



12th Informal ASEM Seminar on Human Rights

*“Human Rights and
Information and Communication Technology”*

27-29 June 2012
Seoul, Republic of Korea

Background Paper

Dr. Wolfgang Benedek
Dr. Madanmohan Rao



ASEM's contribution is with the financial support
of the European Union

Main Rapporteurs

Dr. Wolfgang Benedek

Wolfgang Benedek is Director of the Institute of International Law and International Relations of the University of Graz, Austria and of the European Training and Research Centre for Human Rights and Democracy of the University of Graz (UNI-ETC); Since 2003 he has coordinated several research projects in the field of Internet Governance and the role of human rights in the information society which have resulted in two books, i.e. Benedek/Pekari (ed.), *Menschenrechte in der Informationsgesellschaft* (2007) and Benedek/Bauer/Kettemann (ed.), *Internet Governance and the Information Society* (2008) and several other publications.

He is also editor of the Manual on Human Rights Education “Understanding Human Rights”, available in 15 languages including Thai, Chinese and Japanese and acting co-editor of European Yearbook on Human Rights. He is involved in internet literacy of school teachers and internet education at university level. He has participated in nearly all meetings of the Internet Governance Forum since 2006. Recently, he was leading the elaboration of the so-called Charter of Human Rights and Principles for the Internet, elaborated in the framework of the Dynamic Coalition of Human Rights and Principles for the Internet of the IGF. He has been invited to speak at numerous events like the seminar on Freedom of Expression organized by the Swedish Ministry for Foreign Affairs in Stockholm in March 2011 and at two conferences of the Council of Europe on the Information Society in April 2011 in Strasbourg and in December 2011 in Vienna.

Support has been provided by Mr. Matthias C. Kettemann, Research and Teaching Fellow, Institute of International Law and International Relations, University of Graz.

Dr. Madanmohan Rao

Dr. Madanmohan Rao, an author and consultant from Bangalore, is research advisor at the Asian Media Information and Communication Centre (AMIC). He is the editor of five book series: “The Asia Pacific Internet Handbook”, “The Knowledge Management Chronicles,” “AfricaDotEdu,” “World of Proverbs,” and “The Global Citizen.” He is the research project director of Mobile Monday, a global network of mobile and wireless communication professionals, and co-founder of the Bangalore K-Community, a network of knowledge management professionals.

Madan is also the founder of the Indian Proverbs Project, co-founder of the Singapore Proverbs Project, and world music & jazz editor at Jazzuality and World Music Central. He was formerly the communications director at the United Nations Inter Press Service bureau in New York, and vice president at IndiaWorld Communications in Bombay. He graduated from the Indian Institute of Technology at Bombay and the University of Massachusetts at Amherst, with an M.S. in computer science and a Ph.D. in communications. Madan is a frequent speaker on the international conference circuit, and has given talks and lectures in over 75 countries around the world. He is also adjunct faculty at the International School of Information Management. Madan can be followed on Twitter at <http://twitter.com/MadanRao>

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of the rapporteurs and can under no circumstances be regarded as reflecting the position of the European Union.

The views expressed in this document are the sole responsibility of the main rapporteurs and can under no circumstances be regarded as reflecting the views or opinions of the organisers of the 12th Informal ASEM Seminar on Human Rights, namely the Asia-Europe Foundation, the Raoul Wallenberg Institute, the French Ministry of Foreign Affairs, the Philippine Department of Foreign Affairs, the Korean Ministry of Foreign Affairs and Trade and the National Human Rights Commission of Korea.

“Human Rights and Information and Communication Technology”

27-29 June 2012, Seoul, Republic of Korea

Background Paper*

by Wolfgang Benedek and Madanmohan Rao

Table of Contents

- I. Main Developments in Building the Information Society on the Global and Regional Level
- II. Governance of the Internet
- III. Examples of Good Policies/Practices
- IV. ICT/Human Rights Issues for Working Groups
- V. General Conclusions, New Questions and Future Challenges

I. Main Developments in Building the Information Society on the Global and Regional Level

Evolution of ICTs and Human Rights

A core part of human rights is about communication and information, and a range of media theories address the connection between information, communication, news media and their political impacts. There are three great mediamorphoses in human communication: spoken language, written language, and the digital language.¹ Spoken language led to social group formation, complex problem solving skills, and the development of "broadcast" forms like storytelling and ritual performance - which in turn divided society into performers, gatekeepers, and audiences. Written language ushered in the development of portable documents, mechanical printing, and mass media.

Early long-distance communication systems were based on postal and courier networks, and the corresponding concern by civil society was over the ability of governments to censor and prevent the transfer of mail. This was followed by the growth of telegraphy, telephony and radio, each of

* *The examples mentioned in the background report, be it countries or private companies, are not there to criticize one or another but to illustrate the different topics and difficulties any society is facing with ICT.

¹ Fidler, Roger (1997). Mediamorphosis: Understanding New Media. California: Pine Forge Press.

which evolved along different trajectories with respect to universality and communication rights in the international context.²

The rise of trans-national telecommunications networks led to international standards bodies formed around the deployment of postal services, telegraphy, telephony and radio to resolve conflicts that they raised. It was in this context that the notions of universal service and freedom of transit for communications began to emerge.

The Universal Postal Union (UPU) was established in 1874 and helped shape concepts such as freedom of transit in the transfer of mail through third countries. The International Telegraph Union was founded in 1865, and universality was a stated goal from the outset. The ITU Convention of 1865 articulated support for the availability of telecommunication services for all citizens (which was updated with the invention of the telephone in 1876).

Universality in this context was probably concerned more with practical matters such as interoperability, than with moral and ethical considerations. Radio was invented in 1895, followed by the formation of the International Radio-Telegraph Union (IRU) which addressed issues of spectrum allocation and non-interference. Radio was the first ICT to bring a broad range of citizens into its fold, and evolved into a public discourse medium.³

In 1934, the International Telegraph Union and the International Radio-Telegraph Union merged to form the International Telecommunications Union (ITU). In 1925, the U.S. Communications Act mandated universal service for telephony in the US. The development of the United Nations and its Universal Declaration of Human Rights in the aftermath of World War II added a human rights context to these technological and regulatory developments.

Another branch of human rights arose in the nineteenth century in response to the consequences of the industrial revolution: economic, social, and cultural rights including the right to education, housing, health, employment, adequate income, and social security.⁴ Both these branches of human rights have converged into modern-day concepts of rights and privileges.

Radio and television share several characteristics that have made them especially important in a communication rights context (as compared to print media): use of their output is not dependent on literacy; they enable the broadcasting of information over large geographical areas; content creation barriers are high but access costs are lower. The Internet has changed this dynamic by reducing the costs of content creation, and making the reach of communications more global, instant and archived. Mobility has added the “anytime anywhere any-device” dimension to the online ecosystem.

The de-colonisation of much of Asia and Africa in the mid-twentieth century added new dimensions of discourse such as neo-imperial dominance of news flows by developed countries, taken up by organisations such as the Non-Aligned Movement and calls for a New World Information and Communication Order.

Satellite broadcasting and the backdrop of the Cold War ushered in new forms of political communication and debates over rights and responsibilities of media, between individual and collectivist rights to information and broadcasting; UN agencies such as UNESCO became the frontline for such forums and advocacy. The issue of human rights also became politicised in the

² McIver, William and Birdsall, William (2002). Technological Evolution and the Right to Communicate: The Implications for Electronic Democracy. 2002 Euricom Colloquium: Electronic Networks & Democracy, Nijmegen, The Netherlands.

³ McIver and Birdsall, *ibid*.

⁴ McIver and Birdsall, *ibid*.

international arena, with Western powers being accused of double standards and selective application (which carries on this day in regions like the Middle East).

In relatively rapid succession, cable technology, the Internet and mobile phones added new dimensions to the definitions of information access rights in the late 20th century, and we are now witnessing a convergence between multiple theories of media, telecommunications and digital information society. Interactive media are re-shaping information industries and social formations in successive waves:⁵ teletext, proprietary commercial online services (eg. Prodigy, CompuServe, AOL NiftyServe), text-only email and BBSs (eg. PeaceNet, FidoNet, BitNet), full-fledged multimedia open standards platforms (World Wide Web), and wireless data (mobile networks, WiFi hotspots).

“The Internet was born at the unlikely intersection of big science, military research, and libertarian culture. The Internet did not originate in the business world. It was too daring a technology, too expensive a project, and too risky an initiative to be assumed by profit-oriented organisations”, according to Manuel Castells.⁶

“Technological systems are socially produced. The Internet is, above all else, a cultural creation. The Internet culture today is characterised by a four-layer structure: the techno-meritocratic culture, the hacker culture, the virtual communitarian culture, and the entrepreneurial culture”, adds Castells. These sets of cultures have spurred the open source movement, the gift economy, cyberpolitics, virtual communities, and new venture capitalists.

Mass media theories of information flow and access are based on the gatekeeper model of information control, agenda setting power of the mass media, and structural flows of international content. Telecom theories of information flow are based on penetration (reach and richness) of interactive communication services and the exponential value of such networks depending on their relative user bases. Political theories of communication are based on power dynamics in message flows, political economy of the media, and impacts of message framing. The activities of human rights supporters of the Internet draw on all these theories; for instance, during the Arab Spring, the Internet and mobile phones had a critical mass of users who helped side-step government-controlled mass media, and the instant interactivity of people-to-people messaging helped with the organisation of protests which eventually toppled authoritarian governments.

Digital Media: A Diversity of Challenges, Opportunities and Threats

Frederick⁷ argues that internationally-linked computer networks can vastly transform the capacity of global civil society – the international community of organisations and individuals outside of direct control by governments and corporations⁸ – to build coalitions and organise around issues of human rights, the environment, and social justice. Such networking organisations can thus function in a manner similar to Althusser's ideological state apparatuses⁹, or institutions which perpetuate and reinforce ideology in social formations.

⁵ Rao, Madanmohan (2003). *News Media and New Media: The Asia-Pacific Internet Handbook*. Singapore: Eastern Universities Press.

⁶ Castells, Manuel (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press.

⁷ Frederick, Howard (1993). *Global Communications and International Relations*. Belmont, California: Wadsworth Publishing Company.

⁸ Hamelink, Cees (1990). *Information Imbalance: Core and Periphery*. In: *Questioning the Media: A Critical Introduction*, by Downing, John; Mohammadi, Ali and Sreberny-Mohammadi, Annabelle (eds.). Newbury Park, California: Sage.

⁹ For more details, please see Althusser (1970), *Ideology and Ideological State Apparatuses*, In: *Lenin and Philosophy and Other Essays*, Monthly Review Press.

Computer-mediated communication systems constitute an entirely new form of media called "collaborative mass media" which mixes elements of one-to-many information flow and many-to-many cooperative dialogue.¹⁰

The Internet and mobile phones open up a new range of opportunities, challenges and learning curves for society, ranging from information access and interpretation to creation and curation. A SWOT approach for such analysis in the context of human rights is depicted in Table 1.

