for alternative (language) roots (Fast Track ccTLD iDNs);
- Raise awareness among all stakeholders (a main security risk is the naive and uninformed end-user).

2.10 How to minimize risks of domain name testing, cyber-squatting, & consumer confusion?

Key elements to minimize risks from misuse of the DNS by cyber-squatters, domain-name testers and other are:

- Improve Awareness among all stakeholders;
- Invest into consumer / end user training and education;
- Identify gaps in the PDPs (domain name tasting as example);
- Review and Enhance UDRP mechanisms[6].

[6] UDRP stands for Uniform Dispute Resolution Policy. The UDRP was introduced in the year 2000 to offer an efficient time and cost saving procedure to settle disputes over domain names in the gTLD name space. The UDRP is an online service which is not linked to a special national jurisdiction. The UDRP defines criteria under which conditions a domain name is used in "bad faith" which than allows the UDRP Panel to make a decision on a transfer of the domain name to the challenger. Registrars get their ICANN accreditation only if they accept UDRP decisions as binding. However, conflicting parties can move a case also to a national court which leads very often to long and expensive procedures. UDRP should protect in particular trademarks and intellectual property against misuse in domain names. ICANN has recognized five so-called UDRP Service providers, among them also the WIPO Arbitration Center and the Czech Arbitration Center which is also the dispute resolution service provider for the .eu domain (.euADR). Since its introduction more than 10.000 cases has been settled via the UDRP Procedure. http://www.wipo.int/amc/en/docs/icann291107.pdf

3. CONCLUSIONS

3.1 Is there a European IG Approach?

There is no 'European Internet'. However, the European Commission played a strong and critical role in the making of ICANN in 1998. The European Commission is a member of the GAC and participated also in the WGIG. In 2005 the EU proposed a 'New Cooperation Model' (NeCoMo) at the UN World Summit on the Information Society (WSIS). As a result of this initiative the IGF was created (where the EU is a member of the Multistakeholder Advisory Group/MAG) and a process of enhanced cooperation was started which has significantly improved the communication, coordination and collaboration among the various governmental and non-governmental stakeholders.

Both in the ICANN transition and the IGF formation a strong European voice is needed. There are strong and numerous European players with special interests within the ICANN family like RIPE-NCC[7], CENTR[8], national Registries, Euro-ISPA[9], EU-RALO[10], Internet Economy associations etc. Europeans can contribute with their values, best practices and other experiences for a further improvement of ICANN processes and the IGF.

However the Europeans themselves can still improve the implementation of the principle of multistakeholderism in their own region. The level of interaction and cooperation among the various players and governmental and non-governmental stakeholders within Europe is rather low.

Too often the various constituencies are sitting isolated in their “silos” and do not have the needed close communication with other stakeholders. The European Internet Users Platform (EU-RALO) is still very weak and needs broader support. For national Parliaments in EU member states the issue of Internet Governance does not play a role. Constituencies from European countries, which are not member of the EU – like Russia, Ukraine or Turkey – are totally underrepresented both in ICANN and the IGF.

New initiatives like the 'European Dialogue on Internet Governance' (EURODIG) or the various national IGFs (United Kingdom, Germany, France, Italy) which emerged in 2008 and were driven by mixed consortia of parents from governmental, private sector and civil society organisations have offered new opportunities for an enhanced communication among the various European stakeholders. These discussions will help to develop own positions and to raise the European voice in the global process both within ICANN and at the IGF.

The European Parliament has adopted a resolution in January 2008 to promote a process for the launch of a European Internet governance Discussion platform.

[7] The RIPE NCC is one of five Regional Internet Registries (RIRs) providing Internet resource allocations, registration services and co-ordination activities that support the operation of the Internet globally.

[8] **CENTR** is an association of Internet Country Code Top Level Domain Registries such as .uk and .es.

[9] EuroISPA is a pan European association of European Internet Service Providers Associations (ISPAs).

[10] EU-RALO sub-group of ICANN At-Large (individual Internet user community) for the European region, providing news, key resources and interactive features for information sharing for individuals and end-user groups in the European region interested in ICANN and shaping the future of the Internet, https://st.icann.org/euralo/index.cgi.

The European Commission moderates the 'High Level Internet Governance Working Group' (HLIGWG) a rather closed unit which is open to EU member states only. It would make sense to look into a more holistic approach about European involvement both in ICANN and IGF and to enhance both within the EU and within the broader Europe communication, coordination and collaboration among the various stakeholders.

3.2 Looking into the Future

The governance aspect will remain an important part of the future Internet, in particular if new technical protocols touch public policy components like privacy, security, freedom of expression, intellectual property rights etc. With new innovations it will become more and more difficult to distinguish between the technical and public policy components. There is an objective need for a new governance model which combines the positive experiences of both the traditional and the modern mechanisms. Multistakeholderism will be certainly a guiding principle also for the management of the 'Next Generation Networks' (NGN), for the 'Internet of Things' and the “Object Naming System” (ONS) but it has to be embedded in a right way in already existing mechanisms.

To a certain degree ICANN and IGF can be seen as political laboratories pioneering unchartered territory of policy development in the information age by creating new innovative governance mechanisms. Such mechanisms could become also a source of inspiration for the management of other global challenges like climate change, energy problems and even the financial crisis where a new cooperative model for the interaction among governmental and non-governmental actors are needed.

Traditional intergovernmental organisations will neither disappear nor be substituted. But they will become part of a broader environment and have to enhance their collaboration via new partnerships with non-governmental stakeholders. Each stakeholder has to take its own responsibility in its field of special competence. Such a concept of shared responsibility is needed to meet the global challenges of the 21st century. Shared responsibility can lead also to an enhanced understanding of national sovereignty in the information age in form of 'shared sovereignty', based on mutual respect of basic values. The ongoing power shift as a result of the 'information revolution' will continue and has the potential risk to lead to new forms of power struggles. The challenge is to avoid a 'Clash of Cultures' and to find an innovative, creative and constructive co-existence between the two governance modes.

BRIEFING PAPER PROF. ROLF WEBER :
TRANSITION FROM IPV4 TO IPV6: SUCCESS AND CHALLENGES

EXECUTIVE SUMMARY

In the field of the Internet, technology is an essential aspect of regulation and governance. The transition from IPv4 to IPv6 mainly concerns issues of technical coordination and architecture. Notwithstanding the fact that the capacity shortage of IPv4 as a limited resource does not materialise as early as previously assumed, preparations for the application of the new technical parameters of IPv6 need to be taken at hand. In this respect political and social actors should emphasise the importance of interoperability conditions of the new protocol both at the hardware and the software level. The transition to IPv6 also makes sense since the new protocol improves the built-in security.

The critical aspects of the transition from IPv4 to IPv6 do not concern the openness of the technical access which can be secured by acknowledged mechanisms such as the essential facilities doctrine. Moreover, the administration of scarce resources is the main feature. As experienced in the previous history of ICANN, the actual participation of the Internet users in the discussion is rather limited and representatives of organisations do not always have a democratic legitimisation. Therefore, adequate solutions are to be developed in order to improve the legitimacy in Internet governance (concept of “multi-stakeholderism”).

The introduction and deployment of IPv6 causes costs and increases the need to support less developed countries in building appropriate IT infrastructures, in order to achieve an inclusive information society and bridge the digital divide. As financing mechanisms, the Official Development Assistance, the financial support given by the International Monetary Fund and the World Bank Group, the public-private partnership schemes and the 1% digital solidarity principle can be taken into account. Apart from the actual financial means, less developed countries might also need technical assistance; knowledge-sharing could be a valuable objective of a corresponding EU initiative.

1. INTRODUCTION

As a form of global governance, Internet governance should be seen in the context of an international conceptual setting which describes the combination of rule-making systems, political coordination and problem solving, making global Internet governance a highly ambitious and complex undertaking (Weber, R.H. and Grosz, M., 2007: 119-121). Indeed, the particularities of the Net have to be taken into account, such as its technological foundations as well as its normative "backbone", which, from the very beginning, was based on self-regulation by its users and hence developed beyond a legal framework in the traditional sense.

The discussion topics in the context of the transition from IPv4 to IPv6 particularly relate to aspects of technical coordination and architecture. Internet Protocol (IP) addresses function as unique identifiers of the technical backbone for the Internet hosts connecting to the Net, and as a consequence, enable the interconnectivity between different Internet hosts (Zittrain, J., 2008: 28-29). The transition from the fourth to the sixth version of IP addresses entails several challenges not least in the field of Internet governance.

The following chart allows an overview and the framing of the IPv4/IPv6 allocation (Malcolm, J., 2008: 92; see also the list of abbreviations at the end of this study):

	Technical coordination	**Standards development**	**Public policy**
Rules	ICANN/NTIA JPA	ITRs	Cybercrime Act
Norms	IAB oversight	RFCs	Spam blocklists
Markets	gTLD registries	S/MIME	Content regulation
Architecture	IPv4/IPv6 allocation	DNSSEC	CA/Browser forum
Networks	ICANN SOs and ACs	P3P	LAP

The technical coordination of IPv4 and its architecture need to be embedded in the legal framework in order to give some guidance on the way to achieve an inclusive information society. The relevant legal questions can be summarised as follows:

- How long will enough IPv4 addresses be available? How can a better allocation of the remaining IPv4 address space and better re-use allocated address space be achieved?
- Are there risks of severe economic and technical dislocations during the transition from IPv4 to IPv6? What are the drivers and challenges for the transition towards IPv6 through a dual IPv4/IPv6 environment?
- What are the drivers and challenges of IPv6 deployment? What is the current status of IPv6 deployment?
- What is the role of the different stakeholders in the transition to IPv6? Are Internet-poor countries ready in upgrading themselves to IPv6? Is there a need for an EU initiative on this technology?

In sum, the subject of the ongoing adoption of IPv6 highlights an issue that runs through discussions on Internet governance and the Internet Corporation for Assigned Names and Numbers (ICANN) in particular like a red thread, namely the linkage between technical and public policy issues.

Indeed, ICANN was particularly criticised for positioning itself as a merely standard setting and technical coordination entity (Weber, R.H., 2002: 106-108), whilst it seems clear that important public policy choices are made within this corporation, which accomplishes vital tasks for the functioning of the Internet, specifically with its operation of the Domain Names System (DNS).

The EU Commission correctly reacted to the technical developments by tackling the consequences for the civil society, mainly in the context of the Lisbon Strategy (Commission of the European Communities, 2008: 2-3):

- Communication from the Commission of the European Communities, Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6, Brussels, 21.2.2002, COM(2002) 96[11].
- Active involvement in the establishment of "IPv6 Task Forces" in different regions (European Task Force, African Task Force, Asia Pacific Task Force, Latin American Task Force, Middle East Task Force, and North American Task Force[12]).
- Communication from the Commission of the European Communities, Advancing the Internet, Action Plan for the deployment of Internet Protocol version (IPv6) in Europe, Brussels, 27.5.2008, COM(2008) 313[13].

In the following, the success and challenges caused by the subject of the transition from IPv4 to IPv6 with a view to Internet governance will be addressed.

2. TECHNICAL FRAMEWORK

2.1 Problem of Restricted Capacity

Technically, every Internet host wishing to be directly accessible for another Internet host must be assigned to a public IP address which serves as a unique identifier. The current IP addressing system, IPv4, is at risk not to be able to satisfy all IP addresses requests made by the present and future Internet hosts, since the architecture of addresses, constituted according to IPv4, is a limited resource (Malcolm, J., 2008: 10). As a consequence, a capacity shortage is anticipated; in early 2008, 16% of capacity was left in the pool, i.e. approximately 700 million IPv4 addresses. However, scholars have not yet agreed on the specific point in time, when the shortage will become an actual problem; assumptions count on slightly more than 1000 days (Commission of the European Communities, 2008: 3-4[14]).

The problem of shortage could be mitigated by various techniques such as "Network Address Translation" (NAT), hiding multiple Internet hosts behind a single IP address by connecting private networks to the public Internet. However, such a procedure would have the disadvantage of breaking end-to-end connectivity.

[11] Available at ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ipv6-communication_en.pdf.

[12] *See* http://www.ipv6tf.org.

[13] Available at http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/comm-ipv6-final_en.pdf.