Table 1: Challenges and Opportunities of the Internet in a Human Rights Context

	Opportunities	Challenges	The learning curve: Responses
Users (consumers, citizens)	1. Increased depth, breadth of news and information window 2. Increased interactivity, community participation, sidestepping of government control 3. Any time, any where, any device access	1. Information explosion 2. Scams, fake stories 3. Invasion of privacy	1. Tools, methodologies for managing information 2. Cultivating trust, researching news sources 3. Inspect online privacy policies before divulging personal information to news sites
Creators	1. Re-purposing content for multiple media 2. New narrative structuring (eg. layered stories, blogs) 3. Unprecedented access to research, experts	1. Information explosion 2. Loss of a sense of context, control over pace of industry 3. New legal risks (plagiarism, uncertainties over liability)	1. Tools, methodologies for managing information 2. Rigorous fact checking; advocacy in peer/industry associations 3. Sensitisation to cyberlaw issues
Curators	1. Meeting needs of different citizens 2. Extending shelf-life of editorial products 3. New forms of workflow	1. Dealing with convergence 2. Evolving standards for structuring content 3. New legal risks (eg. deep linking)	1. Co-location of different teams, roles 2. Joining consortia (eg. for XML) 3. Legal counsel, signing formal linking agreements
Commercial	1. Multiple targeting	1. Ad fatigue among	1. Evolve new formats of

¹⁰ Rafaeli, Sheizaf and LaRose, Robert (1993). Electronic Bulletin Boards and "Public Goods" Explanations of Collaborative Mass Media. Communication Research, Vol. 20, No. 2, April 1993.

players	<p>options: Web, email, SMS</p> <p>2. Demographic profiling</p> <p>3. Permission marketing</p>	<p>users</p> <p>2. Concerns over commercial censorship</p> <p>3. Inconsistent metrics</p>	<p>Web/email/search/social advertising</p> <p>2. Join industry consortia for interactive standards</p> <p>3. Seek independent third-party traffic audits, respect consumer and citizen rights to privacy</p>
Alternative media, human rights activists	<p>1. Means of bypassing traditional gatekeepers</p> <p>2. Networking with communities of interest globally</p> <p>3. Scope for mobilisation, advocacy, fund-raising online</p>	<p>1. High cost of ICT infrastructure, access</p> <p>2. Lack of ICT-aware human resources</p> <p>3. Censorship by authoritarian governments</p>	<p>1. Community networks, freeware, open source tools</p> <p>2. Capacity building workshops, funds from donor agencies</p> <p>3. Use of “anonymous” proxies, mirror sites, encryption, mesh networks</p>
Educators, academics, researchers	<p>1. New areas of research</p> <p>2. New forums, resources for collaborating with peers</p> <p>3. e-Learning platforms for delivering courses</p>	<p>1. Rapid pace of change, fear of obsolescence</p> <p>2. Inadequate resources for digital labs</p> <p>3. Lack of cooperation from industry</p>	<p>1. Leverage Web as a learning resource</p> <p>2. Seek partnerships with industry for resources, internships</p> <p>3. Conduct joint studies, create centres of excellence</p>
Government, national policymakers	<p>1. Online dissemination of government content for media, businesses, citizens</p> <p>2. Interactive, transactive e-government services</p> <p>3. Regulation, initiatives promoting local language content</p>	<p>1. Updating existing regulations for convergent media space</p> <p>2. Updating and enforcing laws regarding copyright, cybercrime, freedom of speech, surveillance</p> <p>3. Harmonising standards for local languages</p>	<p>1. Set up ICT ministries, merge existing print/broadcast/telecom ministries</p> <p>2. Lobby in existing international fora (eg. WIPO, ITU)</p> <p>3. Nurture collaboration between multiple technology groups, standards</p>

Source: Adapted from Rao (2003)¹¹

¹¹ Rao, Madanmohan (2003). News Media and New Media: The Asia-Pacific Internet Handbook. Singapore: Eastern Universities Press.

Internet as a (Global) Public Good/Global Commons

The Internet has become “the public space of the 21st century – the world’s town square, classroom, marketplace, coffeehouse, and nightclub”.¹² As a room where opinion are shaped and articulated, the Internet therefore needs to be protected. By definition a public good is inexhaustible and available freely to everybody. The Internet does not fully meet either of the two criteria, in particular if the digital gap is taken into account, which exists on the global level, but also inside countries, for example between urban and rural areas, between the well-schooled and the less educated, between the rich and the poor, and between men and women. Further, the Internet usually is not free of charge. However, there are trends which point in the direction of the Internet as a public good: some countries, like Finland have made access to the Internet a constitutional right and others like Albania, Germany, Estonia etc. have included a right to access to the Internet in their national law.¹³ Indeed, being excluded from the opportunities that information society offers through the Internet is progressively seen as a denial of the fulfillment of human potential and a barrier to human development.

In many countries the Internet is freely accessible in public libraries, in stations, certain trains or airports or in other public places like universities. Citizens can benefit from the opportunities of the Internet freely or at a low cost. In the South, some governments, sometimes with international support, have created hotspots in the countryside in order to provide access to the knowledge society through information and communication technology (ICT). Best practices include the creation of Community Multimedia Centres which combine all the new technologies providing community with ICT infrastructure to gain access to information available worldwide.¹⁴

But the discussion on the Internet as a *global* public good goes beyond national initiatives. Arguably, the Internet is to be a global public good. States have committed, in the four outcome documents of the World Summit on the Information Society¹⁵ to the central tenets of the information society of the future. They committed, in the Geneva Declaration of Principles of 2003, to creating a “people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights”.¹⁶

In the 2005 Tunis Commitment, States have reaffirmed this commitment to the people-centered, inclusive and development-oriented Information Society and added that it was to be based on “international law and multilateralism” with the goal, inter alia, for people to attain “the internationally agreed development goals and objectives, including the Millennium Development

¹² Secretary of State Hillary Rodham Clinton, Internet Rights and Wrong: Choices and Challenges in a Networked World, George Washington University, Washington, D.C., 15.02.2011, <http://www.state.gov/secretary/rm/2011/02/156619.htm>.

¹³ See Organisation for Security and Cooperation in Europe (OSCE): The Office of the Representative on Freedom of the Media, Report on Freedom of Expression on the Internet, Study of Legal Provisions and Practices Relating to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States, Vienna 2011.

¹⁴ See UNESCO, Towards Knowledge Societies, Paris 2005.

¹⁵ World Summit on the Information Society (WSIS), Geneva Declaration of Principles, WSIS-03/GENEVA/DOC/4-E of 12 December 2003; World Summit on the Information Society (WSIS), Geneva Plan of Action, WSIS-03/GENEVA/DOC/0005 of 12 December 2003; World Summit on the Information Society (WSIS), Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E of 18.11.2005; World Summit on the Information Society (WSIS), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18 November 2005.

¹⁶ WSIS, Geneva Declaration of Principles (2003), para. 1.

Goals”.¹⁷ In this light protecting the Internet as a global public good is a key factor in promoting human self-fulfillment and human development.

Public Service Value of the Internet

In this context, there is a need to promote locally the “public service value” of the Internet, because people in a growing number of countries have become increasingly reliant on the Internet as a necessary tool for their managing everyday life. Accordingly, the public as well as the private sector is called upon to strengthen the public service value of the Internet by making Internet access and Internet services accessible and affordable in a non-discriminatory and content-neutral fashion, ensuring secure and reliable connections and taking into account the requirements of human rights and democracy, access and openness, diversity and security.¹⁸ This, too, is a prerequisite for ensuring the people-centered, inclusive and development-oriented information society, as required by the World Summit on the Information Society (WSIS) outcome documents.

Additional Benefits and Opportunities

The direct and fringe benefits of an increased use of ICTs in societies are substantial.¹⁹ Apart from economic progress, ICT use leads to an increase in transparency and information on consumer products which provide the consumer with a better choice and which increases competition between service providers and producers. Through the Internet consumers can have access to a wide range of useful information, including product assessments by their peers.

With regard to information on public services, access to information has increased as a result of ICTs. New forms of e-government provide easy access to information and services, but also create technological vulnerabilities (e.g. hacking and DDoS attacks) and new dependencies on the availability and mastery of ICTs. Civil society benefits from the improved access to information, which in some countries is also a fundamental right under the respective “freedom of information laws”²⁰ that increase the knowledge base for civil society to aggregate issues demanding social change and articulate these demands. Furthermore, civil society benefits from social networks and easier communication through the Internet. Not only the Arab Spring in 2011 has shown the potential of the use of new technologies for sharing information, campaigning or organising, associating and protesting. A better informed civil society is also in the public interest and allows for more inclusive and participatory approaches to societal decision-making.

Companies also benefit tremendously from ICT usage. From fishermen in remote villages who use cell phones to allow customers to order fish to multinational companies, ICTs allow companies to offer and promote their good and services globally at a relatively low cost. E-commerce facilitates transactions and increases commercial ties. In addition, the Internet has created new business opportunities and net-based services have one of the highest growth rates.

¹⁷ WSIS, Tunis Commitment (2005), para. 2.

¹⁸ Compare Recommendation CM/Rec (2007) 16 of the Committee of Ministers of the Council of Europe on Measures to Promote the Public Service Value of the Internet, adopted on 07.11.2007. Cf. further the Council of Europe, Declaration by the Committee of Ministers on Internet Governance Principles, adopted by the Committee of Ministers on 21.09.2011 at the 1121st meeting of the Ministers’ Deputies, <https://wcd.coe.int/ViewDoc.jsp?id=1835773>.

¹⁹ Cf. already Atkinson, R. D. and McKay, A. (2007). Digital Prosperity. Understanding the Economic Benefits of the Information Technology Revolution. Washington, DC: Information Technology and Innovation Foundation.

²⁰ See McDonald QC., John; Crail, Ross and Johns, Clive (2009). The Law of Freedom of Information, 2nd edition, Oxford University Press.

Risks and Threats of ICTs

ICTs do not only enable two ways to realise human rights, they also endanger them. In some societies, ICT usage can lead to a deepening social divide. Exclusion of disadvantaged groups can be intensified through enhanced ICT use by other societal groups. What is important to note though, is that the risks and threats that increased ICT usage poses should not dissuade us from using ICTs but rather suggest a human rights sensitive, development-oriented application of ICTs and a keen eye to ensuring that externalities of ICT usage are remedied by either market forces or the state.

Two main categories of problems in increased ICT use can be identified: those related to the structures of implementing ICTs and those related to ICT usage itself.

Structure-Related Problems of ICTs: Externalisation of ICT Market Risks/Legal Aspects of Monopolisation

One structural problem of ICT usage is the externalisation of market risks. Economists such as Friedman and, more extremely, Robert Nozick, have argued that market capitalism alone can ensure political freedom and human development. But it is rather the state that needs to provide rules laying down the parameters for market behaviour to avoid externalisation of market risks. This is especially true for the ICT sector. These rules have to be considered fair in a societal consensus as unregulated commerce is bad for both the economy²¹ and the polity, but so is overregulated commerce.

Both the European Union (EU) and the United States have introduced legal instruments against monopolisation of the ICT sector, with companies such as Microsoft prominent targets. Since ICT companies are the new gatekeepers of the global information and communication space, they have special responsibilities – more so, if they are monopolies or quasi-monopolies. Recognising that search engines²² and social network providers²³ exercise a central role in the information society as intermediaries, the Council of Europe has introduced recommendations seeking to balance the operation of these services, the monopolisation of the market and the challenges to human rights from algorithm design.

Those services that are so successful in monopolising their service sector in the information space might run the danger of creating a quasi-public place. Such a service would then lose some of the protection based on its private ownership in light of the quasi-public function it offers.²⁴

²¹ Wolff, Jonathan and Nozick, Robert (1991). *Property, Justice and the Minimal State*, Oxford: Polity Press.

²² Committee of Experts on New Media, Draft Recommendation on measures to protect and promote respect for human rights with regard to search engines + Draft Guidelines for search engine providers, 15.09.2011, CoE Doc. MC-NM(2011)15, [http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM\(2010\)004rev2](http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM(2010)004rev2).

²³ Draft Recommendation on measures to protect and promote respect for human rights with regard to social networking services + Draft Guidelines for social networking providers, CoE Doc. MC-NM(2011)15, 15.09.2011, [http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM\(2011\)15_en%20HR%20and%20social%20networking%20services.asp](http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM(2011)15_en%20HR%20and%20social%20networking%20services.asp).

²⁴ Cf. *New Jersey Coalition Against the War in the Middle East v. J.M.B Realty Corp*, 138 N.J. 326, 650 A.2d 757, 1994 N.J. 52 A.L.R.5th 777.

Content-Related Problems: Cyber Security: Cyber Crime, Network Security, Child Security, Identity Theft, Hacking, Publication of Classified Information, Hate Speech

The ICTs on which the information society is based have brought also **new societal risks and threats**, which pose new challenges to achieving a human rights-sensitive and development-oriented information society. The misuse of cyberspace for personal illegal profit, false digital identities, the security of data and of networks, the threat of hate speech on the Internet and the need of protection of children against threats ranging from grooming to sexual exploitation are well known. The success in fighting them, however, has only been limited. Sometimes they are also used as fig leaves to cover less noble legislative attempts to exercise more control over, e.g., political speech or pro-democratic activities.

The **publication of classified information** by websites like Wikileaks or OpenLeaks has received much international attention. Part of the material had been published by newspapers like *The Guardian* before and was not legally challenged. There is a debate, when the publication of such information is in the public interest (“whistleblower-argument”) and in which cases the interest of the protection of the privacy of the individuals or state security considerations should prevail, which either requires a balancing of human rights or can be based on national security as a legitimate exceptions of the right to freedom of expression. Generally, the principle can be applied that what is legal offline is also legal online.

The so-called Cybercrime Convention,²⁵ which was adopted in 2003 under the auspices of the Council of Europe and today informs the legislation of more than one hundred states, criminalises offenses against confidentiality, integrity and availability of computer systems, computer- and content-related offences and through its protocol also xenophobia and racist acts through computer systems.

By “identity theft” we understand the misuse of a digital identity for licit or illicit purposes. By “hacking” we refer to the illegal intrusion into a computer system in order to gain private or classified information. Both are illegal and criminalised by national law.

The Internet has also facilitated the promotion of “hate speech”²⁶ and the spread of groups promoting hatred. Hate speech covers all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance”.²⁷ This also includes intolerance expressed by aggressive nationalism and ethnocentrism and discrimination and hostility against minorities, migrants and people of immigrant origin. Some social network providers have taken steps to remove some forms of hate speech, e.g. through the “Abuse Standards” of Facebook,²⁸ but have to be wary not to impose moral standards on their services that infringe upon the freedom of expression of their users.

Measures of **Child Protection** on the Internet in the European Union are coordinated by “Ins@fe”, an association of national child protection organisations following common principles with the support of the EU. For example, in Austria there exist the Internet portal “stopline”, to which visual material of sexual exploitation of minors and racist content can be reported. The reliance of states and Internet Service Providers on private hotlines is not unproblematic, as a recent case in Denmark showed, where a human error in a police center responsible for listing suspected sites

²⁵ Council of Europe, Convention on Cybercrime, CETS No. 185 (2003).

²⁶ See Weber, Anne (2009). Manual on Hate Speech, Council of Europe.

²⁷ Council of Europe, Committee of Ministers Recommendation 97 (20).

²⁸ Facebook, Abuse Standards 6.2. Operation Manual for Live Operators, <http://www.scribd.com/gawker/d/81877124-Abuse-Standards-6-2-Operation-Manual>.

resulted in the unaccessibility, for some time, of sites such as Google and Facebook.²⁹ Discussions on deletion or blocking of suspected sites have also not led to internationally acceptable results.

Linkages between ICT and Human Rights

The Internet has an enormous potential to increase the level and intensity of communication between humans and even things (-> Internet of Things). Like with any media, there are close linkages between the technology applied and human rights. Because of the relevance of the Internet in all spheres of life, it also touches on nearly all human rights as can be seen from the draft Charter on Human Rights and Principles for the Internet, elaborated by the Dynamic Coalition on Internet Rights and Principles in 2010 and 2011.³⁰

Following up on the various references to the Universal Declaration on Human Rights and the final documents of the World Summit on the Information Society of 2003/2005, the Charter showed the clear link between the Internet and most rights contained in the Universal Declaration, starting from the right to non-discrimination in Internet access, to education, access to knowledge, right to online participation in public affairs and effective participation in Internet governance. Additional rights concerned are the right to development and the right of the child. The core rights of concern to the Internet, however, are the freedom of expression and information and the right to privacy and data protection, which will be dealt with at a later stage in more detail.

Right to Access to the Internet

The right to access to the Internet, which is the first right spelled out by the draft Charter is derived from the conclusion that all the Internet-related rights depend on having access to the Internet in the first place. This has also been recognised by different international bodies like the Council of Europe³¹ and the Joint Declaration on Freedom of Expression and the Internet by the four international special rapporteurs on freedom of expression.³² Still there is some debate whether the right to access should be considered a human right, because it is argued that access to a technology, to a tool, cannot be a human right.³³ However, recent reports confirm access as a human right.³⁴

There is less controversy about the fact that the denial of access to the Internet as such or to part of its content due to blocking and filtering is a violation of human rights. Besides these the Special Rapporteur on the Freedom of Opinion and Expression, Frank La Rue, in his report of 2011, which focused on freedom of expression and the Internet has pointed out a worrisome trend towards “criminalization of legitimate expression” through new laws and practices around the world, which resulted in the imprisonment of bloggers in several countries. He also calls for

²⁹ Cf. Freak, Torrent. Police Censor Google, Facebook and 8,000 Other Sites by Accident, <http://torrentfreak.com/google-facebook-and-8000-other-sites-accidentally-dns-blocked-120302>.

³⁰ See Internet Rights & Principles Coalition, www.Internetrightsandprinciples.org.

³¹ „Convinced that access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the Information Society”; Recommendation CM/Rec(2017)16 on measures to promote the public service value of the Internet.

³² „Giving effect to the right to freedom of expression imposes an obligation on states to promote universal access to the Internet.” International mechanism for promoting freedom of expression, Joint Declaration on Freedom of Expression and the Internet, <http://www.osce.org/form/78309> of 01.06.2011.

³³ Cerf, Vint (2012). Internet Access is not a Human Right. In: New York Times (04.01.2012).

³⁴ See Centre for Law and Democracy, A Truly World-Wide Web: Assessing the Internet from the Perspective of Human Rights, Halifax, Canada, April 2012, www.law-democracy.org.

the decriminalisation of defamation laws, which have a chilling effect on freedom of expression. Further problems identified were practices to hold Internet intermediaries liable for content, which is partly imposed through privacy and data protection laws. In case of a “notice-and-take down” regime, intermediaries can avoid liability if they remove illegal material after having been made aware of it. But this system was also found to be abused by state and private actors.³⁵

Mobile Communications and Internet Access

Smartphones offer users a much richer experience of Internet access, beyond voice and SMS of featurephones. Cameraphones can transform observers into citizen photojournalists and videographers. Mobile Internet rather than landline computer-based Internet access will become the norm for most users in emerging economies.

Mobile networks and the Internet differ in significant ways.³⁶ Mobiles are based on centralised networks, the Internet is based on decentralised networks; mobile services provided by the mobile operator are almost always paid services, but many websites and social media networks provide free or ad-supported services.

Smartphones have mashed together a hybrid world of ‘apps’ – and also introduced a new layer of commercial gatekeepers such as Apple and RIM. Apple has come under criticism for some of its politically and commercially motivated content control, such as banning of Pulitzer Prize-winning cartoonist Mark Fiore.

Governments in emerging markets such as Africa and Asia are much more likely to be wary of SMS communications (and therefore censor them) because the number of people able to send and receive text messages is much larger than those who access the mobile Web. Ironically, an attempt by the Kenyan government to control the media would spawn the Ushahidi project, which has become a success story in enabling disaster news coverage and political reporting.

Broadcast media such as TV and radio were highly regulated from the beginning of their existence; in contrast the Internet has been more protected as a platform for freedom of expression. Mobiles add a new twist by being both a medium and a content delivery platform (Southwood, *ibid.*). Mobile access to the Net brings new perspectives to the debates on Net neutrality and new concerns about privacy of device data, cloud data, location-based services and geo-tracking of citizens activists.

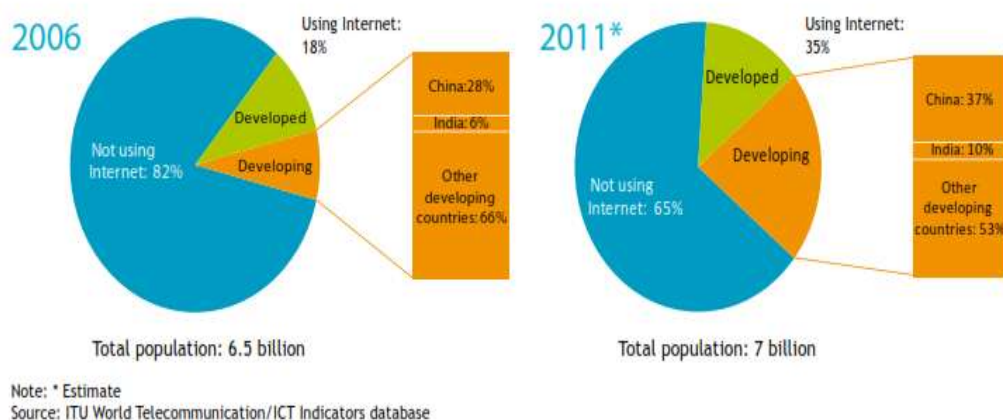
As the Internet becomes increasingly adopted on mobile phones, particularly smartphones, a new set of opportunities and challenges opens up in ensuring that mobiles are accessible and affordable around the world, and that mobile restrictions do not overlay Internet restrictions to content creation and consumption. Today, more than two thirds of the world population live in rural areas. There are now six billion mobile subscribers and this number will exceed seven billion in 2013 (see Fig. 1). More people than ever before have access to mobile phones and many are still in remote rural areas, particularly in emerging economies. But rural areas may have to do with 2G applications for a while longer until 3G coverage becomes widespread and affordable.³⁷

³⁵ Report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, La Rue, Frank, UN Doc. A/HRC/17/27 of 16.05.2011, paras.34-36.

³⁶ Southwood, Russell (2011), <http://www.apc.org/en/node/12433/>.

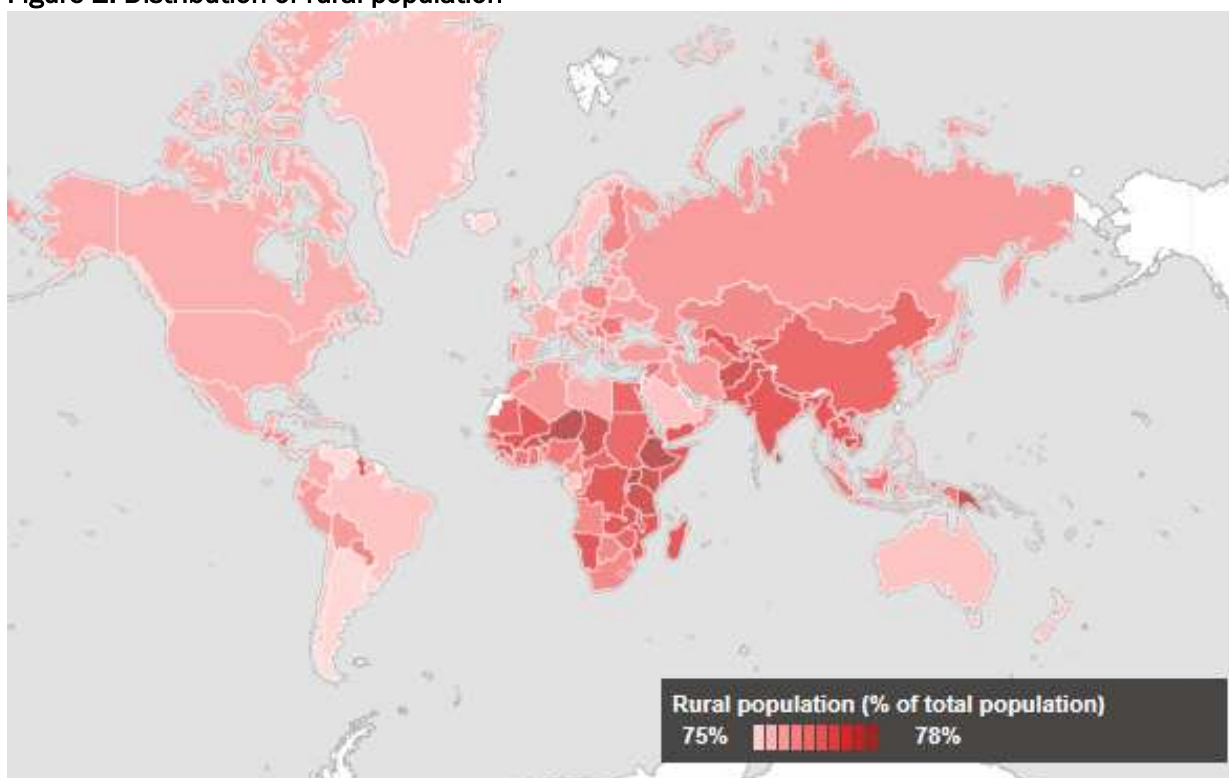
³⁷ Patel, Bashir. Rural Mobile. In: Bruck, Peter and Rao, Madanmohan (2013-forthcoming), Global Mobile: Scenarios and Strategies. New Jersey: InfoToday/Perseus Publishing.

Figure 1. Comparison of Internet users between developed and developing countries



Mobile represents the most effective ICT for delivering services, content and applications to people even with narrow bandwidth. The positive impact mobiles have upon socio-economic development is unequivocal. At a macroeconomic level mobiles increase GDP and the foreign direct investment that less developed countries must attract. Research by Ericsson and Zain on the impact of mobiles in Sudan concluded that a 1 % increase in mobile penetration caused a 0,12 % increase in the country's GDP growth rate, due partly to the greater productivity and efficiency of small businesses which benefited from improved information flows.