[14] *See* http://www.potaroo.net/tools/ipv4/index.html.

As a result, Internet interactivity would no longer be fully granted, making it difficult to establish Internet telephone calls directly between two hosts using standard voice over IP (VoIP) protocols. Furthermore, the method adds complexity as there are two classes of computers: some with a public address and some with a private address, increasing costs for design and maintenance of networks as well as for the development of applications (Commission of the European Union, 2008: 4).

Another measure would consist in establishing a market enabling a trade of IPv4 addresses; further alternatives could envisage offering incentives to sell unused addresses and reclaiming those already-allocated address blocks that are under-utilised. However, these methods also have drawbacks, as IP addresses are not strictly property, and mechanisms for enforcing the return of addresses do not exist (Commission of the European Union, 2008: 4). Nevertheless, despite such technical and administrative means, sooner or later the demand for IP addresses cannot be satisfied anymore by the IPv4 version.

The impact of the shortage of IP addresses on the Internet's interactivity shows the difficulty in establishing architectural change. Already ten years ago (in 1998), the substitute for IPv4, namely IPv6, was recommended as the next generation IP addressing scheme for implementation (Malcolm, J., 2008: 13). The design of IPv6 aims at providing quantitative and qualitative advantages compared to the current IPv4. Originally it was assumed that IPv6 would be adopted by the year 2005; nevertheless, the process has been delayed. However, it is certain that the Internet's technical architecture must be re-engineered in order to cope with the future addressing needs.

IPv6 is the best way forward, as it provides for a long term solution to address space problem, with a huge number of addresses which can be managed more easily than in the framework of IPv4. Furthermore, IPv6 includes issues such as service, auto-configuration, security, and mobility.

Developing and deploying services and applications is less complicated and less costly than in the IPv4, thereby providing a basis for innovation and empowering users, allowing them to have their own network connected to the Internet (Commission of the European Union, 2008: 5).

2.2 Technical Standards

Both IPv6 and IPv4 define the network layer protocol, i.e. how data are sent from one computer to another over packet switched networks[15]. However, IPv6 contains specific addressing and control information to route packets for the next Internet generation. IPv6 has a very large address space and consists of 128 bits as compared to 32 bits in IPv4; the 128-bit system also provides for multiple levels of hierarchy and flexibility in addressing and routing. Therefore, the present shortage or even exhaustion of addresses in IPv4 can be overcome with IPv6, supporting 3.4 times 10^{38} unique IP addresses. In addition, this addressing scheme will also eliminate the need of network address translation that causes several networking problems (such as hiding multiple hosts behind a pool of IP addresses) within the end-to-end nature of the Internet.

[15] Technical information can be drawn from the following website: http://www.ipv6.com/articles/general/ipv6-the-next-generation-internet.htm.

The rules and packet sizes for the transport of IPv6 datagrams differ depending on their topology; there is a Request for Comment (RFC), i.e. a technical standard on a particular aspect of the Internet, covering each topology in detail. For state-less auto configuration, the Media Access Control (MAC) address is used to build the IPv6 address; the rules that govern how IPv6 multicast destination addresses are converted to MAC addresses are the same as those used on Ethernet. IPv6 address negotiation is different from IPv4 since it is done through ICMPv6 neighbour discovery and not through Point-to-Point Protocol (PPP); this technical approach also allows using static addresses. The IPv6 functionality for address auto-configuration supports easy administration and customer configuration with minimal costs and enables peer-to-peer services, push services as well as VolP (Hagen, S., 2006: chapter 7.1).

Mobile IPv6 is an IETF (Internet Engineering Task Force) standard that has augmented the roaming capacities of mobile nodes in the IPv6 network. The major benefit of this standard is that the mobile nodes change their point-of-attachment to the IPv6 Internet without changing their IP address, allowing mobile devices to move from one network to another and still maintain their existing connections. IPv6 uses both types of auto-configuration, such as state-less (network prefix and interface ID) and state-full auto-configuration (DHCPv6). The neighbour discovery feature enables (i) the finding of routers, (ii) the determination of link layer addresses and (iii) the maintenance of reach-ability information. In comparison with the existing IPv4 situation, the advanced features of IPv6 make mobile IP easier to implement since the needed functionality, in particular the route optimisation, is built into the program and ingress filtering problems do not occur[16] (Hagen, S., 2006: chapter 7.3).

IPv6 addresses are denoted by eight groups of hexa-decimal quartets separated by colons in between them.

The addresses are broadly classified into three categories, namely (i) unicast addresses acting as identifiers for a single interface, (ii) multicast addresses acting as an identifier for a group/set of interfaces that may belong to different nodes and (iii) anycast addresses acting as identifiers for a set of interfaces that may belong to different nodes. Multicast and anycast are an integral part of the protocol and available on all IPv6 nodes[17] (Hagen, S., 2006: chapter 7.2).

2.3 Interoperability and Security

A major merit of IPv6 can be seen in its more efficient routing and its reduced management requirements facilitating the interoperability with existing protocols. However, IPv6 is not directly interoperable with IPv4: communication between the different devices is only possible by using application specific gateways (Commission of the European Communities, 2008: 4). Nevertheless, a good interoperability is necessary for the netizens to undertake a smooth transition from one standard to another without having to face any significant disruptions of the services. This is particularly of importance since IPv4 will most likely be used for a significant time to come. But any change from one protocol to the other needs resources, both in terms of money as well as in terms of time in view of the fact that the processes need to be newly attuned.

[16] *See* http://www.ipv6.com/articles/mobile/Mobile-IPv6.htm.

[17] *See* http://www.ipv6.com/articles/general/IPv6-Addressing.htm.

Since ICANN modified the DNS route servers on 20th July 2004, the IPv6 adoption and its development have been stimulated. A number of transition mechanisms allow IPv6-only compatible hosts to access services offered by IPv4 protocol; this forms the backbone of the interoperability ingrained in the IPv6 protocol[18]. Consequently, IPv6 can be enabled in parallel with IPv4 on the same device and on the same physical network. This co-existence is expected to last for 10, 20, or even more years (Commission of the European Communities, 2008: 4-5).

Recognising the importance of IPv6 compatibility with the existing IT infrastructure, prominent research groups are conducting studies to test the interoperability parameters of the new protocol both at the hardware and the software level, including firewalls, voice, wireless and application layer interface testing. At the hardware level, such research pertains to testing the performance of different system configurations in an IPv6 framework; at the software level testing involves an assessment of the coordination of various applications at different levels of protocol transition processes[19].

IPv6 also improves the built-in security: Compliance with security concerns include an eased implementation of encryption, authentication, and Virtual Private Networks (VPN) through header extension. The security elements are to be used within IPv6 itself or by applications on top of IP without imposing organisational or legal settings that may render the basic services unusable for the word-wide Internet. The security framework is standardised by the IETF IP Security Protocol Working Group (PSEC), encompassing specific security elements for encryption and authentification as well as definitions for using concrete cryptographic algorithms and specific security policies[20] (Hagen, S., 2006: chapter 5). Notwithstanding the fact that the Court of Justice has recognised that IP addresses may be considered personal data, thereby falling within the scope of application of the Data Protection Directives (95/46 and 2002/58; ECJ, Case C-275/06, Promusicae vs. Telefonica, judgment of 29th January 2008, paragraph 45) and that concerns have been expressed about the IPv6 privacy (Article 29 Data Protection Working Party, 2002), technical experts assume an improvement of the security level in the IPv6 environment.

3. Specific Issues regarding the Transition Period

3.1 Time Factor

The transition from IPv4 to IPv6 is advancing and cannot be stopped, for both technical reasons as well as consumer needs; consequently, IPv6 will co-exist with IPv4. As experience with the introduction of new techniques regularly shows, however, the process is always slower than anticipated. Insofar, it is possible, if not to say probable, that the transition period will last for a few years.

[18] http://www.ipv6.com/articles/hardware/IPv6-Interoperability.htm.

[19] http://www.ipv6.com/articles/hardware/IPv6-Interoperability.htm.

[20] http://www.ipv6.com/articles/security/IPsec.htm.

Since a better re-use of IPv4 only helps temporarily, the problems of the deployment of a new technical architecture cannot be avoided in the long term, but must be tackled and solved. Insofar the EU-Commission is consequent in advocating for a 25% penetration of IPv6 in Europe by the end of 2010 (Commission of the European Communities, 2008: 8[21]).

IPv6 deployment is gaining speed as IPv6 infrastructure is being installed throughout the Internet backbone and the major wide-area networks. In particular the networks of many large telecommunications enterprises as well as the most important Research and Development (R&D) networks have already tested and introduced IPv6. In fact, the simplest way to start using IPv6 has proven to be the implementation of single IPv6 hosts in IPv4 networks; they will auto-configure for a link-local IPv6 address and will be able to communicate with one another over IPv6, by using ICMPv6 neighbour discovery messages (Hagen, S. 2006: chapter 7.4).

Another important issue concerns the question how the remaining IPv4 capacity will be allocated during the next few years. As mentioned (see above No. 2.1.), the shortage problem is not immediate and can be mitigated; however, measures need to be introduced which avoid that the remaining capacity is hoarded up by a few market participants on the basis of a first-come first served mechanism. Moreover, less developed countries having limited financial resources for the transition from IPv4 to IPv6 merit special attention and a priority allocation of capacity to such regions should be taken into account.

3.2 Compatibility

From a technical point of view, the risks related to the existence of two technical architectures and consequently two address systems functioning in parallel do not seem to be very substantial. Most likely, the industry will gradually improve the technical environment thereby enabling to more easily switch between the two architectures. Nevertheless, in the long run it is not deemed efficient to have two systems. Their maintenance costs are relatively high and the handling for the users quite uncomfortable; therefore, a certain "pressure" will exist to completely adopt the IPv6 architecture over time.

In addition, since technologies are in fact socio-technical systems, the characteristics of the systems are to be shaped by the economic and political incentives of the corporate and individual actors as well as by laws and social norms within the design and capabilities of the technologies deployed.

In light of such considerations, the transition period should be used to analyze and test initiatives which ensure the interoperability of IPv4 and IPv6 during a period of smooth coexistence and transition.

Since the Internet is a global framework, many actors worldwide need to be considered. The relevant stakeholders and their responsibilities are listed subsequently (Commission of the European Communities, 2008: 6-7):

- Internet organisations (including the Regional Internet Address Registries) need to manage common IPv6 resources and services and continue to develop needed standards and specifications.
- Internet service providers need to offer IPv6 connectivity and IPv6 based services to costumers.

[21] http://www.ipv6.com/articles/general/timeline-of-ipv6.htm.

- Infrastructure vendors need to integrate IPv6 capability into their products.
- Content and service providers need to be reachable by enabling IPv6 on their servers.
- Business and consumer application vendors need to ensure that their solutions are IPv6 compatible and increasingly need to develop products and offer services that take advantage of IPv6 features.
- End-users need to purchase IPv6 capable products and services and enable IPv6 on their own networks or home internet access.

The business sector in particular should be motivated to better promote the deployment of IPv6 and take into account the following actions (ICC 2007: 35-36):

- The business sector should take advantage of scheduled equipment and software upgrades and develop a timeline, a program as well as procedures to upgrade Internet servers and relevant devices to IPv6, recognizing that the upgrade will require costs and entail further burdens. Such a demonstration of leadership by business will encourage other Internet stakeholders and underline the value that IPv6 brings to the Internet.
- The business sector must recognise that the security and stability of the existing network is an essential requirement in the transition period in which IPv4 and IPv6 will coexist.
- The business sector should continue its efforts to improve government and consumer awareness of the importance and benefits of IPv6, for example, through initiatives such as the IPv6 Forum[22] a consortium of vendors, which organises information events around the world to increase awareness and promote the adoption of IPv6.
- The business sector should continue to provide expert input into the technical coordination bodies responsible for developing and overseeing IP and its related protocols, particularly the Internet Engineering Task Force (IETF). This input will help ensure that as new technologies develop, they are compatible with and take advantage of IPv6.

Since there is “no such thing as a free lunch” the introduction of the new IPv6 architecture will cause costs not only for the industry, but also for the registries and the users. This fact allows the assumption that the establishment and utilisation of IPv6 is more likely to happen in the developed countries in which the civil society is less cost-sensitive. For the same reason, a slower transition process causes the risk that the “digital divide” will become deeper if less developed countries are not in the economic position to speed up the transition process.