Figure 2. Distribution of rural population



Source: World Bank³⁸

³⁸ World Bank, <http://data.worldbank.org/indicator/SP.RUR.TOTL.ZS/countries?display=map>.

Many of the developing countries need to ensure that they have the necessary national backbone infrastructure in place in order to offer broadband services, although many will ‘leap frog’ through adopting new wireless technologies such as LTE and SCDMA in order to offer broadband services. Affordable mobile broadband will eventually make a valuable contribution to rich-media access in rural areas of the world (see distribution of worldwide rural population in Fig. 2; India, China and Africa account for a huge share).

The first decade of the 21st century has represented the ‘mobile voice revolution’ with SIM penetration reaching 60 % or more in many of the major developing economies by the end of 2011. The second decade is set to be the age when the Internet reaches people not only in urban but also in rural areas, be it via a nomadic service or a more traditional fixed-line connection (see Table 2 for ICT distributions).

Table 2. ICT subscriber totals and penetration rates by regions

Key Global Telecom Indicators for the World Telecommunication Service Sector in 2011 (all figures are estimates)									
	Global	Developed nations	Developing nations	Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas
Mobile cellular subscriptions (millions)	5,981	1,461	4,520	433	349	2,897	399	741	969
Per 100 people	86.7%	117.8%	78.8%	53.0%	96.7%	73.9%	143.0%	119.5%	103.3%
Fixed telephone lines (millions)	1,159	494	665	12	35	511	74	242	268
Per 100 people	16.6%	39.8%	11.6%	1.4%	9.7%	13.0%	26.3%	39.1%	28.5%
Active mobile broadband subscriptions (millions)	1,186	701	484	31	48	421	42	336	286
Per 100 people	17.0%	56.5%	8.5%	3.8%	13.3%	10.7%	14.9%	54.1%	30.5%
Fixed broadband subscriptions (millions)	591	319	272	1	8	243	27	160	145
per 100 people	8.5%	25.7%	4.8%	0.2%	2.2%	6.2%	9.6%	25.8%	15.5%
Source: International Telecommunication Union (November 2011)							via: mobiThinking		

Source: ITU³⁹

Increased competition amongst operators can help force down prices, and greater collaboration between manufacturers and content producers will be needed to bring the fruits of ICTs to a broader subscriber base.

Governmental Censorship (Blocking and Filtering)

Countries across the world vary in the extent to which they promote or restrict freedom of expression. This is also a function of other parameters such as existence of powerful media watchdogs, supporting legal systems, and a culture of open critique. Organisations such as the Open Net Initiative (ONI) track the openness of a country’s Internet ecosystem based on the government’s decisions to filter or abstain from filtering the Internet, as well as the impact, relevance, and efficacy of technical filtering in a broader context of Internet censorship.

³⁹ ITU, http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html.

The technical filtering data alone, however, do not amount to a complete picture of Internet censorship and content regulation. A wide range of policies relating to media, speech, and expression also act to restrict expression on the Internet and online community formation. Filtering of the Internet occurs at the following levels:

1. Political: This category is focused primarily on websites that express views in opposition to those of the current government.
2. Social: This group covers material related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive.
3. Conflict/security: Content related to armed conflicts, border disputes, separatist movements, and militant groups is included in this category.
4. Internet tools: Web sites that provide e-mail, Internet hosting, search, translation, Voice-over Internet Protocol (VoIP) telephone service, and circumvention methods are grouped in this category.

The relative magnitude of filtering for each of the four themes is defined as follows by ONI:

1. Pervasive filtering: Filtering that is characterised by both its depth — a blocking regime that blocks a large portion of the targeted content in a given category — and its breadth — a blocking regime that includes filtering in several categories in a given theme.
2. Substantial filtering: Filtering that has either depth or breadth: either a number of categories are subject to a medium level of filtering or a low level of filtering is carried out across many categories.
3. Selective filtering: Narrowly targeted filtering that blocks a small number of specific sites across a few categories or filtering that targets a single category or issue.
4. Suspected filtering: Connectivity abnormalities are present that suggest the presence of filtering, although diagnostic work was unable to confirm conclusively that inaccessible Web sites are the result of deliberate tampering.
5. No evidence of filtering: Testing did not uncover any evidence of Web sites being blocked.

Ranking of these parameters also includes a measure (low, medium, or high) of the observed transparency and consistency of blocking patterns. The transparency score given to each country is a qualitative measure based on the level at which the country openly engages in filtering. Two measures of governance are introduced by ONI: rule of law and voice and accountability. Rule of Law includes several indicators which measure the extent to which agents have confidence in and abide by the rules of society. Voice and Accountability includes a number of indicators measuring various aspects of the political process, civil liberties, political and human rights, measuring the extent to which citizens of a country are able to participate in the selection of governments.

The ITU also uses two measures of Internet accessibility: the Digital Opportunity Index (DOI) and Internet users as a percentage of the population. The DOI is based on eleven core ICT indicators that are agreed upon by the ITU's Partnership on Measuring ICT for Development. These are grouped in three clusters by type: opportunity, infrastructure, and utilisation. Internet regulation and filtering practices are often dynamic processes, subject to frequent change, and as the context for content regulation and the practice of Internet filtering evolve, updates will need to be made to such studies and new countries may be added, as summarised in Table No. 3.

Table 3: Ranking format of Internet filtering practices

	No filtering	Suspected filtering	Selective filtering	Substantial filtering	Pervasive filtering
Political					
Social					
Conflict/Security					
Internet tools					

Source: Adapted from The Open Net Initiative⁴⁰

Updates to such Internet rankings are needed because even progressive countries sometimes are tempted to take on pro-surveillance or anti-freedom stances based on local political compulsions. Some may even proactively use the Internet to track dissident movements. For all the talk about the democratising power of the Internet, authoritarian governments are effectively using the Internet to suppress free speech, improve their surveillance techniques, disseminate cutting-edge propaganda, and pacify their populations with digital entertainment.

Lawyer and social commentator Evgeny Morozov⁴¹ shows that by falling for the supposedly democratising nature of the Internet, Western do-gooders may have missed how it also entrenches dictators, threatens dissidents, and makes it harder—not easier—to promote democracy. Buzzwords like “21st-century statecraft” are belied by the reality that “digital diplomacy” requires just as much oversight and consideration as any other kind of diplomacy. “The revolution will be Twittered!” declared journalist Andrew Sullivan after protests erupted in Iran in June 2009⁴², but this may be a rather simplistic interpretation of the power of social media.

Morozov cautions that we must stop thinking of the Internet and social media as inherently liberating and why ambitious and seemingly noble initiatives like the promotion of “Internet freedom” might have disastrous implications for the future of democracy as a whole. Social networking tools and other digital technologies also potentially facilitate increased government surveillance by the state.

Human Dignity as Core Concern in the Virtual World

Human Dignity is a core concern in the virtual world as well. It is best preserved by respecting, protecting and fulfilling human rights. In the context of the Internet, the obligation is not only on the state, which is the main duty-bearer, but on all stakeholders, in particular also business, while the state has a monitoring function regarding non-state actors. The problem is that territorial state jurisdiction faces difficulties to deal with problems in global cyber space. Therefore, international cooperation is needed, both with regard to protecting human rights as well as to preventing cybercrime, as human dignity can be endangered both by states and non-state actors.

⁴⁰ The Open Net Initiative, <http://opennet.net/research/profiles>.

⁴¹ Morozov, Evgeny Morozov (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs Books.

⁴² *ibid*

The Internet as Enabler or Threat to Human Rights?

The Internet can be both, a threat to and an enabler of human rights, depending on its use. For example, it may be used to incite others to violence, racism, intolerance, hate speech, or for the glorification of terrorism, which is prohibited by most states and several international conventions. It might be used for grooming, cyber-bullying or sending images depicting sexual exploitation of minors or other forms of cybercrime or for the infringement of privacy and data protection rules, all by private actors. Further human rights issues arise among private actors in relation to the debate on access to knowledge (“free information”) versus copyright. This worries governments, and it should.

As a backlash reaction, the Internet can become a field of censorship, filtering, blocking or of spying on citizens by governments. Accordingly, it increases threats, which exist also with other media, which, however, can be more easily regulated or controlled. This is what worries civil society.

However, the Internet can also serve the fuller enjoyment of numerous human rights, as in particular the freedom of expression and information, the right to education or access to knowledge. It contributes to the preservation of diversity of expression and languages and it allows for new forms of political participation. The Internet as an enabler of human rights provides new opportunities for people to better use their human rights. It is, in the words of Special Rapporteur Frank la Rue, a “catalyst for individuals to exercise their right to freedom of opinion and expression” and thereby a facilitator for the “realization of a range of other human rights”.⁴³

Role of the Internet during the Arab Spring

One case in point was the “**Arab Spring**” of 2011, where a young generation of protesters used social media to prepare and coordinate their protests for democracy and to discuss political topics within and across borders. Through the social media of the Internet the bloggers were able to share their views and experiences with the outside world, thus shaping international public opinion and garnering international solidarity.⁴⁴ They could inform about the situation in places, where journalist were not allowed using short films uploaded on YouTube and thus acting as community reporters (or ‘citizen journalists’). The experience from Tunisia and Egypt repeated itself to a certain extent in Syria in 2012. The total shutdown of the Internet as tried by Egypt and Libya proved not to be a solution for the government, because too many functions of the state and economy depended on the Internet and IT companies, including Skype, quickly made technological deviations available. For these reasons, but also because of international criticism of the blocking of freedom of expression, Egypt had to reopen the Internet within days after the shutdown.

Since the essence of rights and freedoms protected by Article 19 of the Universal Declaration of Human Rights has crystallised into a norm of international customary law,⁴⁵ it is applicable independent of state commitments. There are some cases where authorities can legitimately shutdown certain servers or sites for reasons of national security or the protection of ordre public. Calls to war or to political violence can be seen as a legitimate threat which needs to be

⁴³ Ibid., para. 22, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

⁴⁴ See Liechtenstein Institute at Princeton, Social Media Revolutions, All Hype or New Reality?, Spring 2011.

⁴⁵ Rundle, Mary and Birdling, Malcolm (2008). Filtering and the International System: A Question of Commitment. In: Deibert, Ronald; Palfrey, John; Rohozinski, Rafal and Zittrain, Jonathan (eds.) (2008), Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press, <http://opennet.net/accessdenied>, 73-103.

stopped.⁴⁶ But with regard to the extent of the protection of freedom of expression through the International Covenant on Civil and Political Rights, the Human Rights Committee, its supervisory organ, has clearly ruled that “[t]he legitimate objective of safeguarding and indeed strengthening national unity under difficult political circumstances cannot be achieved by attempting to muzzle advocacy of multi-party democracy, democratic tenets and human rights; in this regard the question of deciding which measures might miss the “necessity” test in such situations does not arise”.⁴⁷ Thus, except for very limited cases, a blanket regional or national shutdown is therefore unjustifiable under international human rights law.

Trends in Europe

In Europe, the Information Society has become a reality for most citizens, which raised the issue of how to cope best with the new challenges of the Internet. Universal values like democracy, human rights and rule of law should be preserved, but the user had also to accept major obligations. For example, the **Data Retention Directive**⁴⁸ of the EU requires all member states to commit Internet Service Providers (ISPs) to store all connection data for at least six months and make them available upon request to the police. This was originally motivated with the fight against terrorism, but in practice the data can be obtained for any criminal offense threatened with a certain punishment (in Austria it is one year of prison). There have been protests against the implementation of this directive in several countries. An evaluation⁴⁹ showed that it is not very effective, that a revision was required, and that several cases had been decided by national Constitutional Courts, setting certain limits, while others are still to come.

Frameworks for Assessing Country Positions on Digital Human Rights

A good way to assess the relative positioning of different countries when it comes to their protection of human rights and ICT access is the comparative framework called the “8 Cs” of the information society (parameters beginning with the letter C): connectivity, content, community, commerce, culture, capacity, cooperation and capital.⁵⁰ There are two ways of looking at ICTs: as an instrument, and as an industry. As an instrument, affordable and usable ICTs can indeed transform the way societies work, entertain, study, govern and live – at the individual, organisational, sector, vocational and national levels. As an industry, ICTs represent a major growing economic sector covering hardware, software, telecom/datacom and consulting services.

The “8 Cs” framework is used to tease apart some of the key challenges in implementing the vision of knowledge societies which respect and support human creativity and liberties, such as increasing ICT diffusion and adoption in developing countries, scaling up ICT pilot projects, ensuring sustainability and viability of ICT initiatives, and systematically analysing research on the global information society.