A major effort should be taken in respect of encouraging the progressive compatibility between IPv4 and IPv6. Corresponding pressure could be introduced by governments for example in public procurement procedures, if criteria such as compatibility and early migration are requested, as introduced in the recently announced “plan numérique” in France. Governmental support should also attempt to elaborate a policy setting framework, outlining the long term vision for IPv6 and considering the users’ expectations.

[22] http://www.ipv6forum.org.

4. CHALLENGES OF IPV6 DEPLOYMENT

4.1 Allocation of "Critical Resources"

Voices in civil society as well as in legal doctrine often address the problem of "critical resources" of the Internet without delineating a clear definition of the notion. For example, paragraph 72 (j) of the mandate of the IGF also stresses that it is important to "discuss inter alia issues related to critical Internet resources" without providing for a definition[23]. Indeed, "critical resources" in the context of the Internet can have a very broad meaning: Electricity is a critical resource for a mobile computer over time as well as wireless or fixed access to the Internet if electronic communications are to be exchanged (Huston, G., 2007: 1). In the context of IPv4 and IPv6, address elements seem to be the major issue regarding the criticality of resources. From the angle of the informational context, access to valuable contents could also be regarded a scarce resource.

In view of the concrete problems that "critical resources" cause, it appears to be obvious that the term does not only describe a technical access topic, but also the administration of the Internet's naming and addressing of domains. Theoretically, the routing slots could be a finite capacity; as a consequence, if routing would not work, the address would not be available in the routing system. However, as the development of IPv6 shows, the technical industry provides for solutions in order to overcome such shortages.

Therefore, critical Internet resources should be understood in a way which allows the inclusion of the institutional and human elements which are critical to the functioning of the Internet, such as organisations, regulatory frameworks and users. In this light it is obvious that the management of critical Internet resources has significant public policy implications. Insofar, the basic structure supporting decision-making must be internationally recognised and clearly mandated. This objective is jeopardised by the fact that the influence on the actual activities in this field is not evenly distributed among all nations of the world; some nations feel that in particular the United States have a privileged position of control and influence, mainly due to their relationship to ICANN.

In general, in order to ease access to scarce resources, the following regulatory issues play a role (Weber, R.H., 2003: 96): (i) open access, (ii) open standards, (iii) open source software and (iv) widespread availability of access points. In the context of the Internet, however, this approach needs an adaptation since technical aspects are not the main relevant issues, but administrative topics are gaining importance. The allocation of IP communication possibilities must be realised in the framework of an emerging, global spontaneous and people-oriented environment.

4.2 Open Technical Access

The matter of technical access is a well known regulatory problem in the telecommunications industry, usually dealt with under the heading of "interconnection" and "unbundling". For several years, legal doctrine and court decisions have recognised that in the case of a monopolistically controlled structure in a specific market, legal intervention is justified if such enterprises misuse their position by not granting open access.

[23] http://www.intgovforum.org/mandate.htm.

This concept has come to be known as the “essential facilities doctrine” (see Radio Telefis Eireann and Independent Television Publications Ltd. vs. Commission of the European Communities, Judgment of the European Court of Justice of 6 April 1995, C-241/91 P and C-242/91 P; IMS Health GmbH & Co. OHG vs. NDC Health GmbH & Co. KG, Judgment of the European Court of Justice of 29 April 2004, C-418/01). A right to access to the essential facility by a competing market participant can be justified on the basis of competition laws (Art. 82 TEC) and of specific regulatory frameworks (electronic communications directives). In the context of the Internet, however, experience has shown that open technical access has not become a problem.

4.3 Administration of Scarce Resources

An important body in the Internet governance field is the Internet Society (ISOC), having been founded as a non-profit, non-governmental membership society with the aim to promote the development, the availability and the associated technologies of the Internet (Grosz, M. forthcoming). ISOC is the organisational home for entities responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). Since the establishment of ISOC in 1992, its central role is to support, facilitate, and promote different aspects on Internet development; therefore, ISOC is engaged in the global transition to the new technology of IPv6. Its guiding public policy principles include open, unencumbered, and beneficial use of the Internet. However, ISOC does not have any decision-making power and can therefore not been seen as the “critical” body being responsible for an adequate deployment of IPv6.

The present central governing core of the Internet is ICANN, a non-profit Californian organisation. In order to ensure universal resolvability, which allows the netizens from all over the world to find all valid addresses on the Internet, a global system of unique identifiers needs to be coordinated and must ensure stable and secure operations (Weber, R.H., forthcoming). The unique identifiers encompass three functional sets, namely the domain names, the Internet Protocol addresses and autonomous system numbers, as well as the protocol port and parameter numbers. ICANN is responsible for the management and oversight of these specific functions; thereby, its main values envisage the preservation and enhancement of the operational stability, reliability, security, and global interoperability of the Internet.

As discussed in the context of the Domain Name System (DNS), an obvious risk of the present ICANN system concerns the fact that privately-established rules may erode or undermine the power of sovereign states. Moreover, the actual participation of the Internet users in the discussions is rather limited (Weber, R.H. and Weber, R., forthcoming) and representatives of organisations do not always have a democratic legitimisation (Weber, R.H. and Grosz, M., 2008: 301-304).

Furthermore, the US influence might be considered as an undue privilege by other nations. Nevertheless, it should not be overlooked that social norms in the form of self-regulation often create efficient rules in non-hierarchical communities. With social norms, participants usually access problems more directly and generate fewer transaction costs compared to administrative legal frameworks. Furthermore, social norms signify a decentralised form of social control; experience in the online world shows that participants maintain a continuing commitment to the principle of open process developed in the field of the Internet.

The intensive discussions held in relation to ICANN’s administration of the DNS equally apply to the allocation of IP parameters and the deployment of IPv6.

The relatively young, but maturing institutions such as the IETF, the ICANN, and the Regional Internet Address Registries provide a new locus of authority over governance processes affecting Internet standards and causing governments to begin figuring out how to react to these “native” institutions. Consequently, adequate solutions are to be looked for in order to improve the legitimacy in Internet governance. Generally, a self-regulatory approach must fulfil certain basic conditions, particularly in respect of Internet Protocols (Weber, R.H., 2002: 109): (i) The administration of scarce resources needs to be transparent; (ii) a private organisation should also be obligated to account for its actions; (iii) the rule making process and any dispute resolution system must provide due process; (iv) acceptable criteria are necessary to protect third parties. In a nutshell, satisfying democratic needs requires truly people-centred responses.

Notwithstanding the importance of these principles it cannot be overlooked that the main actors of allocation of the mentioned critical resources remain the Internet Service Providers (ISP). Substantive principles can “only” be promoted by governments in view of the fact that IPv6 has elements of a public good which should be allocated to individuals based on reasonable and proportionate standards. Known approaches such as “first come, first served” or “auction procedures” can be too radical if the interests of the weaker parts of the civil society are not properly taken into account. In addition, another aspect should not be underestimated: The transition from IPv4 to IPv6 could be taken as a reason for changing the address allocation process from the present system including ICANN, the Regional Internet Address Registries, and the Internet Service Providers to a new system which would “insert” National Registries into the process. Such a development could increase the risk of a strict national control of Internet traffic which does not seem to be in the interest of the civil society.

The heterogeneity of the different actors in the field of the Internet is addressed by the concept of “multi-stakeholderism”, encompassing the governments, the private sector, the civil society and the international organisations, thereby overriding the differences between public and private actors and building global participation (Weber, R.H. and Grosz, M., 2008: 308-310). The comprehension of a unitary stakeholder foundation may be questioned, in particular in view of perceptions of a rather fragmented and polarised Internet. Shifting the focus to the different organisational bodies involved in the numerous aspects of the Internet helps channelling a very manifold stakeholder-basis into an intermediate level of representatives within the organisational structures. In deciding who shall be admitted as a representative and to what extent specific prerequisites should be met, valuable inputs could be derived from the EU as a supranational organisation, having to balance the objectives of the Union as a whole with the interests of the individual Member States (Komaitis, K., 2008: 69-75).

With the affected stakeholders delineated, legitimacy could be enhanced by adhering to particular architectural principles. Such key principles need to be considered as a source for legislation and a guideline for governing different aspects of the Internet. Similarly to a Magna Charta or a constitutional approach, substantive principles should call for self-constraints by the governing authorities; by existing independently of the actual policies and the decision-making entities, such principles foster the establishment of a sort of “checks and balances” regime, provide for a basis for the assessment of the governing outcomes, and facilitate transparency and accountability (Komaitis, K., 2008: 71; Weber, R.H. and Grosz, M., 2008: 310).

4.4 Availability of Resources – Financing Mechanisms

Another important topic concerns financing and knowledge-sharing aspects. The introduction and deployment of IPv6 causes costs and increases the need to support technologically less developed countries in building appropriate IT infrastructures in order to achieve an inclusive information society and bridge the digital divide. The Internet as a global framework asks for people of all regions to be involved. The fact that private persons can be involved in the deployment of IPv6 makes assistance to and support of developing countries important in order to include all interested parties in the process.

4.4.1 Action related to the European Union

The European Commission has provided and will provide financial aid through standardisation support actions to improve interoperability of networks. In this context the Commission is supporting standardisation actions on protocols running over IPv6 networks. In a public consultation, the use of public procurement was identified as an efficient way to speed up the transition to IPv6 (European Commission, 2008: 9).

Furthermore, the European Commission is encouraging research projects funded by Framework Programme 7[24]; thereby, new IT hardware and software should be developed which increase the possibility of choosing computer network protocols and facilitate the utilisation of IPv6 (European Commission, 2008: 9).

The European Commission is also envisaging to bring together IT managers from member states to exchange their experiences and to monitor the progress of IPv6 deployment and will specify IPv6 capabilities as well as carry out timely and appropriate internal trials and projects to prepare for IPv6 (European Commission, 2008: 10).

In addition, the European Commission intends to undertake awareness campaigns and support actions to disseminate practical deployment knowledge as well as standardisation actions in relation to IPv6 interoperability. Furthermore, member states are invited to support the inclusion of IPv6 technology knowledge in relevant retraining curricula and in computer and network engineering courses of universities etc. The launch of accompanying studies as well as the organisation of conferences is expected within the next year (European Commission, 2008: 10).

The efforts of the European Commission in raising awareness of the challenges related to the transition from IPv4 to IPv6 merit a positive appreciation.

Indeed it is important to achieve compatibility and interoperability of standards at an early stage in order to allow the users of the Internet to easily adapt their requirements to the new protocol. The standards supporting actions are also valuable, but attention needs to be paid to the risk of eventual anticompetitive distortions by governmental interventions privileging certain suppliers of goods and/or services. Therefore, supporting actions should be supplier-neutral. As long as financial aid is mainly directed towards encouraging research projects of independent facilities, the respective risks can be mitigated. If properly applied, the actions designed by the European Commission might contribute to the establishment of an inclusive society within a reasonable time frame.

[24] http://www.nerc.ac.uk/funding/framework.

4.4.2 Action related to Developing Countries

With regard to developing countries, although generally favouring a market-based approach, politicians and academics emphasise that, with regard to the high investments, the private sector is unlikely to be able to answer the financial needs of the developing world alone, without some support from the public sector. As the Recommendation (2007) 16 of the Council of Europe (Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on the measures to promote the public service value of the Internet, adopted on 7 November 2007) requests, member states should develop strategies which promote technical interoperability and open standards in ICT. It is therefore paramount, on the one hand, that governments strive to provide the enabling environment and basic conditions for the private sector to play its growth-driving role by spending more funds on development and, on the other, that the international community commits to increased development aid. As the Commission for Africa Report underlines: “the promotion of growth is not a question of the state versus the private sector but a question of how they combine to generate growth” (Commission for Africa, 2005: chapter 7 para. 31).

Already large varieties of financing mechanisms are in place and could be taken into account when considering possibilities of financing ICT development (Weber, R.H. and Menoud, V.: 63-177):

- The Official Development Assistance (ODA) provided by national states has still not yet received the 0.7% of the gross national product as committed in the Monterrey Consensus and should improve governance aspects, notably by making more coordination disclosure efforts, as well as streamlining national ODA strategies in order to pay more attention to the Millennium Development Goals.
- The financial support given by the International Monetary Fund (IMF) and the World Bank Group should be better coordinated and designed in a more concrete way in order to improve country specific needs and to allow the provision of quick advisory support related to a country’s agenda.
- Public-private partnership schemes are a valuable alternative if the public and private sector cannot easily act individually, detached of each other, and if governance principles, transparency requirements and accountability disciplines are nailed down.
- A promising new financing mechanism is the 1% digital solidarity principle enabling a state authority (on a national, regional and local level) to levy a 1% charge on the value of public procurement contracts in the ICT field; such amounts are to be made available to ICT projects in less developed countries.

The costs of upgrading IPv4 to IPv6 should not be overestimated; however, apart from the actual financial means many less developed countries might also ask for technical assistance. As far as the new technologies are concerned, a need for an EU initiative appears to be given; knowledge-sharing would call for technical support.

5. CONCLUSION

The transition from IPv4 to IPv6 mainly concerns issues of technical coordination and architecture. Notwithstanding the fact that the capacity shortage of IPv4 as a limited resource does not materialise as early as previously assumed, preparations for the application of the new technical parameters of IPv6 should be taken at hand. In this respect political and social actors need to recognise the importance of interoperability conditions of the new protocol both at the hardware and the software level. Since IPv6 also has its merits as it improves the built-in security, the transition is a worthwhile movement. As far as the remaining IPv4 capacity is concerned, attention has to be given to an appropriate world-wide allocation taking into account the needs of less developed countries.

The simplest way to start using IPv6 has proven to be the implementation of single IPv6 hosts in IPv4 networks; they will auto-configure for a link-local IPv6 address and be able to communicate with one other over IPv6, by using ICMPv6 neighbour discovery messages. The EU-Commission is consequent in advocating for a 25% penetration of IPv6 in Europe by the end of 2010. Since IPv4 and IPv6 will have to be used in parallel for quite some time, compatibility of the technical parameters needs to be realized to the most advanced stage possible.

The critical aspects of the transition from IPv4 to IPv6 do not concern the openness of the technical access which can be secured by acknowledged mechanisms such as the essential facilities doctrine, notwithstanding the fact that open access, open standards, open source software and widespread availability of access points are important to ease access to scarce resources. However, in the framework of the Internet, administrative topics need to be considered in particular. The allocation of IP communication possibilities must be realised in the framework of an emergent, global spontaneous and people-oriented environment, i.e. the administration of scarce resources is the main feature. As experienced in the previous history of ICANN, the actual participation of the Internet users in the discussion is rather limited and representatives of organisations do not always have a democratic legitimisation. Therefore, adequate solutions are to be developed in order to improve the legitimacy in Internet governance (concept of "multi-stakeholderism").

The introduction and deployment of IPv6 causes costs. Accordingly, the establishment and utilisation of IPv6 is more likely to happen in the developed countries in which the civil society is less cost-sensitive. Consequently, increased support to less developed countries in building appropriate IT infrastructures is necessary in order to achieve an inclusive information society and bridge the digital divide. As financing mechanisms, the Official Development Assistance, the financial support given by the International Monetary Fund and the World Bank Group, the public-private partnership schemes and the 1% digital solidarity principle can be taken into account. Apart from the actual financial means, less developed countries might also need technical assistance; knowledge-sharing could become a valuable objective of a corresponding future EU initiative.

BIBLIOGRAPHY

Art. 29 Data Protection Working Party	Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf.
Commission of Africa (2005)	Our Common Interest: Report of the Commission for Africa, March 2005, available at http://www.commissionforafrica.org.
European Commission (2008)	Advancing the Internet, Action Plan for the deployment of Internet Protocol version (IPv6) in Europe, Brussels, 27/05/2008, COM(2008) 313, available at http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/comm-ipv6-final_en.pdf
Grosz M. *(forthcoming)*	Grosz, M., 'Internet Society (ISOC)', Tietje, Ch. and Brouder, A. (eds), *Handbook of Transnational Economic Governance Regimes*, Martinus Nijhoff, Leiden, forthcoming 2008.
Hagen S. (2006)	Hagen, S., *IPv6 Essentials*, O'Reilly, Beijing, 2nd edition 2006, available at http://proquest.safaribooksonline.com/0596100582.
Huston G. (2007)	Huston, G., 'On the Hunt for "Critical Internet Resources', available at http://www.circleid.com/posts/critical_internet_resources/.
ICC (2007)	ICC, *An Inventory of Policy Positions and Practical Guidance*, 1st ed. Paris 2007.
Komaitis K. (2008)	Komaitis, K., 'Aristotle, Europe and Internet Governance', *Pacific McGeorge Global Business & Development Law Journal*, Vol. 21, 2008, pp. 57-77.
Malcolm J. (2008)	Malcolm, J., *Multi-Stakeholder Governance and the Internet Governance Forum,* Terminus Press, Perth, 2008.
Weber R.H. (2002)	Weber, R.H., *Regulatory Models for the Online World*, Schulthess, Zürich, 2002.
Weber R.H. (2003)	Weber, R.H., *Towards a Legal Framework for the Information Society*, Schulthess, Zürich, 2003.
Weber R.H. (2008)	Weber R.H., 'Accountability in Internet Governance', forthcoming 2008.
Weber R.H. (forthcoming)	Weber R. H., 'Internet Corporation for Assigned Names and Numbers (ICANN)', Tietje, Ch. and Brouder, A. (eds), *Handbook of Transnational Economic Governance Regimes*, Martinus Nijhoff, Leiden, forthcoming.
Weber R.H. and Grosz M. (2007)	Weber, R.H. and Grosz, M., 'Internet Governance – From Vague Ideas to Realistic Implementation', *Medialex*, No. 3/07, Stämpfli Publikationen AG, Bern, pp. 119-135.
Weber R.H. and Grosz M (2008)	Weber R.H. and Grosz, M., 'Legitimate Governing of the Internet', in: Kierkegaard, S. M. (ed.), *Synergies and Conflicts in Cyberlaw*, 3rd International Conference on Legal, Security and Privacy Issues in IT, Prague, September 3-5, 2008, pp. 300-313.
Weber R.H. and Menoud V. (2008)	Weber, R.H. and Menoud, V., *The Information Society and the Digital Divide*, Schulthess, Zürich, 2008.
Weber R.H. and Weber R. (forthcoming)	Weber, R.H. and Weber, R., 'Public Participation in the Internet – Lessons from the Environmental Legal Framework?'.
Zittrain J. (2008)	Zittrain, J., *The Future of the Internet and How to Stop It*, Yale University Press, New Haven, 2008.

LIST OF ABBREVIATIONS

CA/Browser Forum	Certification Authority Browser Forum
COM	(European) Commission Document
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ECJ	European Court of Justice
ed./eds.	editor/editors
gTLD	Generic Top-Level Domain
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
ICANN ACs	Internet Corporation for Assigned Names and Numbers Advisory Committees
ICANN SOs	Internet Corporation for Assigned Names and Numbers Supporting Organisations
ICC	International Chamber of Commerce
ICMPv6	Internet Control Message Protocol Version 6
ICT	Information and Communication Technology
ID	Identification
i.e.	that is; Latin abbreviation for "id est"
IETF	Internet Engineering Task Force
IMF	International Monetary Fund
IP	Internet Protocol
IPv4/IPv6	Internet Protocol version 4/6
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITR	International Terrestrial Reference System
JPA	Joint Project Agreement
LAP	London Action Plan
MAC	Media Access Control
NAT	Network Address Translation
No.	number
NTIA	National Telecommunications and Information Administration
ODA	Official Development Assistance
OJ	Official Journal of the European Union
p/pp	page/pages
PPP	Point-to-Point Protocol

PSEC	IETF IP Security Protocol Working Group
P3P	Platform for Privacy Preferences
RFCs	Request for Comments
R&D	Research and Development
S/MIME	Secure/Multipurpose Internet Mail Extensions
TEC	Treaty establishing the European Community (consolidated text), OJ C 325 of 24 December 2002, 33-184
VoIP	Voice over IP
Vol.	Volume
VPN	Virtual Private Networks
vs.	versus

BRIEFING PAPER PROF. YVES POULLET
INTERNET OF THE FUTURE: ACHIEVING TRANSPARENCY, PLURALISM AND DEMOCRACY

EXECUTIVE SUMMARY

The title quite ambitious leads to analyse the main challenges our fundamental freedoms have to face in our Information Society. Our reflections start with a description of the main characteristics of the technological landscape and their significance. This description introduces two main debates:

- the first one is related to the impact of new ICTs on our privacy considered in the broadest sense as the condition for each individual to dignity and self determination;
- the second one analyzes how freedom of expression is threatened in our Information Society.

On these two issues, certain avenues of inquiry will be developed and solutions will be suggested in order to avoid interference with these two fundamental liberties. In conclusion we will address reflections about the role of the Technology, the State and the Citizens.

1. INTRODUCTORY REMARKS

ICT a major tool for our liberties - Information Communication Technologies (ICTs) with their ubiquitous and universal characteristics are drastically modifying our environment as well as our economic and social relationships. This trend will increase in the future in a way which is only partially predictable at the time being. The ICT are used in an increasing number of contexts and are offering to each of us a place without limits where we are able to better express ourselves, where we have access to more and more personal services but also where the physical or social barriers which separated the various visions of the world tend to disappear. In this sense, ICTs create a unique opportunity to develop ourselves and to enter into a dialog founded on the recognizance of a large diversity of opinions. This might contribute to a cultural, economic, intellectual, democratic and human enrichment of the global society.

Between dream and nightmare - Nevertheless, if we are not cautious, this dream − which is inherent to the potential development of the Information Society − might turn into a real nightmare. The way in which the technologies are presently designed and applied can severely affect the development of our liberties and of our democracies. Our contribution aims to define the challenges raised by the development of ICTs in order to propose certain reflections and possible solutions both at the European level and at the global level in the context of the next IGF.

2. THE INFORMATION SOCIETY: MAJOR TRENDS[25]

2.1 Trends as regards the technologies themselves

About Moore's Law **-** The development of ICT can be firstly described in a continuous and tremendous growth of computer and communication systems capacities. The so-called Moore's Law predicts that every 18 months the storage capacity of a computer is multiplied by two for the same price, which implies the multiplication by 1,000 in fifteen years. It is becoming possible to store on a personal computer the records of all the events of my life and to set-up a central GRID collecting the basic identification data of all people around the world. This capacity of storage doubled by an increasing capacity of processing and transmission explains how Google can validate your request, scanning in less than 10 seconds more than a thousand million sites worldwide. It explains also the development of what we call the Web 2.0 multimedia applications like YouTube, Daily motion, etc.

Internet revolution **-** The Internet revolution might be described from different points of view. The global character of this network has a double meaning. It means not only the universal dimension of this infrastructure, implying the interoperability of technical norms[26]. Internet also leads to the convergence of all networks, which were traditionally clearly separated like TV channels and mobile infrastructure and thus the possibility to cross match the data created by all these communication activities. That convergence is doubled by the convergence of the terminal. Our mobile devices and computers are achieving today activities like voice telephony services, TV or radio programmes reception, e-mails communications, etc. which 30 years ago were reserved to specific and dedicated terminals.

Ambient Intelligence **-** Ambient Intelligence[27] is perhaps the more recent outcome of the ICT evolution. With the miniaturization of the terminals to a "smart dust" and their implantation in objects, clothes and even in our own bodies, it is now possible to conceive interaction among human beings and their environment, through this "Internet of Things". The technology is becoming ubiquitous covering all the events of our everyday life. We also speak of a "learning technology" insofar as it is able to adapt its functioning to the data obtained through its use. The networks created by the dialogue between things, among things or between things and people create a space progressively invested by ICTs. At the heart of these networks, the human being can become a "thing" itself inserted into a relation with other things which react to its or his/her presence.

[25] For a more complete view on these trends, see Y. Poullet – A.Rouvroy, "Introductory Remarks, General report, European Conference on Ethics and human rights in a Information Society organized by UNESCO and Council of Europe, Strasbourg, 13-14 Sept., 2007 available at the UNESCO website.