⁴⁶ Nowak, Manfred (2005). CCPR Commentary, 2nd ed., Kehl/Strassburg/Arlington: Engel, Art. 19, No. 54.

⁴⁷ Mukong v. Cameroon, U.N. Doc CCPR/C/51/D/458/1991 (1994), para. 9.7.

⁴⁸ Directive 2006/24/EC of the European Parliament and of the Council of 15.03.2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105/54 of 13.04.2006.

⁴⁹ See Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM (2011) 225 final of 18.04.2011.

⁵⁰ Rao (2003).

Table 4: The “8 Cs” of the Information Society

	ICTs as an instrument	ICTs as an industry
Connectivity	How affordable and widespread are ICTs (eg. PCs, Internet access, software, mobile phones) for the common citizen?	Does the country have ICT manufacturing industries for hardware, mobile phones, software, datacom solutions and services?
Content	Is there useful content (foreign and local) for citizens to use in their daily lives?	Is content being generated in local languages and localised interfaces? Is this being accessed/used abroad?
Community	Are there online/offline forums where citizens can discuss ICTs and other issues of concern?	Is the country a hub of discussion and forums for the worldwide ICT industry?
Commerce	Is there infrastructure (tech, legal) for digital commerce for citizens, businesses and government? How much commerce is transacted electronically?	Does the country have indigenous digital commerce technology and services? Are these being exported?
Capacity	Do citizens and organisations have the human resources capacity (tech, managerial, policy, legal) to effectively harness ICTs for daily use?	Does the country have the human resources capacity (tech, managerial, policy, legal) to create and export ICTs and set standards?
Culture	Is there a forward-looking, open, progressive culture at the level of policymakers, businesses, educators, citizens and the media in opening up access to ICTs and harnessing them? Or is there nervousness and phobia about the cultural and political impacts of ICTs?	Are there techies, entrepreneurs and managers pro-active and savvy enough to create local ICT companies, services and models and take them global?
Cooperation	Is there adequate cooperation between citizens, businesses, academics, NGOs and policymakers to create a favourable climate for using ICTs?	Is there a favourable regulatory environment in the country for creating ICT products/services, M&A activity, and links with the Diaspora population?
Capital	Are there enough financial resources to invest in ICTs? What is the level of FDI and foreign player participation?	Is there a domestic venture capital industry; are they investing abroad as well? How many international players are active in the local private equity market? Are there stock markets for public listing?

Source: Rao (2003)⁵¹

⁵¹ Rao, Madanmohan (2003). “Visions of the Information Society: A developing world perspective.”, <http://www.itu.int/osg/spu/visions/developing/index.html>.

Based on the analysis from Table 4, it is possible to classify information societies along a continuum based on their support for human rights and Internet access. Countries at the embryonic stage include Afghanistan, where ICT environments are being created with a lot of donor support. Countries at the negotiating stage include China, which have large domestic Internet infrastructure but very strict rules on regulation of Internet content, social media and search engines. Countries at the intermediate stage in Asia include India and the Philippines, which have a generally unfettered environment for online expression but also have a huge digital divide. Countries at the advanced stage include Japan and South Korea, with high levels of ICT penetration and bandwidth and flourishing content environments for Internet and wireless.

At the embryonic stage, Afghan journalists working for the Institute for War and Peace Reporting (IWPR) launched the Afghan Recovery Report (ARR), a free service providing local media outlets and the international community with objective and reliable news from local sources. International Non Governmental Organisations (NGOs) have been focusing attention on Afghanistan using the Internet, including ReliefWeb and InterNews.

On the wireless content front, Japan and South Korea are exporting their successful technologies and operating strategies to other markets like the US and Europe. Several new business models, content strategies, and alliances have been unleashed by the mobile Internet in markets like Japan. Regions like North America and Europe also set the agenda in terms of discourse on human rights and ICTs; Europe is far more integrated and coordinated in this aspect of consensus on ICTs and human rights than is Asia.

Table 5: Evolution of national digital environments for human rights

Type	Characteristics	Examples
Embryonic	<ol style="list-style-type: none"> 1. ICT infrastructure is just being rolled out 2. Donor agencies are active in funding and providing human resources 3. Most content is driven by Diaspora, NGOs 	Afghanistan
Emerging	<ol style="list-style-type: none"> 1. Most media and NGOs have a basic online presence 2. Local capacities exist for online content 3. Widespread digital divide exists 	Nepal, South Sudan
Negotiating	<ol style="list-style-type: none"> 1. Strong Internet/wireless infrastructure exists 2. Local capacities and markets exist for online news, e-commerce, m-commerce 3. Government is “negotiating” benefits and challenges of new media; authorities exercise strong control over online content, search engines; political and cultural censorship of Internet is practised 	China
Intermediate	<ol style="list-style-type: none"> 1. Sizeable markets for Internet, e-commerce, wireless exist 2. Digital divide is still an issue, donor agencies are active 	India, Philippines, Brazil

	3. Political climate is generally free of censorship	
Mature	1. Large-scale penetration of Internet, wireless 2. Mature business models for online content 3. Political climate is generally free of censorship	Australia, New Zealand
Advanced	1. Large-scale penetration of broadband and wireless Internet 2. Political climate is generally free of censorship 3. ICT industries are major players in global markets; wireless content models are being exported; these are digital human rights benchmarks	Japan, South Korea, US, UK, EU

Source: Adapted from Rao (2003)⁵²

⁵² Rao, Madanmohan (2003). News Media and New Media: The Asia-Pacific Internet Handbook. Singapore: Eastern Universities Press.

II. Governance of the Internet

From Code as Law to International Regulatory Efforts

In the 1970s and 1980s Internet Governance mainly referred to social norms, the 'Netiquette' as it was later called,⁵³ that guided the way the Internet was run by a highly experienced group from the technical community. They relied on decentralised technical rules agreed on by 'rough consensus'.⁵⁴ Still in the 1990s, Internet governance mainly meant the technical management of domain names, IP addresses, Internet protocols and the root server system by scientific or "technical" actors. Matters were settled by rough consensus and running code, which has been described as "governance without governments".⁵⁵ It is against this background that John Peter Barlow, in 1996, promulgated his famous "Declaration of Cyber Independence".⁵⁶ According to it, governments were not welcome in cyberspace and had no "moral right" to rule cyberspace. Governmental sovereignty was considered to be at odds with a virtual space where no borders existed. In 1999, Lawrence Lessig explained that "code", together with standards and protocols, the software and the hardware of cyberspace, really was the new law of cyber space.⁵⁷ But even early Internet engineers were fully aware that technical choices had moral implications and that the technical community had a responsibility for human rights.⁵⁸

Regulatory Approaches on the Internet: Self-Regulation, Co-Regulation

There exist different ways of regulation: the business sector usually prefers self-regulation, while states or international organisations, such as the European Union, prefer to regulate from above. In the case of the Internet, however, innovative regulatory choices have taken hold in selected Internet Governance regimes.

In the dynamic technological environment characterised by a multistakeholder structure some trust can be placed in the self-regulatory powers of the stakeholders. Different ideological approaches to the relative role of governments and the private sector may lead to a more critical approach, but if the normative goals of the system permit it and no outside constraints forbid it, self-regulation can be very effective.

If the level of state involvement should be higher in light of the normative goals, then co-regulation could be envisaged. One international organisation that has committed to an effective combination of self- and co-regulation is the Council of Europe.⁵⁹ The organisation has developed a number of instruments to deal with human rights challenges on the Internet, including

⁵³ Request for Comments 1855 (Sally Hambridge), <http://www.dtcc.edu/cs/rfc1855.html>, 24.10.1995.

⁵⁴ Cf. the influential RFC 2418: Bradner, S. (ed.) (1998). RFC 2418, Working Group Guidelines, September 1998, <http://tools.ietf.org/html/rfc2418#section-3.3>, at 3.3.

⁵⁵ Kleinwächter, Wolfgang (2008). Multi-Stakeholder Internet Governance: the Role of Governments. In: Benedek, Wolfgang; Bauer, Veronika and Kettemann, Matthias C. Internet governance and the information society, global perspectives and European dimensions, eleven international publishing, Utrecht, 9-30, 10ff.

⁵⁶ Barlow, John Peter (1996). Declaration of Cyber Independence, Davos (08.02.1996), <http://www.worldtrans.org/sov/cyberindependencede.html>.

⁵⁷ Lessig, Lawrence (1999). The Code Is the Law, The Industry Standard, 09.08.1999, <http://www.lessig.org/content/standard/0,1902,4165,00.html>; Lawrence Lessig, Code 2.0, New York: Basic Books, 2006, 72, <http://codev2.cc/download+remix/Lessig-Codev2.pdf>.

⁵⁸ Cf. Cerf, Vint (2012). Internet Access is not a Human Right. In: New York Times (04.01.2012).

⁵⁹ On the Council of Europe's approaches to regulating information society, see Benedek, Wolfgang and Kettemann, Matthias C. The Council of Europe and the Information Society. In: Kicker, Renate (ed.) (2010), The Council of Europe: Pioneer and Guarantor for Human Rights and Democracy, Council of Europe: Strasbourg, 88-93.

recommendations for states and self-regulatory guidelines for search engine providers and social networking providers. This dual approach – co-regulation and ‘guided’ self-regulation – seems promising. It assures that states do not have to be involved in day-to-day management. In both cases, however, states need to ensure that recourse against self-regulatory decisions to the statal rule of law structures is possible.

Development and Role of ICANN

The US government, which had a crucial role for the development of the Internet, accepted the position that there should be as little government involvement as possible in the management of critical Internet resources, such as the domain name system and thus opted for privatisation. Therefore, it supported the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998 as a non-for profit private corporation under Californian law. However, the US Department of Commerce kept some oversight through a Memorandum of Understanding (MoU) on the management of the Top Level Domains (Internet Assigned Names and Numbers Authority (IANA) function) and the A-root server, the technical backbone of the Internet. This MoU was extended several times until 2009, when it was finally terminated handing over full authority to ICANN. However, the contract regarding the “IANA functions”, chiefly managing the root zone file, was kept as a separate matter and only given to ICANN on a temporary basis.

The reaction by the European Communities in 1998 to the ICANN proposal was that while it agreed with the privatisation of the DNS-management, it preferred a more global management for this global resource. The International Telecommunication Union (ITU) criticised the MoU and stated that the development of the Internet should be led by the market and private initiative.⁶⁰

The role of governments in ICANN was restricted to a Governmental Advisory Board (GAC), which can only ask for “consultations” with the ICANN Board, if its advice is not taken. More than 100 governments are part of the GAC, but many are not participating regularly. The ICANN Board itself is composed of 14 “directors” and the president (CEO). Two members of the board are nominated by each of three supporting organisations, i.e. the Address Supporting Organization (ASO), the Generic Names Supporting Organisation (GNSO) and the country Code Name Supporting Organisation (CCNSO). The others are proposed by a Nominating Committee, while a geographical representation has to be respected. There is a strong role of business and of the Internet community. Besides the GAC, ICANN has a number of other advisory committees, like the At-Large Advisory Committee representing the at-large community organised on a regional basis.⁶¹

Over time, ICANN has gained a good reputation for its transparent work asking comments from the community for all regulatory projects and providing open access to its half-yearly meetings, where its policies are discussed. Certain governments and the European Union were more critical of its structure and performance, which gives them only a limited advisory role. In 2009, the US Department of Commerce (DoC) decided to hand over its oversight function based on the MoU which had been substituted in 2006 by a “Joint Project Agreement” regarding the DNS and root server management. The Affirmation of Commitments (AoC) signed between the DoC and ICANN⁶² is happened also in reaction to international criticism of the privileged role the US had maintained until this time.

In 2012, the US Department of Commerce also put the IANA contract related to managing the root zone file and the generic domain names on tender, but the procedure ended without result

⁶⁰ Compare Kleinwächter, op. cit., 15ff.

⁶¹ See Schweighofer, Erich (2008). Role and Perspectives of ICANN. In: Benedek, Wolfgang; Bauer, Veronika and Kettemann, Matthias C. (eds.) (2008), Internet Governance and the Information Society, Global Perspectives and European Dimensions, Eleven International Publishing, Utrecht, 79-92.