[26] An additional effort to coordinate infrastructure is being propelled by the European Organization for Nuclear Research (or "CERN", Europe's scientific consortium where the World Wide Web was born). CERN's Large Hadron Collider Computing Grid project includes a plan "to integrate thousands of computers worldwide into a global computing resource," or Grid. The project's most enthusiastic proponents contend: "*The Grid goes well beyond simple communication between computers and aims ultimately to turn the global network of computers into one vast computational resource.*".

[27] "*The central idea of these networks is to create environments in which people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects. It is an environment that is capable of recognizing and responding to the presence and actions of different individuals in a seamless, unobtrusive and often, invisible way using several senses*".

***Digital identities* -** "Digital identities" are increasingly linked to individuals or to be more precise with his or her bodies (biometric data) or with objects under their use (cookies or IP as regards the personal computer or the communication mean; tag number as regards RFID[28] enshrined in clothes or…) or simply with works or objects belonging to individuals or not[29]. One underlines the different roles of these "digital identities". They firstly might be used as "authentication" tool, especially to permit the access to certain resources. Secondly they are essential for the reconstruction of an informational image about a person - identified or not - apart from pieces of information scattered in databases geographically dispersed through the network and that without any limit of borders. In other words they permit the traceability (the capacity to follow the movement of a person, a good or a message) and more the ability to establish links among different databases in order to retrieve the information concerning the same individual identified or not (e.g. cookies, RFID tag number, etc.)[30]. Digital identifiers (like IP address, RFID tag number) permit also to contact people by sending us appropriate messages. **That triple characteristic of digital identifiers, link ability, traceability and contact ability, explains why special attention must be given to that kind of data, which at first glance seem less sensitive than biographic data.** Finally, let us notice that biometric data precisely because there are directly linked with the body are available during the entire life of the individual and that traces revealing DNA might be found very easily (blood, hair, etc.).

2.2 Trends as regards applications

***User Generated Content* -** User Generated Content's applications definitively constitute, from the Internet user point of view, the most prominent new applications on the Web. About 60% of the content available on the web is coming from these new applications, like social networks, Wikipedia, online games or You Tube, generally grouped under the concept of Web 2.0 applications. These emerging applications radically transform the relationships among the actors. In the traditional scheme, the role of the information service provider on one side and the role of the Internet users on the other are quite distinguished and the regulation available is normally reserved only to professionals. What happens when the Internet users are, in the context of these new applications, playing a similar role as the traditional information providers by posting news on there blogs or on You Tube and becoming data controllers by putting information online about themselves and about third parties? Can we consider that the author of a blog is a journalist or an editor, subject to the same deontology and legal duties that the press companies? New risks and threats derive from the very sensitive nature of the data they are posting, the illicit or harmful information they are diffusing, etc. **The privacy risks created by the use of these data by third parties in the context of certain secondary uses are to be pinpointed**.

[28] RFID = Radio Frequency IDentifier.

[29] See the Object Names System (ONS) put into place by GSI in the context of a large development of RFID and in a way quite similar to that chosen for the DNS operated by ICANN with the cooperation of Verisign. ONS will permit to trace a product to know exactly the producer, distributor, the ingredients, etc. Placed at a certain distance of a reader which might be the mobile, it permits a consumer to know exactly the product he or she is purchasing.

[30] Digital identities might be considered as "matching identifiers". "Matching identifier" refers to an item of information making it possible to identify the same individual in two data processing operations, each of which has a different file controller or a distinct purpose. Items of personal data include matching identifiers such as cookies which enable individuals to be recognised and their actions or movements to be tracked over time, whether in cyberspace or not.

We know that employers are often using data concerning their employees available at social networking sites and that companies are using this data to build up profiles and to take decisions on the basis of these profiles which can potentially discriminate the internet users.

***Profiling techniques* -** Precisely the profiling techniques[31] seem to be more and more used by companies or administrations**.** Profiling might be defined as a computerised method involving data mining from data warehouses, which may enable to place individuals, with a certain degree of probability, and hence with a certain induced error rate, in a particular category in order to take individual decisions relating to them. Taking the opportunity of the huge number of traces generated by the Internet users apart from their use of communications services and by the data collected just in time thanks to the technologies and coming from a large variety of sources, companies or administrations are defining profiles and apply these profiles to individuals in order to take decisions towards individuals identified or not. “Adaptive pricing” is often quoted in that context. According to the profile of the customer, the information service provider might decide to adapt the price of a service or a product. One to one marketing is largely based on that technique and more and more administrations are detecting presumed smugglers or terrorists using that method.

New actors: the intermediaries - Before discussing the implications of these applications as regards our fundamental liberties, we would like to underline the increasing role of **intermediaries.** By intermediaries, we mean all the activities which render useful the usage of the applications. It might be platforms offering the Web 2.0 services, search engines or all communications services providers as well as operators intervening in support of these communication services like certification providers. These persons play a decisive role by providing added value services but at the same time might be considered as gatekeepers to the information provided by or to internet’s users. They are ranking the information, facilitating the access to that information and in certain cases, selecting the information offered.

To what extent they might be held liable in case of diffusion of illicit or illegal messages by their platform? The question has recently been raised after the diffusion on You Tube of images provided by the future Finnish killer[32]. Two additional remarks: firstly, the economy of the functioning of these services is often quite obscure since they are using the information they collect for their own benefit or the benefit of a third party by developing marketing operations or other added value services; secondly, the law enforcement authorities might be tempted to cooperate with such services providers in order to find potential suspects in criminal affairs.

Privatization of cyberspace – By privatization of cyberspace we refer to a quadruple evolution present in cyberspace. The first one concerns the fact that more and more through technical means (Digital Rights Management systems, Tattooing[33], etc.) the information might become the “property” of their producers or authors by restricting the access to third parties or controlling their uses.

[31] R. Brownsword, ‘Knowing Me, Knowing You—Profiling, Privacy and the Public Interest’ in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen*, Dordrecht, Springer, 2008, pp. 362-382.

[32] The 18 year old Pekka-Erik Auvinen in November 2007, see for instance timesonline, "Finish "YouTube Killer" was bullied at school", 8 November 2007.

[33] Tattooing (or watermarking) is creating a permanent, indelible mark in the digital record, see Edward Barrow, "Rights clearance and technical protection in electronic environment", February 1996.

We will come back on that reality later (see point 2.2). The second point underlines the fact that entering into the cyberspace requires going through certain private gatekeepers who control the content and the access to the public space of information and discussion. The third point recognizes that technologies are blurring more and more the traditional distinction between public and private spaces. So, for instance, surfing the Internet from my home reveals outside of the four walls of my private domicile, my habits and my preferences better than if I were in the street or in public or professional spaces. Finally, it is quite clear that protocols' norms as well as terminals' ones which generate or regulate the data flows are no more fixed and regulated by public authorities but by private companies or standardisation bodies like IETF, W3C or ICANN[34].

3. Liberties and Information Society

How Democracy is at stake in our Information Societies? **-** Democracy is at the same time the condition for the autonomy of human individuals and conditioned by the effective exercise of this autonomy. Insofar as Privacy defined as self-determination is considered as ensuring our self development, it might appear as an intrinsic condition of our democracy and its vitality. Freedom of expression is the result of this free participation. It implies the right for everyone to be heard and to have access to pluralistic and diverse opinions.

3.1 Privacy and Information Society

What does privacy or self-determination mean?[35] **-** In 1983, the German Constitutional Court in the famous census case[36] has approached the privacy as the fundamental right to self-determination and have underlined, in a very prospective way, the risks incurred by our privacy in our modern Information Society. The Court said**:**

"*The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behavior by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about* actions *to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behavior is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behavior. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would have also impact the common good ("Gemeinwohl"), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate.*"

[34] IETF = Internet Engineering Task Force; W3C = World Wide Web Consortium; ICANN = Internet Corporation for Assigned Names and Numbers.

[35] On that topic, read A. Rouvroy- Y.Poullet, art cit.

[36] Constitutional Court, Dec. 15, 1983, EuGRZ, 1983,p ; 171 and ff.

The Court's assertions might be analyzed in three steps: first, the Court gives a broad definition of the right to privacy; second, it enumerates the new threats to privacy in our information society; finally, in the third step of its reasoning, the Court recognizes a clear link between privacy protection and democracy. What "self-determination" presupposes and what it allows in a given society (the "facets" of privacy) is unavoidably contingent on many evolving factors.

Besides the state of technological development − suggested by L. Lessig[37] as the central, if not exclusive, reason to adapt our normative instruments −, the nature of prevailing institutional arrangements and socio-political structures is a critical factor to take into account in order to explain the chronological development of the diverse and interdependent facets of the right to privacy. To summarize, **we argue that privacy, as a legal right, should be conceived essentially as an *instrument* for fostering the specific yet changing *autonomic capabilities* of individuals that are, in a given society at a given time, necessary for sustaining a vivid democracy.**[38] **The Court anchors the privacy and the data protection legislation directly in two ethical values which undoubtedly are of universal nature: the right to dignity and to self-development.**

***Privacy as a "fundamentally fundamental right"* -** Our capacities for both reflexive autonomy and deliberative ability to participate within the societal discussion are threatened in a unprecedented manner by the intensification of surveillance and monitoring technologies such as CCTV, data mining and profiling, RFID and the "internet of things", ubiquitous computing, and "ambient intelligence".[39] The German Court acknowledged that self-imposed restrictions on deviant behaviour, or on participation in an assembly or in a civil society initiative by fear that this behaviour and activities could be disclosed to others with adverse consequences ensuing put our democracies at risk since they hinder the free expression and the autonomy of the citizens, what is fully necessary in order to ensure a democratic discussion.

As expressed by Burkert[40], privacy may be considered a "*fundamentally fundamental right*". Privacy is not a freedom on the same rank with the others: essential to human dignity and individual autonomy, and translating these moral principles in the legal sphere, privacy is a necessary precondition to the enjoyment of most other fundamental rights and freedoms.

Privacy as a broad, twofold and evolving concept - The Court anchored their approach to the right to privacy in two distinct constitutional provisions reflecting the primacy, in the German constitutional order, of two fundamental values: human dignity on the one hand, and individual self development in a free society on the other hand. The combination of these values inspired the Court's acknowledgement that a "generic right to personhood" ("*An Allgemeine Persönlichkeitsrecht*"), existed as the core of the legal constitutional order of the German Republic.

[37] L. Lessig, Code and other Laws in Cyberspace, New York, Basic Books, 1999.

[38] See, in the same sense, R. Sunstein, *art. cit.,* p. 157.

[39] For further reflections on how the internet revolution and more recently the Ambient Intelligence technologies are metamorphosing the risks incurred by the individuals and their basic rights and call for new legislative actions reinforcing the different identified facets of the right to privacy, see Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence', *Studies in Law, Ethics and Technology (forthcoming).*

[40] H.Burkert, 'Dualities of Privacy -An Introduction to 'Personal Data Protection and Fundamental Rights'', *in Privacy- New visions,* M.V. Perez, A. Palazzi (eds), Cahier du Crid, to be published in 2008.

That right, transposed in the technological context of 1983, was to be understood as a right to informational self-determination that justified the adoption of the Data Protection Act. That anchorage of the right to data protection to human dignity and self-development must be underlined. **It implies that data protection legislation is definitively to be considered as a condition for ensuring the dignity of the person but in the same time it reveals that data protection legislation is not exhausting the right to dignity and that the privacy protection must be evaluated in certain cases directly by reference to this dignity principle**.

Chronologically, privacy has first been conceptualized as a right to 'seclusion' (opacity, or privacy as solitude) and, secondly, as individual informational control or empowerment ("the ability of an individual to control the terms under which his or her personal information is acquired and used", formalised through fair information practices).

The initial interpretation of the right to privacy as understood by the 1950 Council of Europe Convention on Human Rights had much in common with the American "right to be left alone", in the intimacy of one's private and family life, home and correspondence. The right to opacity means that each individual must have a physical place where to express him or her self and the possibility to exchange views or to reveal his intimate beliefs to others through private communications means without being observed from outside or by third parties.[41] This 'right to seclusion' (in other words, the right to not participate within the Information Society) might well be even more vital today in our modern society than ever before, justifying the new legal tools put into place in order to protect 'opacity' against the new technological and socio-political challenges of the day. **What characterizes the present Internet world is precisely the unprecedented possibility that we will be constantly surveyed through the multiple traces we leave in the cyberspace and through the gradual invasion of our private sphere by terminals of multiple and ubiquitous nature (from personal computers, GPS, mobile phones, RFID, etc.), dissolving the traditional distinction between public and private spaces**.

The other facet is precisely the right when we are participating to the Information Society to have a certain master ship on the data flows concerning ourselves.

It implies and explains the fundamental principles of data protection (fair processing, performed for specific purpose, on the basis of the subject's consent or of other legitimate basis laid down by law, subjective rights of the data subject to access and rectify collected data) have been formalized in the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe,[42] and restated in the fair information principles of the European directive on the protection of individuals with regard to the automatic processing of personal data[43] and in the European directive concerning the processing of personal data and the protection of privacy in the electronic communication sector.[44]

[41] About the history of the privacy concept, read notably D.J. Solove, "*Conceptualizing Privacy*", 90 *California Law Review*, 2002, 1085 and ff..

[42] Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe, ETS, N°108, Strasbourg, 28 January 1981.

[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23 November 1995.

[44] European Directive 2002/58/EC EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.

"*The ability of an individual to control the terms under which their personal information is acquired and used*"[45] is often presented as the hallmark of data protection.

New risks in our Information Society **-** The rationale behind the data protection regimes relates to the risks to individual self-determination carried by the early development of the information technologies infrastructures. The use of information technologies have been considered, from the beginning, as worsening power asymmetries between data subjects (the individuals whose data are processed) and the data controllers (in charge of the collection, storage, processing, use and dissemination of data). Technological developments gradually create a situation where:

> *'a) there is virtually no limit to the amount of information that can be recorded,*
>
> *b) there is virtually no limit to the scope of analysis that can be done-bounded only by human ingenuity, and*
>
> *c) the information may be stored virtually forever.'*[46]

These developments had of course direct impact on the autonomy of the data subjects: vast collection and intensive processing of data enable data controllers such as governmental authorities or private companies to take decision about the individual on the basis of this collected and processed personal information without allowing for any possibility for the data subject to know exactly which data would be used, for which purposes, for which duration and overall without control of the necessity of this processing as regards the purposes pursued by the public or private bureaucracies. Data Protection regimes were thus designed (and, in some countries, translated into self-regulatory measures) in order to better balance 'informational power'.

This resulted in a widening of the protection previously limited and centred on intimate and sensitive data, which now includes all personal data defined as "information about identified or identifiable individuals", and in the attribution of new rights to the data subjects, including an 'access right' allowing a better control over the uses and dissemination of personal data and, finally, the imposition of limitations to the permissible processing by data controllers, especially through the requirements that data processing will be fair, legitimate (another word for proportionate both as regards the existence of the processing and its content), and secure.[47]

The relationships between data controller (D.C) and data subjects (D.S) in our information Society between KAFKA and ORWELL worlds –"Towards an Observation Society"- In a recent book, Solove describes the evolution of the relationships in our Information Society using two paradigms drawn down from two novels: "The Trial" of KAFKA and the " 1984" or "BIG BROTHER" of Orwell. With the first, it denunciates the radical and increasing opacity of the data capture and data flows permitted by the increasing use of ICTs and their ubiquitous character. This opacity leads to a certain anticipatory conformism in the sense that data subjects adopt the behaviour they believe is expected by the data controllers.

[45] M.J. Culnan, « Protecting Privacy online: Is self-regulation working?, 19 *Journal of Public Policy Market,* 2000, 1, pp. 20 and ff.

[46] H. Nissenbaum, « Protecting Privacy in an Information Age: the Problem of Privacy in Public.Spaces, 17 *Law and Phil.,* 1998, pp. 576.

[47] Security is envisaged in its broadest sense, meaning integrity, confidentiality, accountability and availability.

The increasing asymmetry of informational powers is also due to the huge number of data, Data Controllers are collecting and processing which enables them to define profiles and to take the “appropriate” decisions on the basis of the data they are capturing about our behaviours, our movements, facial emotions, clicking habits: in other words on the basis of a lot of instantaneous slices of our lives we never expected they might be of a certain significance. One adds that Information systems might keep memory of all these events by storing that at long term. Information systems have a memory an individual has not.

This phenomenon comes together with the emergence of certain applications which are linked to the technologies of ubiquitous computing, inducing what we might call the “**Observation Society**” paradigm, Under this paradigm, the D.C. combines multimodal capture of data "extracted" from human bodies with an implicit understanding and interpretation of this data as valid and privileged source of "truth" about the persons, their preferences, intentions, etc., following the assumption that the ‘body does not lie’. Decisions are taken *a priori* on the basis of this data and profiles rather than on information by the data subjects. Since the Data subjects are not aware of this they are faced with decisions they are unable to understand and definitively to contest.

Do we need new legislation? – **Transparency and proportionality as two key principles -** Our privacy legislations are grounded on two main principles: transparency and proportionality. Undoubtedly, these two principles must be asserted again and in a certain extent enlarged.

i. So, we do consider that ***transparency*** should encompass in our information society the right to a mastered and transparent functioning of the terminals equipment including RFID or other sensors embedded in our daily environment. Our computers are functioning to a large extent without possibility for us to know exactly what they are exchanging, receiving and processing. **The transparency of the processing means also the right to be informed about the data flows generated and the D.C. involved in these networks (Who has access? For which purposes? …). As regards the profiling, special attention must be given to an access to their existence and logic. The possibility for refusing the profiling application and blocking certain automated data flows has to be granted to the individuals.**

ii. The ***proportionality*** principle has to be recalled at a moment where data capture is so easy and data processing capacities have grown to an unexpected level and that data even when they concern instantaneous slices of my life might be kept for an unlimited period. Economic efficiency including in the interest of the consumers or the citizens (see the e-government efficiency myth) and private or public security nowadays are presented as justifying the processing. We have to resist to the temptation that since data is getting easier to capture and to process, its use to promote efficient services making more rentable the activities of companies or ensuring a better public service or control of the respect of the public regulations must be *a priori* permitted.

A societal control measuring the impact of the ICT applications on the individuals’ autonomy is needed. That means that the balance between better efficiency and public interests has to be analysed extensively and from a social, psychological and ethical point of view too.

Proportionality and the debate between public security and privacy – Societal evaluation is crucial as regards applications developed by law enforcement agencies and intelligent services in the name of public security interests. Considering certain of these applications,

> “*one can safely assert that the mental privacy, the most intimate sphere, is being threatened, violating person’s most secluded dimension. After 9/11, “privacy in the age of terror” would appear to be doomed. Not only is privacy no longer regarded as a fundamental right; in fact, it is too often considered a hindrance to security, and overridden by emergency legislation*”[48].

The debate between security and privacy is too often presented as a conflict between two fundamental rights placed on the same footing; sometimes it is argued that the right to security is more fundamental than the right to privacy. Against this argument, we totally agree with the European Data Protection Supervisor when he asserts:

> *«a message such as: "No right to privacy until life and security are guaranteed" is developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford. […] the Home Secretary of the United Kingdom, Dr John Reid, called for human rights law to be rewritten, stating that "The right to security, to the protection of life and liberty, is and should be the basic right on which all others are based". […]This position could be potentially dangerous and may produce more problems than it seeks to solve... There should be no doubt that effective anti-terror measures can be framed within the boundaries of fundamental rights. It is these rights that need to be protected under all circumstances in a democratic society. In the past examples can be found in different parts of Europe where the failure to protect fundamental rights has served as source of continued unrest rather than ensure safety and stability ».*[49]

Need to reinforce Data Protection authority – Both the trend to evacuate more and more the proportionality judgment and the more and more opaque ICT environment have to be counterbalanced by granting more and more powers of investigation to DPA. The role of the DPA is definitively to ensure that the main principles of the Data Protection legislation are effectively respected and in case where a societal assessment is needed to create the possibility of a public debate and to stimulate it. **We are convinced that this debate due to the global character of the technology and their promoters has to be led at the European level, notably thanks to the Article 29 Working Party[50] by giving to this Group a real autonomy including financial, personal and managerial means.**

***Need to focus on terminal and information systems* – Our traditional data protection legislation is considering only the relationship between data controllers and data subjects.** Telecommunications protocols and the functioning of the terminals do not include data protection as a key requirement but as an option generally left to the discretion of manufacturers of the hardware and software that incorporates these standards.

The Article 29 Working Group has argued that the principle enacted by Recital 2 under the Data Protection Directive which clearly asserts that technology must be at the benefit of the individuals and the society, might be considered as a justification for imposing on manufacturers of terminal equipment (including software elements incorporated into the terminal) certain obligations aimed at the transparency of their operation and preventing the unfair or illicit use of personal data associated with the connecting to and communicating with the network.

[48] S. Rodota, “Data Protection as fundamental Right”, in *Reinventing Data Protection,* S. Gutwirth et alii, Springer Verlag, 2008 (to be published).

[49] CEPD, « Letters to the incoming presidency: fundamental rights are not captives of security”, 11 June 2007, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf.

[50] The Working Party was established by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (in short: the Data Protection Directive). Its tasks are laid down in Article 30 of Directive 95/46/EC and in article 15 of directive 2002/58/EC.

It should be noted that these manufacturers are not covered as such by the present directive since they are not controllers of a file. **However, as the design of the equipment influences many processing operations, certain security responsibilities should be imposed on them so as to prevent operations to be carried out in unfair or illicit manner by third parties, They should be required to ensure transparency since the user of the equipment must be able to exercise a certain amount of control over the data flows generated by their use.**

3.2 Freedom of Expression and Information Society

***Positive preliminary statement and from privacy to freedom of expression* -** The development of the Information Society increases the chances not only for individuals but also for communities to freely express opinions in cyberspace and receive information necessary for the exercise of their rights as citizens, as a community, as a state. Blogs, Web 2.0 services have recently contributed to the increase of that capacity for everybody to participate fully to the democratic discussion within the public space of the Internet. Traditionally, the Internet has been viewed as the ideal forum for individuals to express themselves and to enter into contact with others and have access to their expression. **The recognition of Privacy has to be considered as a preliminary requirement for the exercise of the freedom of expression.** Would I dare to sign a petition in favour of a worthy cause if I know that tomorrow a powerful search engine would offer a potential employer, the means to stigmatise me for my standpoint?

Two other preliminary conditions for the freedom of expression have to be underlined:

i. The first one refers to the ***right of each citizen to an education which renders him or her capable of expressing him or herself in cyberspace***. Definitively this first condition refers to the values of solidarity and social justice which justify the various components of the universal service. Universal service[51] means not only a non discriminatory and accessible access to an infrastructure of quality including the development of "public access points" like libraries, schools and administration but also the right to be educated how to use Internet services, what we call the "computer literacy". "Computer literacy" has to be understood broadly as asserted by the Council of Europe not only as the computational aspects of the use of internet services but overall as an critical and ethical education in the use of these new services by a better understanding of the societal impact of the Internet services.

This ethical education is even much more necessary given that with Web 2.0 applications, each of us might become tomorrow a publisher, an author and a data controller. **We plead for the spreading at all levels (at the levels of internet communities, ISPs and intermediaries) of ethical codes discussed as possible with the different stakeholders).**

ii. The second condition for the effectiveness of our freedom of speech relates to the ***ambiguous relationship between IPR and freedom of expression***. It is quite obvious that IPR regimes have been created for stimulating the creativity and for supporting the action of dissemination of ideas and opinions. By asserting that, we re-emphasize that copyright finds its ultimate justification in the freedom of expression recognized by Article 10 of the 1950 Council of Europe Convention.

[51] Please note that the author is referring to universal service as a generic term, and not to the concept of USO as defined in the regulatory framework.

> At the same time the copyright regime guarantees the possibility -in case of prevalent general public interest- to have access to the works and deny the possibility to transform the copyright into a "property right", through adequate technological measures (like Digital Rights Management Systems or tattooing) and ever-lasting contractual provisions.