⁶² See Kulesza, Joanna (2012). International Internet Law, Routledge: London, 132 et seq.

as no applicant (i.e. ICANN) was found to fulfil all requirements. The refusal of ICANN to provide more transparency and accountability seems to have been an important factor.⁶³ Another reason might have been the refusal by ICANN to include “global public interest” consideration in its new policy on generic Top Level Domains.⁶⁴ It is expected that in a second round ICANN will gain the contract, which it had administered all along so far, with an improved application providing for more accountability.

In the meantime, ICANN, based on a decision of the Board, which was taken against the advice of the GAC has launched a call for new proposals for generic domain names, for which there had been a strong demand from business and private initiatives “like.berlin”. By the deadline, end of March 2012, there were more than 800 applications for registration of new top level domain names, which will now go through a detailed procedure. Those admitted to a full application will have to pay a US \$ 185.000 registration fee.⁶⁵

The World Summit on the Information Society (2003-2005)

The World Summit on the Information Society (WSIS) was organised by the United Nations on the request of governments, which felt that they should have a stronger role in the governance of the Internet. For example, China proposed to move the ICANN functions to the ITU. Also India, Brazil and South Africa were critical of the principle of private sector leadership. The Summit was to address a broad range of issues, in particular the “digital gap” with regard to access to the Internet. The Summit was organized in two phases, a first conference in Geneva in 2003 and a second in Tunis in 2005. As there was no agreement on the concept of “Internet governance”, a Working Group on Internet Governance (WGIG) was established in Geneva which provided a definition, which was adopted in Tunis, according to which Internet governance is:

*“the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet.”*⁶⁶

In the absence of an agreement on who should be in charge of the management of the critical resources of the Internet, the WGIG in Tunis proposed the creation of a multistakeholder Internet Governance Forum (IGF).

The outcomes of the two meetings in Tunis and Geneva in the framework of WSIS are the normative backbone of Internet Governance: the substance of the emerging field of Internet Governance law. They are the Geneva Declaration of Principles and Plan of Action of 2003 and the Tunis Agenda for the Information Society and the Tunis Commitment of 2005.⁶⁷

⁶³ NTIA, Notice - Cancelled Internet Assigned Numbers Authority (IANA) Functions - Request for Proposal (RFP) SA1301-12-RP-IANA, 10.03.2012, <http://ntia.doc.gov/other-publication/2012/notice-internet-assigned-numbers-authority-iana-functions-request-proposal-rf>.

⁶⁴ Cf. Murphy, Kevin (2012). NTIA says ICANN “does not meet the requirements” for IANA renewal, 10.03.2012, <http://domainincite.com/ntia-says-icann-does-not-meet-the-requirements-for-iana-renewal>. For a discussion, see Kettemann, Matthias C., Good News or Bad News? On NTIA, ICANN, ITU and Why Internet Governance is No Puppet Show, International Law and the Internet Blog, 10.03.2012, <http://internationalallawandtheinternet.blogspot.com/2012/03/good-news-or-bad-news-on-ntia-icann-itu.html>.

⁶⁵ Cf. ICANN, Benefits and Risks of Operating a New gTLD, <http://newgtlds.icann.org/en>.

⁶⁶ See Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1) (2005), para. 34.

⁶⁷ World Summit on the Information Society (WSIS), Geneva Declaration of Principles, WSIS-03/GENEVA/DOC/4-E of 12.12.2003; World Summit on the Information Society (WSIS), Geneva Plan of Action, WSIS-03/GENEVA/DOC/0005 of 12.12.2003; World Summit on the Information Society (WSIS),

Human Rights at the WSIS

Human rights have been called the “missing link” between technology-oriented and value-oriented approaches.⁶⁸ They have also been portrayed as the “pole star” of the Information Society.⁶⁹ Human rights concerns were already discussed in the Geneva phase, mainly due to the instigation of civil society, which had organised an international symposium on that topic, which produced pertinent recommendations.⁷⁰ The Geneva part of WSIS ended with a Declaration of Principles which highlighted the importance of human rights in building a people-centred and development-oriented information society, with explicit references to the Universal Declaration of Human Rights in general and its Art. 19 on freedom of expression in particular.⁷¹ The second part of WSIS produced the so-called “Tunis Commitment”, which reaffirms the “universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration” (para. 3) pointing to the respective paragraphs 3-5 of the Geneva Declaration. It further recognises that “freedom of expression” and the free flow of information, ideas, and knowledge, is essential for the information society and beneficial for development” (para. 4).⁷²

Relevance of the Multistakeholder Approach (Role of Governments, International Organisations, Business, Civil Society, Academia)

The Geneva Declaration of Principles of 2003 contained a commitment by the international community to a multistakeholder-based Internet Governance process. It should involve “all [three] stakeholders and relevant intergovernmental and international organizations”.⁷³ Taken together, the multistakeholder approach to Internet Governance is therefore based on the cooperation of five actors to whom the Tunis Agenda for the Information Society of 2005 allocates certain roles:

- “(1) states, who enjoy “[p]olicy authority for Internet-related public policy issues” as a sovereign right;
- (2) the *private sector*, enjoying an “important role in the development of the Internet, both in the technical and economic fields”;
- (3) *civil society*, playing “an important role on Internet matters, especially at community level”;
- (4) *intergovernmental organizations*, having a “facilitating role in the coordination of Internet-related public policy issues”; and
- (5) *international organizations*, filling an important function “in the development of Internet-related technical standards and relevant policies”.⁷⁴

The international community called for the multistakeholder approach to be “adopted, as far as possible, at all levels”⁷⁵ of Internet Governance. With the creation of the Internet Governance

Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E of 18.11.2005; World Summit on the Information Society (WSIS), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18.11.2005.

⁶⁸ See Joergensen, Rikke F. and Marzouki, Meryem (2005). Human Rights: A Missing Link. In: Heinrich Böll Foundation (ed.), Vision in Process II – The WSIS, at 17.

⁶⁹ Hurley, D. (2003). Pole Star: Human Rights in the Information Society.

⁷⁰ See Statement on Human Rights, Human Dignity and the Information Society, 04.11.2003; www.pdhre.org/WSIS/statement.doc.

⁷¹ See Declaration of Principles, Doc. WSIS-03/GENEVA/DOC/4-E of 12.12.2003, paras. 1 and 4.

⁷² See Tunis Commitment, Doc. WSIS-05/TUNIS/DOC/7-E of 18.11.2005.

⁷³ Geneva Declaration of Principles, para. 49.

⁷⁴ Tunis Agenda for The Information Society, para. 35.

⁷⁵ WSIS, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E of 18.11.2005, 34.

Forum (IGF), the attempt was made to ensure a setting for a global dialogue on the most pressing issues of Internet Governance.

Internet Governance in Asia

Important issues of Internet governance especially with the context of Asia are addressed by the Asia Pacific Regional Internet Governance Forum (APRIGF)⁷⁶. Globally, the Asia-Pacific region has seen the fastest growth of the Internet in recent years; China, India and Indonesia are respectively the first, second and fourth most populous countries on the planet (the US is in third position).

It was the consumption of IP addresses in the Asia-Pacific that triggered the final release of IPv4 addresses at the global level by IANA (Internet Assigned Numbers Authority). Challenges arise in the transition to IPv6 as well as the potential extra-territorial impact of domestic legislative action. For instance, there is concern in Asia that domestic legislation in the US, such as the Cyber Intelligence Sharing and Protection Act (CISPA) may have a similar global impact as international treaties, such as Anti-Counterfeiting Trade Agreement (ACTA) or pending Trans-Pacific Partnership Agreement (TPP). The Third APRIGF to be held in Japan (18-20 July) will discuss a wide range of Internet governance issues, such as IPv6, cybersecurity, privacy, child safety online, freedom of expression and Internet democracy.

Issues of a more technical nature are the domain of the Asia-Pacific Network Information Centre⁷⁷, the regional Internet registry that allocates IP numbers in the Asia Pacific region. Internet governance in the region is also the focus of forums such as Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT)⁷⁸. Issues discussed include how IGF can continue to be a multistakeholder forum, supported by multistakeholder voluntary funding mechanisms with an independent secretariat.⁷⁹ The trilateral India, Brazil and South Africa (IBSA) mechanism, proposes a revision of the IGF's original mandate for it to become more outcome-oriented; to have the capacity to make policy recommendations; have an expanded secretariat located within the UN system; and even suggest the creation of a new global Internet policy decision-making body.

Internet governance issues of importance to the Asia-Pacific region include Internet for disaster relief and recovery (especially in the wake of the Japan tsunami), cyber-security, privacy, data protection, and international law enforcement.

In 2010, APRIGF met in Hong Kong for the first time to provide inputs from the region to the global-level Internet Governance Forum. Singapore has taken the lead in launching multilingual domain names in Chinese and Tamil. But the IDN process is regarded by many to be cumbersome and dense; for example, the IDN ".sg" (Singapore) versions took a considerable time for approval. There are other challenges with cross language or script homophones. There are also concerns that the IDN issues will likely vastly favour Western registries - incumbent or new - at the expense of the poorer IDN peoples and cultures. "Thus it is well possible that after 13 years of disinterest in the East's needs for IDN, the largely West-led ICANN will provide the needed IDNs but only at a great financial, social and cultural cost to many native IDN communities", according to an RIGF panel.⁸⁰

⁷⁶ <http://2012.rigf.asia>

⁷⁷ www.apnic.net

⁷⁸ <http://www.apricot.net>

⁷⁹ APRICOT/APNIC 2012 conference, <http://meetings.apnic.net/33/program/igov>.

⁸⁰ RIGF Asia, http://2011.rigf.asia/summary-reports/APrIGF%20Summary%20Report_Final_August%202011.pdf.

Within Asia, individual countries also hold their own internal consultations on Internet governance. For example, a multi-stakeholders 'Consultation on 7th Internet Governance Forum (IGF), World Summit on the Information Society Forum 2012 (WSIS+10) & Broadband Commission for Digital Development's broadband action plan'⁸¹ was hosted by the Bangladesh Telecommunication Regulatory Commission (BTRC) on 7th May 2012 in Dhaka. The consultation was jointly organised by Bangladesh NGOs Network for Radio & Communication (BNNRC), and Angkur ICT Development Foundation in collaboration with BTRC.

The IGF: A Forum for Permanent Multistakeholder Dialogue

The first IGF was convened in Athens and focused on four main topics: openness, diversity, access and security. These main topics were enlarged later to include critical Internet resources, privacy, emerging issues like cloud computing etc. Further IGFs took place in Rio de Janeiro (2007), Hyderabad (2008), Sharm-el Sheik (2009), Vilnius (2010) and Nairobi (2011). The 2012 IGF will take place in Baku, Azerbaijan.⁸² From the beginning, the IGFs, which are supported by a small UN-backed Secretariat, refrained from making any recommendations, let alone decisions. The purpose of the IGFs is to allow for an open discussion between all stakeholders, i.e. governments, intergovernmental organisations, business, civil society and academia, in a multi-stakeholder approach. With around 1.500 participants which meet in plenary and workshop sessions, open for all, regional and dynamic coalition meetings, the IGF allows for a free exchange of views and expertise on an equal level. All events try to have representatives of all stakeholders at the table. An innovation are the "dynamic coalitions", which work in a multi-stakeholder approach on certain issues of common concern like Freedom of Expression, Linguistic Diversity, Privacy, Gender, Core Internet Values, Internet of Things, Accessibility and Disability, Climate Change or Development. They are supposed to work also during the year and then come back with new reports at each IGF. A number of them address human rights issues and human rights concerns are emerging also in many other topics discussed at the IGF.⁸³

A good example for an active coalition whose activities bear on human rights, is the Dynamic Coalition on Internet Rights and Principles (now: Internet Rights and Principles Coalition), which produced a draft Charter of Human Rights and Principles for the Internet,⁸⁴ which has been first presented at the IGF in Vilnius in 2010 and since further developed.⁸⁵ For example, a commentary on the draft charter has been elaborated⁸⁶ as was a very condensed version of the Charter in form of "10 Internet Rights and Principles", in 2011.⁸⁷

⁸¹ Bangladesh Consultation on 7th IGF, WSIS+10 & Broadband Targets for 2015 of Broadband Commission, <http://www.apc.org/en/blog/bangladesh-consultation-7th-igf-wsis10-amp-broadba-0>.