These measures reinforced by their legal enactment[52] contribute to limit *a priori* the access to certain works including despite legal exceptions (DRM) or/and acknowledge the presence of the work in any of its fragment without any discussion about the subsistence of the conditions of the legal protection in all these fragments (Tattooing). They permit a reinforcement of the control of any reuse of each element of the work. And, in the same sense, the use of filtering and contractual provisions might be imposed without respect to the copyright regulation requirements. The chilling effect on creativity might be feared. **That is why we do recommend to analyze deeply the impact of all the new technical and contractual tools on the traditional balance enshrined in the copyright legislation. Furthermore, we do encourage states to provide an electronic universal access to economic, legal, social, cultural information held by the public sector like the Archives, the public libraries, the museums, etc. (as suggested by WSIS)[53].**

Network Neutrality: an emerging but crucial debate - The concept refers to a policy principle which implies a non discriminatory treatment as regards access to online content services. It means for networks' operators the prohibition of blocking or degrading, the submission to unreasonable and discriminatory conditions and even the prioritisation between the online services providers providing similar service.

This principle prohibits any control of the data flow and imposes an equal treatment to each data flow. It meets the initial so-called "Internet end-to-end principle" which was enacted for ensuring a maximum efficiency of the transmission to minimize the cost of the network and in case of insufficient network capacities to impose the "first-come, first-served" rule.

That rule creates problem while dealing with delay sensitive internet application such as notably Voice on the Internet services, streaming videos, etc..

[52] See on that issue, the Geneva Declaration on the future of WIPO: "*As an intergovernmental organization, however, WIPO embraced a culture of creating and expanding monopoly privileges, often without regard to consequences. The continuous expansion of these privileges and their enforcement mechanisms has led to grave social and economic costs, and has hampered and threatened other important systems of creativity and innovation. WIPO needs to enable its members to understand the real economic and social consequences of excessive intellectual property protections and the importance of striking a balance between the public domain and competition on the one hand and the realm of property rights on the other.* "

[53] This idea of a 'Public Domain Content' has been clearly promoted by the UNESCO. See, Point 15 of the 'Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace', adopted by the UNESCO General Conference at its 32nd session (Oct. 2003): '*Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation.*'

Engineers have developed technologies which permit apart from now "traffic prioritisation" and thus solve the "Quality of Service" (QoS) problem raised by these "time sensitive applications". At the same time, it introduces the possibility for a network operator to prioritise and shape traffic at the router level by automated recognition of the identities of the sender/receiver of a data flow and/or of its content. This can potentially lead to anticompetitive measures being taken by mobile or cable infrastructure operators such as blocking e.g. the VoIP[54] and peer to peer systems by giving priority to certain service providers affiliated to them. Beyond that, it introduces the possibility of a "two tier" Internet, an Internet with high performance and great capacities of transmission for certain information providers and/or rich customers and another one with degraded performance accessible to the others. **This possibility imposes certain legislative actions beyond the application of competition law in order to ensure the transparency of the usage and purposes of the technology of prioritisation and perhaps to ensure that all internet users are provided a minimum quality of services what implies a re-evaluation of the Universal Service[55].**

Minimal regulation for content **-** Freedom of expression, off line and online is a basic inalienable right of the citizens. If certain limitations are provided for by the text which enunciates these principles, we must resist to the temptation of regulating *a priori* the freedom of expression on the Internet. The temptation is great since certain recent events attempt the governments to justify interference by public authorities. The technology might help by creating solutions which were not possible in the offline world, notably by screening all messages in order to detect expressions or images considered as shocking, offending or disturbing. On that point, one have to recall the practice of the European Court of Human Rights (ECHR) which asserts that the democratic debate imposes the existence of a variety of opinions even if they might be considered as offending or disturbing people. We must learn to live with that risk and to concentrate our efforts only on certain precise regulations focussing on manifestly illicit (e.g. racism or pedo-pornography) or seriously harmful contents and trust the powers of freedom of expression reinforced by the Internet and its capacity to allow each citizen to react, discuss, and protest against certain practices or content. In our opinion, more speech might be the best way to solve the problem instead of developing filters, blocking measures or sanctions.

In that context, an 'open' and transparent self-regulation (versus the confiscation by certain intermediaries of this self-regulation) conceived as the participation of all stakeholders in the regulation of the content on the Internet is an appropriate way to maintain the Internet as a public discussion place and forum to acceptable limits. The next point is precisely dedicated to this issue.

The "Death of Public Forum in Cyberspace"[56] - The horizontal effect of the 1950' European Convention of Human Rights imposes that the same freedom of expression principle and its limits are available also towards the intermediaries like search engines and Web 2.0 platforms.

[54] As it was decided in the US Madison River and Comcast Corporation cases (about these case and more generally on the "Network neutrality" debate, read, P.Vaelcke, "Network Neutrality: legal Answers from a EU Perspective", *RDTI*, Sept.2008, p. 323 and ff.

[55] See the OECD report, « Internet Traffic Prioritization: An Overview », Note by TIPS, (2007), DSTI/ICCP/TIPS(2006).

[56] D. Nunziate, "The Death of the Public Forum in Cyberspace", *Berkeley Technology Law Journal,* 2005, p. 1115 and ff.

Since they are becoming the private gatekeepers of the public discussion space, it is important that their policies as regards the control of the Internet content would be clear and transparent to the public. Until now, these policies are quite unclear. The fear of an "over-censorship" by these private authorities calls for a control over their practice. Otherwise, as stated by Nunziate, the Internet will become transformed by this privatization of the public space "*into a collection of* largely *privately owned and privately regulated places"* without judiciary control. My opinion is that the countries have a positive duty to impose the respect of the freedom of expression to all actors and to recreate public places (i.e. public forums in cyberspace).

That assertion does not contradict with the self-regulatory or co-regulatory measures like quality labels, moderators' intervention, rating systems, put into place by communities or information providers services themselves. These initiatives might be interesting to promote the confidence and awareness of the ethical aspects of what must be our behaviour on the Internet. As already said, instead of punishing and sanctioning, it would be better to achieve the same goal by education and through codes of ethics discussed or clearly accepted and by developing ways and tools for Internet users and Information services providers to internalize norms and values.

***New editors, new journalists* -** With the new world of Internet, the concept of press has to be reassessed. Not only because the actors are no more linked to specific countries but are active throughout the world or a large part of the world but also because everywhere new actors are now contributing to the formation of the public opinion without having all the elements of the definition. For instance, can we consider that Google News with selecting press articles has to be qualified as a press institution? You Tube is diffusing opinions, records about what has happened around the world but its activity might not easily be considered as the one of an editor even if there is a certain selection of information and images and definitively a classification of them. The traditional press sector develops also new services online such as forums of discussion and journalist's blogs which sometimes are clearly outside the control of the editorial board.

The role of search engine has to be assessed in the same context. To what extent is democracy concerned by their activities? Even if we certainly agree that search engines provide a major input to the democratic debate thanks to the possibility given to everyone to retrieve and access, from any country - including not only developed countries - all adequate information on a topic, we, nevertheless, would like to put into question this progress. The equity of chance to exist and to be consulted on the WEB scene is far from being obvious when we do consider the "link popularity" metric applied in most of the engines. The lack of transparency thus is the major issue raised in this context. Most of the users do ignore how the ranking is done and often consider it as the true response and vision of the world of their queries.

Even if it is normal that the logics governing the functioning of the search engine are greatly dictated by economic and efficiency concerns, it remains that the method of selection has to be clear to everybody and might not be operated in an unfair way for ideological, anticompetitive or other reasons.

As regards the actors implied in Web 2.0 services, everybody might become journalist, commenting through his or her blog the day to day events and his or her website can have a strong audience comparable to that of the newspapers.

The concept of a journalist is not defined but it is commonly considered that his or her activity is to disseminate through the editors his or her independent opinion on events which are of public importance and due to their important contribution to the formation of the public opinion, are submitted to a deontology which ensures the public's confidence (duty to check the sources, duty to limit him or herself to the information published to what is needed for the formation of the public opinion, etc.). The respect of these obligations is, ensured by self-regulatory rules and organized by the peers themselves. To what extent this deontology might be applicable to citizens publishing their own opinions normally directed to a restricted public?

How to ensure the cultural diversity in a global environment? - Having asserted the absolute priority of the freedom of expression, EU has to recognize that certain values might be considered in a certain country differently than in the EU for religious, cultural or societal reasons. Nudity is accepted in some countries but is rejected and considered a threat to public morality in other. The French Yahoo case[57] concerning racist content illustrates the difference of approaches between US and EU as regards the prohibition of this kind of content. The adoption in 2005 of the UNESCO Convention on the diversity of cultural expression[58] is a clear recognition of this plurality of national perceptions of public order and moral. The abolition of physical frontiers in the context of the Internet might create difficulties for the countries to enforce in the context of the Internet their own perceptions of what might remain an attribute of their national sovereignty. This sovereignty is however recognized even by WTO Conventions since article XIV a) of the GATS permits a country to go against their market access commitments if taking measures is "necessary to protect public morals or to maintain public order". The conciliation of public national sovereignty on one hand and of the global character of the Internet on the other hand is not easy to solve. On basis of the famous ANTIGUA vs. US case[59] about online gambling services, Rundle[60] observes that this kind of debate might not be correctly solved in the context of WTO, only on the basis of a balance between trade interests and public interests.

Another solution must be found at the international level in order to conciliate the freedom of expression principle and the right of each sovereign State to limit this fundamental liberty for prevalent public or general interest reasons.

Perhaps an International Court of Justice created under the auspices of the UNESCO might be the appropriate solution. It implies the necessity that the infrastructure design gives the possibility for each nation to enforce the decision taken which might be difficult if the Internet configuration does not permit this enforcement.

That refers to the delicate problem of the State sovereignty on the Net, a question we will address in our final statements.

[57] The first Court decision has been pronounced in 2000 by the Tribunal de Grande Instance de Paris, (decision available at:http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm with a lot of comments). This decision has been followed by numerous decisions in contradictory senses both in US and in France.

[58] Convention on protection and promotion of the diversity of cultural expression, adopted by the UNESCO General Assembly, Paris, 20 October 2005.

[59] WTO, Appellate Body Report, Measures Affecting the Cross-Border Supplies of Gambling and Betting Services, WT/DS285/AB/R, 7 April 2005, see www.**wto**.org/english/tratop_e/dispu_e/285arb_13_e.doc. On that issue, read, M.V. Perez Asinari, "Internet Gambling and betting services: When the GATS' rules are not applied due to morals/public order exception. What lessons can be learnt?, CL&SR, 2006, 1 and ff.

[60] M. Rundle, "Beyond Internet Governance: the emerging International Framework for Governing the Networked World", Research Publication N° 2005-16, Fall 2005, http://cyber.law.harvard.edu/publications.

4. FINAL STATEMENTS

4.1 ICT challenging or enhancing liberties? Towards a value sensitive design of the technologies

Technology is the risk, it might also be the solution **-** ICTs are a tool, more precisely a "social construct" since their design and use are not predetermined but contains enshrined logic and pursued by their users. If technology certainly offers to them new opportunities and means to realize their goals, it is quite obvious that choices are still possible. We should never forget that if technology creates the risk in the same time it might bring solutions. In short, the technology can make a contribution to humanity just as it can put in peril the liberties of citizens. As already quoted, the Article 29 Working Party on Data Protection and RFID noted, under the basis of the Data Protection Directive preamble: "*Technology must be at the service of the human being, his or her freedom and dignity*".

It implies that from a very early stage, the research laboratories, the information system producers and the public or private standardization bodies have to take into account these concerns and follow a "human values sensitive design". That means an enhanced integration of 'moral and legal values' from the very starting stage of technological design. In order to ensure this integration a societal assessment should be initiated both at the level of research laboratories and definitively at the level of standardisation bodies'. It presupposes that computer scientists would be more aware of the legal and societal environment and impact of their findings and that public discussion might be organized at different levels. **Correlatively, Terminal equipments' producers and Information Systems designers will have to support liability in cases where their products or services permit their users to infringe Human Rights legislation.** In conclusion, it is at the roots of the Technology where we should find the solutions to the risks created by the use of that Technology.

4.2 Crucial role of the state

The role of the state in enforcing human liberties **-** According to the jurisprudence of the ECHR the state is not merely under the obligation to abstain from interfering with individuals' privacy, but also to provide individuals with the material conditions needed to allow them to effectively implement their right to private and family life.[61]

In other words, according to the theories of the "positive duties" of the state combined with that of the "horizontal effect" of the EHCR, states are under the obligation to take all appropriate measures to protect the fundamental rights of the individuals including against their infringement by other non-state parties.

[61] The positive duty of the State to provide the means necessary in order to allow effective enjoyment of rights is not as such recognised in the United States, neither by the law, nor by the jurisprudence.

Our duty as European states is not limited to the defence of the fundamental liberties within the European Union but also implies a commitment to ensure that this protection will be ensured at a global level. As regards Privacy protection, the Council of Europe Convention N°108[62] might be considered as the necessary global privacy regulatory framework since it is opened to signature by third countries and is offering a minimal common and acceptable basis for all countries.

The need for a global dialog founded on certain basic ethical values **-** Zoning the Net[63] according to citizenship might seem at first glance a sensible way to maintain the modern world's citizenship lines. However, such a practice will encounter problems, not the least of which will be citizens' dissatisfaction with differential treatment based on nationality. As in other areas of governance, a global approach is needed. It requires that each country seriously takes into account the various cultural approaches existing throughout the world, the refusal to impose on the others nations a unilateral view as regards the public order. **A regulatory framework based on human Rights implies a commitment to enter into a dialog founded on a mutual recognition of the cultural differences and on some ethical common values revealed in international documents (especially the UNESCO Convention on protection and promotion of the diversity of cultural expression and the UNESCO Declaration on Bioethics and Human Rights[64]) and universally accepted. These common values could be enumerated as follows: 1) person's dignity and autonomy; 2) solidarity between men and peoples and social justices; 3) need for beneficent technologies and prevention of their damaging effects**.

If this dialog does not happen, one might fear that the internet will become a Tower of Babel where fear and hate of the others' speech will be the sad result and will have as a result the loss of this unique and unedited chance of cultural, intellectual, political and human enrichment of the global society.

The need for a societal assessment - Beyond that, it is the role of the state and thus of Your Parliament to require as it has been recommended by the Commission on the particular case of RFID[65] that **societal assessment should be initiated with the participation of all stakeholders, empowering what we might call the "ordinary" voices, such as representatives of all groups of society in particular the vulnerable ones, but also civil liberties associations, trade union representatives or consumer groups. Perhaps a permanent working group, a sort of observatory, has to be set up at least at European level. Its role would be multiple: to give advice and recommendations to the European Institutions at their demand or on its own initiative, collect information and disseminate good practices, organize the public debate about the technological evolution and their societal impact.**

[62] Council of Europe Convention of the protection of individuals with regards to the automatic processing of personal data N°108.

[63] On the possible temptation of certain States to come back to a zoning of the Net, through the technical design of the infrastructure and definitively through the intervention of intermediaries like Internet access providers or payment systems , read J. Reidenberg, "States and Internet Enforcement, 1 *Univ. of Ottawa Law and Techn. Journal,* Vol. 1, N° 213, 2004.

[64] Adopted by acclamation on October 2005 by the 33rd session of the General Conference of UNESCO.

[65] See Commission Communication of March 15, 2007 on 'radio frequency identification (RFID) in Europe': Steps towards a policy framework', COM(2007)96 and the Study commissioned by the European Parliament, STOA on 'RFID and identity management in everyday life, June 2007.

The application of the precautionary principle, that implies the duty of the society to impose a certain assessment before to decide the exploitation of an innovation, as well as the shared responsibility of the producers of technology given the risks created, principles clearly asserted in the environmental law, has to be applied as regards the ICT technology. The principles of transparency and deliberation ("multi-stakeholderism") affirmed notably by the Aarhus Convention[66], will henceforth find an echo. This will enhance the active role of the citizens and their participation on the Internet.

The role of citizens: from adrift to active participation – In its UNESCO report on the Network Governance, Rundle speaks about the citizen's adrift[67] as the major problem of the future Information Society. Technological evolution is far beyond their ability to understand. Definitively that evolution brings many advantages and might lead to a new democracy where everybody might learn from the others, confront his or her ideas and therefore might participate more actively to the "vouloir vivre ensemble". But in order to be realised, this promise presupposes that citizens should be seen not as simple consumers of services, manipulated to an extent never reached. For ensuring this citizens' master ship of the technological environment, privacy regulation aiming to ensure the preservation of the autonomy of the individuals is definitively the main concern.

That recognition and even - as already proposed - enhancement of our privacy regulation is not sufficient. The public voice must be heard. It refers not only to the societal debates which have to be organised at all levels including at the global level h but also to the free debates the citizens must open and promote by discussing all the possibilities offered by the technology. We underline the importance of the citizens' networks supported or not by civil associations in order to defend alternative ways to develop the Internet. "Creative Commons", "Open Net movements"[68] are examples but many others examples developed by "peers to peers" networks might be quoted in the context of the use of Internet services, taking fully into account the benefits of the technological tools at their disposal.

In order to promote participation, citizens' education is a major issue, particularly as regards their awareness of the ethical issues and of the liability implied by their participation in the Information Society.

[66] The UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, usually known as the Aarhus Convention, was signed on June 25, 1998 in the Danish city of Aarhus. It entered into force on 30 October 2001.

[67] "*As the above account tells, governments have responded quickly to meet challenges in cyberspace: They have set certain parameters for people's online dealings. They have kept the doors open for e-commerce. They have let an international trade court review national rules on Net content. They have pooled resources for infrastructure development. They have set up cybersecurity arrangements. They have even cooperated to safeguard the financial stability of the networked world. However, in letting the framework for Net governance evolve in an ad hoc way, policymakers have focused on surface problems, at the expense of deeper, more fundamental questions of democracy. Sooner or later, the networked world must confront an issue facing all societies: that is, the relationship between the state and its citizens. »* (M. Rundle, "Beyond Internet Governance: The Emerging International Framework for Governing the Networked World", Center for Internet and Society at Stanford Law School, Research Publication No. 2005-16,Fall 2005).

[68] The **OpenNet Initiative** is a joint project whose goal is to monitor and report on internet filtering and surveillance practices by nations. The project employs a number of technical means, as well as an international network of investigators, to determine the extent and nature of government-run internet filtering programs. Participating academic institutions include the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet & Society at Harvard Law School; the Oxford Internet Institute (OII) at University of Oxford and the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge, (Wikipedia Encyclopedia).

That education is definitively needed at a moment where we are full actors on the Internet through the web 2.0 services. Internet increases tenfold the power of individuals who in a targeted or a dispersed way, in a conscious or unconscious manner, can with a simple message posted on the Internet destroy the reputation of the others, transmit a virus, send or receive pedo-pornographic contents and thus encouraging the enslavement of human beings. The Internet gives to our actions without a particular effort on our part a "global impact" which prompts us to question individual and collective responsibility. Perhaps this individual and collective commitment to play a critical and active role in the design and choices of our Information society constitutes a chance for our democracies.

BIBLIOGRAPHY

Barrow, E (1996) Barrow, E (1996) "Rights clearance and technical protection in electronic environment", February 1996.

Brownsword R. (2008) Brownsword, R., 'Knowing Me, Knowing You—Profiling, Privacy and the Public Interest' in M. Hildebrandt and S. Gutwirth (eds), Profiling the European Citizen, Dordrecht, Springer, 2008, pp. 362-382.

Burkert H. (2008) Burkert, H., "Dualities of Privacy -An Introduction to 'Personal Data Protection and Fundamental Rights'', *in Privacy- New visions,* M.V. Perez, A. Palazzi (eds), Cahier du Crid, to be published in 2008.

Council of Europe Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe, ETS, N°108, Strasbourg, 28 January 1981.

Culnan M.J. (2000) Culnan, M.J., "Protecting Privacy online: Is self-regulation working?", 19 *Journal of Public Policy Market,* 2000, 1, pp. 20 and ff.

Council of Europe 1950 Convention on Human Rights Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, Rome, 4.XI.1950, ETS No 005 and protocol ETS No. 155.

Council of Europe Convention N°108 Council of Europe Convention of the protection of individuals with regards to the automatic processing of personal data N°108, ETS N°108.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23 November 1995.

Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.

ETAG European Technology Assessment Group, Study commissioned by STOA for the European Parliament on "RFID and identity management in everyday life", June 2007.

European Commission Communication of March 15, 2007 on 'radio frequency identification (RFID) in Europe': Steps towards a policy framework', COM(2007)96

Geneva Declaration Declaration on the future of WIPO http://www.cptech.org/ip/wipo/futureofwipodeclaration.pdf

Hustinx, Peter Data Protection Supervisor, letter to Minister of Justice Alberto Costa and Minister of State and Internal Administration Antonio Costa, "Presidency work programme and the protection of individuals with regards to the processing of personal data and the free movement of such data", 11 June 2007, see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf

Lessig L. (1999) Lessig, L., "Code and other Laws in Cyberspac", New York, Basic Books, 1999.

Nissenbaum H. (1998) Nissembaum, H., "Protecting Privacy in an Information Age: the Problem of Privacy in Public.Spaces", 17 *Law and Phil.,* 1998, pp. 576.

Nunziate D. (2005) Nunziate, D., "The Death of the Public Forum in Cyberspace", *Berkeley Technology Law Journal,* 2005, p. 1115 and ff.

OECD report (2007), "Internet Traffic Prioritization: An Overview ", Note by TIPS, (2007), DSTI/ICCP/TIPS(2006).

Perez Asinari MV. (2006) Perez Asinari, M.V., "Internet Gambling and betting services: When the GATS' rules are not applied due to morals/public order exception. What lessons can be learnt?, CL&SR, 2006, 1 and ff.

Reidenberg J. (2004) Reidenberg, J., "States and Internet Enforcement, 1 Univ. of Ottawa Law and Techn. Journal, Vol. 1, n° 213, 2004.

Rodota S. (2008) Rodota, S., "Data Protection as fundamental Right", in *Reinventing Data Protection*, S. Gutwirth et alii, Springer Verlag, 2008 (to be published)

Rundle M. (2005) Rundle, M., "Beyond Internet Governance: the emerging International Framework for Governing the Networked World", Research Publication n°2005-16, Fall 2005 available at: http://cyber.law.harvard.edu/publications.

Rouvroy A. et al (2007) Rouvroy, A., and Poullet, Y., "Introductory Remarks, General report, European Conference on Ethics and human rights in a Information Society organized by UNESCO and Council of Europe", Strasbourg, 13-14 Sept., 2007 available at the UNESCO website.

Rouvroy A. et al (2008) Rouvroy, A., Poullet, Y., The right to informational self-determination and the value of self-development - Reassessing the importance of privacy for democracy, in Reinventing Data Protection Gutwirth, S., Poullet, Y, De Hert, P., de Terwangne, C., Koops, B.J., (ed.), Springer Verlag, 2008, to be published.

Rouvroy A. (X) Rouvroy, A., "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", Studies in Law, Ethics and Technology (forthcoming).

Sunstein R. (2003) Sunstein, R., *Why Societies Need Dissent*, Harvard University Press, 2003, pp. 157-158.

Solove D.J. (2002) Solove, D.J., "Conceptualizing Privacy", 90 California Law Review, 2002, 1085 and ff.

UNECE Convention (Aarhus Convention) The UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, signed on June 25, 1998, Aarhus. Entered into force on 30 October 2001.

UNESCO Convention UNESCO Convention on protection and promotion of the diversity of cultural expression, adopted by the UNESCO General Assembly, Paris, 20 October 2005.

UNESCO Declaration Declaration on Bioethics and Human Rights, Adopted by acclamation on October 2005 by the 33rd session of the General Conference of UNESCO.

UNESCO Recom. "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace', adopted by the UNESCO General Conference at its 32nd session (Oct. 2003).

Vaelcke P. (2008) Vaelcke, P., "Network Neutrality: legal Answers from a EU Perspective", RDTI, Sept.2008, p. 323 and ff.

WTO WTO, Appelate Body Report, Measures Affecting the Cross-Border Supplies of Gambling and Betting Services, WT/DS285/AB/R, 7 April 2005.