⁸² See at www.intgovforum.org. There are also proceedings available of the IGFs, see: Doria, Avri and Kleinwächter, Wolfgang (eds.) (2009). Internet Governance Forum (IGF), The First Two Years, UNESCO 2008, Mac Lean, Don, Internet for All, Proceedings of the Third IGF in Hyderabad, United Nations, NY 2009, Drake, William J. (ed.), Internet Governance: Great Opportunities for All, The 4th Internet Governance Forum, Sharm El Sheikh, Egypt, 15.-18.11.2009, United Nations, New York 2010 and Gutterman, Brian (ed.) (2011). Developing the Future Together, The 5th Internet Governance Forum, Vilnius, Lithuania, 14.-17.09.2010, United Nations, Nairobi.

⁸³ See Benedek, Wolfgang (2008). Internet Governance and Human Rights. In: Benedek, Wolfgang; Bauer, Veronika & Kettemann, Matthias C. (eds.), Internet governance and the information society, global perspectives and European dimensions, eleven international publishing, Utrecht, 31-50.

⁸⁴ Internet Rights and Principles Coalition, Charter of Human Rights and Principles, <http://internetrightsandprinciples.org/node/367>.

⁸⁵ Charter of Human Rights and Principles for the Internet, Version 1.1, at www.Internetrightsandprinciples.org.

⁸⁶ See Commentary on the Charter of Human Rights and Principles for the Internet, prepared by the Center for Law and Democracy, Version 2, October 2011, www.Internetrightsandprinciples.org.

⁸⁷ See Internet Rights and Principles Coalition (IRP), www.Internetrightsandprinciples.org.

The future of the IGF was subject to a review by the United Nations undertaken after five years, which resulted in a prolongation for another five years.⁸⁸ Still, discussions were conducted in 2011 and 2012 in the United Nations Committee on Science and Technology for Development (UNCSTD) regarding an improvement of the working methods and resources for the IGF to make it more effective by improving the preparatory process and the selection for the Multistakeholder Advisory Group (MAG), which consists of 56 members. One of the issues debated was the meaning of a possible “enhanced cooperation” and whether it should take place inside or outside the IGF. There are also controversial discussions on a possible WSIS +10 event.

The success of the multi-stakeholder approach of the IGF⁸⁹ stimulated a number of regional and national fora also devoted to a multi-stakeholder dialogue, which feed their results into the global IGF in an informal way. Such regional fora have become a regular practice in Africa,⁹⁰ Asia⁹¹ Australia and the Pacific,⁹² the Americas,⁹³ and Europe, where the first EuroDIG (European Dialogue on Internet Governance)⁹⁴ took place in Strasbourg in 2008 and since has taken place in Geneva 2009, Madrid 2010 and Belgrade 2011 and is scheduled to take place again in Stockholm in June 2012. The Council of Europe serves as the main convener with the assistance of civil society and other stakeholders. Successful efforts were made to introduce young people to Internet governance issues by regular training and summer courses.⁹⁵

At the 2011 IGF in Nairobi, Kenya, plans were voiced to turn the IGF into a feeder event for Internet-related public policies to be forwarded to the UN General Assembly (with regional IGFs acting as feeders for the main IGF), but other roles have also been considered.⁹⁶ Such a role could eventually lead to a normative procedure such as the one currently used by the International Law Commission, albeit on a much more limited scale, with experts providing reports and suggestions, and the General Assembly adopting the norms, if agreement can be found.

Processes at the UN Level – Threats to Internet Freedom?

Besides the IGF process, there have also been efforts by certain states to promote an international code of conduct for information security.⁹⁷ While this addresses the general concern

⁸⁸ See United Nations General Assembly Resolution A/RES/65/141 of 02.02.2011.

⁸⁹ See de la Chapelle, Bertrand (2007). *Towards Multi-Stakeholder Governance – The Internet Governance Forum as Laboratory*. In: Kleinwächter, Wolfgang (ed.), *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment*, Berlin, 256-270 and Malcolm, Jeremy (2008). *Multi-Stakeholder Governance and the Internet Governance Forum*, Perth: Terminus Press.

⁹⁰ Southern African IGF, <http://www.apc.org/en/node/12747>; East Africa Internet Governance Forum, <http://www.eaigf.or.ke>; West Africa Internet Governance Forum, <http://www.waigf.org>.

⁹¹ Asia Pacific Regional Internet Governance Forum (APrIGF), <http://2011.rigf.asia>.

⁹² Pacific Internet Governance Forum, <http://pacificigf.org>.

⁹³ Latin American and the Caribbean Regional Preparatory Meetings for the Internet Governance Forum, <http://lacnic.net/en/eventos/mvd2008/igf.html>.

⁹⁴ European Dialogue on Internet Governance (EuroDIG), <http://www.eurodig.org>.

⁹⁵ See for the courses of DiploFoundation, <http://www.diplomacy.edu/isl/ig>, and Kurbalija, Jovan (2010). *An Introduction to Internet Governance*, 4th ed., and the annual European summer courses at Meissen on “Teaching the Internet Governance Leaders of Tomorrow”, which are open to candidates from all the world, www.euro-ssig.eu.

⁹⁶ Cf. Kleinwächter, Wolfgang (2011). *Towards an Improvement of the IGF: Eight proposals for an enhanced role of the IGF*, 14.03.2011, http://www.unctad.info/upload/CSTD-IGF/Contributions/M1/Wolfgang_Kleinwachter.pdf.

⁹⁷ See Letter dated 12.09.2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General on Developments in the Field of Information of Telecommunications in the Context of International Security, UN General Assembly, 14.09.2011, A/66/359.

for cyber-security already discussed for some time in the United Nations and also the Council of Europe,⁹⁸ the proposal did not meet consensus because it focused on state control over the Internet and seemed to discard important human rights concerns and multistakeholderism. In reaction to the proposed code of conduct, the Civil Society Internet Governance Caucus (IGC) sent an open letter to the President of the UN GA pointing out concerns with the proposed draft resolution, notably the lack of a reference to a multi-stakeholder approach as foreseen in the definition of Internet Governance by WSIS. IGC further criticised that “a multilateral, transparent and democratic Internet management system”, which was proposed in the letter as an institution of states would exclude civil society as it was not mentioned anywhere in the proposal. Furthermore, fears were expressed regarding the impact of certain language on the universality of human rights and on the permissible limitations on freedom of expression.⁹⁹ This lack of inclusion of important stakeholders and some elements of its contents led to the failure of the proposal and showed the strength of international consensus on some of the core architectural principles of Internet development. But the fight is not over. Indeed, the proposal really seems to aim at putting the International Telecommunication Union (ITU) in charge over Internet Governance and establish intergovernmental control instead of the multi-stakeholder approach and ICANN.

The envisaged revision at the International Telecommunication Union’s 2012 summit (WCIT-12)¹⁰⁰ of ITU’s International Telecommunication Regulations (ITRs)¹⁰¹ will indeed be an important event to clarify the role of states in managing aspects of the Internet. The danger of states to renegotiate on WSIS commitments and try to reassert their sovereignty by, e.g., extending the reach of the ITRs to all ICTs has led some commentators to warn of an “U.N. Threat to Internet Freedom”¹⁰² or to identify the start of a “World War 3.0” between the forces of “order” and “disorder”.¹⁰³ However, also Google-co-founder Sergey Brin fears that the freedom of the Internet faces great threats, both, because of efforts of states to strengthen their control over the internet and its users, but also because of the practices of Facebook and Apple to keep users linked only to their platforms and thus contribute to the fragmentation of the Web,¹⁰⁴ NGOs are feeling excluded from the internet debate in the ITU.¹⁰⁵

There are basic differences of opinion on future forms of governance of the Internet between certain states, which would like to give ITU a larger role to deal with public policy issues and other states as well as civil society who fear that this may lead to restrictions of the freedom of the Internet and, in particular, the multi-stakeholder principle in decision-making. One proposal discussed in this context, is the Indian proposal to create a “Committee on Internet-related Policies” (CIRP) to “democratise” the Internet. This proposal aims at a multilateral inter-

⁹⁸ See International and multi-stakeholder co-operation on cross-border Internet, Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, Council of Europe Doc. H/Inf (2010) 10.

⁹⁹ See Open letter to President of the UN General Assembly on International Code of Conduct for Information Security, Nairobi, 28.09.2011, by Internet Governance Caucus.

¹⁰⁰ ITU, 12th World Conference on International Telecommunications, <http://www.itu.int/en/wcit-12/Pages/default.aspx>.

¹⁰¹ ITU, International Telecommunication Regulations (ITRs), <http://www.itu.int/ITU-T/itr>.

¹⁰² See McDowell, Robert M. (2012). The U.N. Threat to Internet Freedom, Wall Street Journal, 21.02.2012, <http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html>; Cf. also Black, Edward J. (2012). UN's ITU Could Become Next Internet Freedom Threat, Huffington Post, 09.03.2012, http://www.huffingtonpost.com/edward-j-black/uns-itu-could-become-next_b_1332768.html.

¹⁰³ Gross, Michael Joseph (2012). World War 3.0, Vanity Fair, May 2012, <http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking.print>.

¹⁰⁴ Katz, Ian (2012). Web freedom, faces greatest threat ever, warns Google's Sergey Brin, The Guardian, 15.04.2012.

¹⁰⁵ Center for Democracy and Technology, ITU Move to Expand Powers threatens the Internet: Civil Society Should have a Voice in ITU Internet Debate, Washington, 12.03.2012.

governmental forum in order to redistribute power away from the US and big business.¹⁰⁶ India and some other countries want a multilateral body to have oversight of standard-setting, decision-making and crises management regarding the Internet, to which part of civil society, which feels excluded, is opposed.

The Democratic Promise and Freedom of Online Expression in Asia

Many of the media laws in Asia were enacted during the centuries of colonial rule by European powers, but several countries after independence modified these laws to encourage more democratic and open flows of news and information. The rise of the Internet after commercialisation of access in 1995 raised hopes that the Internet would open up new opportunities for freedom of expression in the region, especially for those under repressive and authoritarian regimes.¹⁰⁷

Countries like Singapore have laws restricting websites and blogs that promote hatred of ethnic and religious groups¹⁰⁸. Some countries with single-party systems have also implemented restrictions in cyberspace, ranging from firewalls to arresting of dissidents. Such parties embrace the economic potential of the Internet but not its accompanying freedoms of expression.

While online dailies such as Malaysiakini have carved out an important independent space in Malaysian media discourse, the challenge for them is to actually keep the online venture economically viable. Economic sustainability of Web publications that promote independent expression is thus becoming a challenge, especially in emerging economies. In some cases, funding from Western NGOs also raises allegations by local governments about “foreign bias and interference” in local politics.¹⁰⁹

An important contribution of the Internet to Asian discourse is the use of online media by its Diaspora communities, who are based in other more open Asian countries or in the West, and mobilise support for government change. “The Internet has become the single most important medium among Burmese exiles for lobbying work and attempting to change the power balance.”¹¹⁰

In contrast, the Internet has become essential in the formation of public opinion in South Korea. “The openness and speed of the Internet has helped to mobilise the younger generation’s participation in politics and beat the conservatism of the traditional mainstream media.”¹¹¹ The Internet continues to reinvent itself and its role in bringing about democratic change has only just begun. Thanks to its inherent characteristics of information sharing and collaboration, the Internet and online communities will continue to leverage new platforms like mobiles and narratives like blogging.¹¹²

¹⁰⁶ See Parminder Jeet Singh, India’s proposal will help take the web out of U.S. control. In: *The Hindu: Today’s Paper/Opinion*, 17.05.2012.

¹⁰⁷ Gan et al, 2003.

¹⁰⁸ Details can be found in George, Cherian (2012). *Freedom from the Press: Journalism and State Power in Singapore*, Singapore.

¹⁰⁹ Gan et al, *ibid*.

¹¹⁰ Oo, Zaw (2003). “Mobilising online: The Burmese Diaspora’s cyber strategy against the Junta.” In Gan et al.

¹¹¹ Lee, Eun-Jeung (2003). *E-democracy@work: The 2002 presidential election in Korea*. In: Gan et al.

¹¹² Long, Geoff (2003). *Why the Internet still matters for Asia’s democracy*. In : Gan et al (2003).

Unfortunately, the use of the Internet by terrorists to coordinate their activities has “handed a victory to advocates of very tough security measures and strict regulation of the Internet”, according to Reporters Sans Frontiers.¹¹³

Impact of Anti-Terror Laws on Media and Civil Liberties in Europe and Asia

In the aftermath of the 9/11 attacks, a number of legislations have been enacted that progressively granted the government more power in the name of security, to crack down on traditional and online media.¹¹⁴ Mary Robinson, former UN High Commissioner for Human Rights, has said that anti-terror legislation can “undermine journalistic integrity and discourage critical voices.”¹¹⁵ The Committee to Project Journalists warns against creating a culture of violence against the media in the name of national security, when ironically media can play a positive role in social stability.¹¹⁶

For instance, Section 76 of the UK’s Counter-Terrorism Act 2008 proposed that it could be a criminal offence to take a picture of a police officer. Some governments have said they will wiretap journalists suspected of “co-mingling” with terror suspects, or shut down Web sites under national security laws. Some Sri Lankan journalists have also been detained under anti-terror laws, and while countries such as Indonesia have made the transition to democracy, anti-terrorism laws have posed challenges there as well for media operations.¹¹⁷

The Regional Dimension: The Council of Europe, the European Union and OSCE

The governance of the Internet is a multi-layered process as it is taking place at all levels of governance. In this respect the role of the Council of Europe and of the European Union deserve special attention. The Council of Europe, which has a membership of 47 European states and a particular focus on human rights due to the European Convention and the European Court of Human Rights in particular, has developed into the most active international organisation with regard to the challenges of the information society. The conventions elaborated in its framework in this field are usually “open conventions”, like the Cybercrime Convention, which has the US, Canada or Australia among its signatories and the US among its parties. The only Asian country that has signed, but not ratified the Convention is Japan.¹¹⁸ The Council of Europe has participated in and contributed to the Internet Governance Forum since its inception and taken responsibility for the European regional multi-stakeholder forum, i.e. EuroDig.¹¹⁹

With the help of various groups of experts and sometimes in cooperation with other stakeholders, the Council of Europe has elaborated and adopted a number of declarations, recommendations

¹¹³ Reporters Sans Frontiers http://arabia.reporters-sans-frontieres.org/article.php3?id_article=3676.

¹¹⁴ Seneviratne, Kalinga and Yeo, Lay Hwee (2011). *Balancing Civil Rights and National Security*. Singapore: AMIC and European Union Centre in Singapore.

¹¹⁵ International Freedom of Expression eXchange network (IFEX), http://www.ifex.org/international/2011/09/13/shadow_of_terror_laws/.

¹¹⁶ Seneviratne and Yeo, *ibid*.

¹¹⁷ Seneviratne and Yeo, *ibid*.

¹¹⁸ Council of Europe, Convention on Cybercrime, Status as of 06.04.2012, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

¹¹⁹ See Benedek, Wolfgang and Kettemann, Matthias C. (2010). The Council of Europe and the information society. In: *The Council of Europe, Pioneer and Guarantor of human rights and democracy*, Council of Europe Publishing, Strasbourg, 109-115.

and guidelines, in particular on issues of Internet Governance, and on human rights and the Internet, which were also presented to the IGF and might inspire other regions or actors.¹²⁰

Regarding the role of human rights in the Information Society and Internet Governance, the Council of Europe, already in 2005, the year of the conclusion of WSIS in Tunis adopted a “Declaration on human rights and the rule of law in the Information Society”.¹²¹ It adopted human rights guidelines for Internet Service Providers,¹²² human rights guidelines for Online Game Providers¹²³ and Recommendation on measures to protect and promote respect for human rights with regard to social networking services and search engines.¹²⁴

These examples show the efforts of the Council of Europe to address practical issues of the information society from a human rights perspective and may provide guidance as best practices well beyond Europe.

In the recently adopted “Council of Europe Strategy for Internet Governance 2012-2015”, the Council of Europe commits itself once again to promoting an Internet based on its core values and objectives, namely human rights, pluralist democracy and rule of law, with a maximum of rights and freedoms for Internet users and a minimum of restrictions. For this purpose, a “compendium” of existing human rights for Internet users, which also helps them to seek effective recourse to key Internet actors and when their rights have been violated is foreseen to be developed.¹²⁵ Another focus will be advancing privacy and data protection while freedom of expression and information remains a core concern as does effective cooperation against cybercrime.

The European Union, in comparison with the Council of Europe, follows a more economic and political agenda with regard to the governance of the information society. While the Council of Europe is more concerned with standard-setting, the EU is more involved in shaping international policies as can be seen from the debate around the future of ICANN.¹²⁶ It has pronounced a European Digital Agenda in 2010, which also propagates the development of “digital user rights”.¹²⁷ However, the EU is currently involved in several debates regarding the revision of its standards, in particular in the field of data protection, where the directive dating from 1995 is to

¹²⁰ See Kettemann, Matthias C. (2010). Ensuring Human Rights Online: An Appraisal of Selected Council of Europe Initiatives in the Information Society Sector in 2010. In: Benedek/Benoit-Rohmer/Karl/Nowak (eds.) (2011), European Yearbook on Human Rights 2011, NWV/Intersentia, Vienna/Antwerp, 248-267.

¹²¹ Council of Europe, Committee of Ministers, CM (2005) 56 final of 13.05.2005.

¹²² Human Rights Guidelines for Internet Service Providers, developed by the Council of Europe in Cooperation with the European Internet Service Providers Association (EurolSPA), Council of Europe, Doc. H/Inf (2008) 9.

¹²³ Human Rights Guidelines for Online Game Providers, Developed by the Council of Europe in cooperation with Interactive Software Federation of Europe, Council of Europe Doc. H/Inf. (2008) 8.

¹²⁴ Draft Recommendation on measures to protect and promote respect for human rights with regard to social networking services + Draft Guidelines for social networking providers, CoE Doc. MC-NM(2011)15, 15.09.2011, [http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM\(2011\)15_en%20HR%20and%20social%20networking%20services.asp](http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM(2011)15_en%20HR%20and%20social%20networking%20services.asp); Committee of Experts on New Media, Draft Recommendation on measures to protect and promote respect for human rights with regard to search engines + Draft Guidelines for search engine providers, 15.09.2011, CoE Doc. MC-NM(2011)15, [http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM\(2010\)004rev2](http://www.coe.int/t/dghl/standardsetting/media/MC-NM/MC-NM(2010)004rev2).

¹²⁵ Internet Governance – Council of Europe Strategy 2012-2015, Council of Europe, Council of Ministers CM (2011) 175 final of 15.03.2012.

¹²⁶ See Kettemann, Matthias C. (2010). Internet Governance and Human Rights in Europe: Towards a Synthetic Approach. In: Benedek/Benoit-Rohmer/Karl/Nowak (eds.), European Yearbook on Human Rights 2010, NWV/Intersentia, Vienna/Antwerp, 335-352.

¹²⁷ See Granada Ministerial Declaration on the European Digital Agenda of 19.04.2010, <http://ec.europa.eu/ceskarepublika/pdf/press/ks7rada.pdf>.

be replaced by a new regulation and a new directive.¹²⁸ Users should be given more autonomy over their data including “a right to forget”, i.e. to have their data deleted after some time by Internet intermediaries and service providers.¹²⁹

The European Parliament has commissioned an interesting study on ICTs and human rights, which emphasises the new opportunities created by ICT to more fully realise human rights. It also highlights that ICTs have equipped human rights activists with new tools for defending human rights. It further analyses the new threats to human rights by the use of ICT, including the growing use of censorship and surveillance mechanisms by states.¹³⁰ Against this background the European Parliament has become active in trying to curb the export of surveillance technology. As one result the European Council in March 2012 has banned the export of surveillance technologies to Iranian authorities because of alleged serious human rights violations.

The Organization for Security and Cooperation in Europe (OSCE), which has 56 members, including the United States and Canada, in 1996 established a Representative on Freedom of the Media within the OSCE Office in Vienna, who at present is Dunja Mijatovic. She is increasingly confronted with issues of censorship of the Internet and raises her voice for the defence of freedom of expression and information with all media. A broad study commissioned by the OSCE Representative on “Freedom of Expression on the Internet” based on a questionnaire showed that about one third of the members have legal provisions enabling access to the Internet, but also that many restrictions exist on Freedom of Expression.¹³¹

Example of business-based value-driven self-regulatory scheme: Global Network Initiative (Google, Microsoft, Yahoo! etc.)

Not only states and civil society are concerned with human rights and the Internet. The **Global Network Initiative** (GNI) can be considered an example of good practice of three major ICT companies (Google, Microsoft and Yahoo!) who, through self-regulatory measures, have taken a major active role towards meeting the challenges of ensuring human rights while doing business in the ICT sector. Together with a number of civil society organisations, a few investors and academic organisations GNI was launched in 2008 and started to work in 2010.¹³² It has since focused on freedom of expression and privacy in particular¹³³ and developed implementation.¹³⁴ The multi-stakeholder collaboration has also developed standards of responsible company

¹²⁸ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, Brussels, 25.01.2012; Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, Brussels, 25.01.2012.

¹²⁹ On the right to delete, see Mayer-Schönberger, Viktor (2009). Delete. The Virtue of Forgetting in the Digital Age, Princeton University Press.

¹³⁰ European Parliament, Directorate-General for External Policies, Policy Department, Information and Communication Technologies and Human Rights, 2010. The study was commissioned by the Sub-Committee on Human Rights (DROI) from Global Partners and Associates, London.

¹³¹ Organisation for Security and Cooperation in Europe (OSCE) (2011). The Office of the Representative on Freedom of the Media, Report on Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating states, Vienna, <http://www.osce.org/fom/80723>.

¹³² Global Network Initiative, <http://globalnetworkinitiative.org>.

¹³³ Global Network Initiative, Principles, <http://globalnetworkinitiative.org/principles/index.php>.

¹³⁴ GNI, Implementation Guidelines, <http://globalnetworkinitiative.org/implementationguidelines/index.php>.

decision-making,¹³⁵ drawing inspiration from the Framework to protect, respect and remedy and the principles adopted by the Human Rights Council in light of the proposal by the Special Representative of the United Nations Secretary General on Business and Human Rights, John Ruggie, in 2008 and 2011 respectively.¹³⁶ It presents its process as a shared learning experience, using human rights impact assessments and creating transparency and accountability standards. The GNI has also managed to mobilise an important number of academic institutions and human rights NGOs who have agreed to join the initiative.¹³⁷

Among the good practices developed by the three companies, which try to engage other business operators as well, is the “Transparency Report” by Google, which gives a picture – with certain limitations – every six months of the requests received to remove content or hand over user data from governmental agencies and courts around the world.¹³⁸ It is left to the observer whether it considers those requests and Google’s reaction to be fair and in keeping with international human rights law. Unfortunately, the information provided is less than sufficient for that purpose. Analysing the data published so far gives the impression that a growing number of states from all parts of the world are making such removal requests, but that Google tends to comply only in cases of violations of its Community Standards, some local law or international law.¹³⁹

Recently, a civil society group developed the Stockholm Principles for Governmental Transparency Reporting on Net Freedom. These Principles are based on the conviction that more data is needed on governmental limits on Internet Freedom and that transparency is needed with regard to the policies that governments pursue to censor Internet content.¹⁴⁰

ICTs: Access, Expression and Human Rights in Asia

Despite hurdles in basic connectivity and unfavourable legislation in some Asian countries, the Internet has had a significant impact on the freedoms of access and expression in the region.¹⁴¹

Online citizens in Bangladesh could circumvent the government’s ban of the Far Eastern Economic Review magazine’s Bangladesh issue by reading it online. The Internet played a key role as a communication conduit during the Fiji coup of 2000.¹⁴²

India has a free press climate as compared to some of its Asian counterparts, but overcoming the digital divide will remain a key concern in India for years to come and some recent regulatory proposals about social media content have drawn the ire of free speech advocates. South Korea is one of the most vibrant markets for wired and wireless Internet content, and leads the world in broadband Internet penetration, online stocktrading, mobile banking and citizen journalism impacts.

In the Philippines, online coverage of the impeachment trial of former president Joseph Estrada and the role of SMS in mobilising popular support against him showed the world the power of the

¹³⁵ GNI, Governance, Accountability & Learning Framework, <http://globalnetworkinitiative.org/governance-framework/index.php>.

¹³⁶ See Mares, Radu (ed.) (2012). The UN Guiding Principles on Business and Human Rights.

¹³⁷ See Global Network Initiative, 2011 Annual Report, http://globalnetworkinitiative.org/files/GNI_2011_Annual_Report.pdf.

¹³⁸ See Google Transparency Report, <http://www.google.com/transparencyreport>.

¹³⁹ Google Transparency Report, Government Requests, <http://www.google.com/transparencyreport/government-requests>.

¹⁴⁰ The Stockholm Principles for Governmental Transparency Reporting on Net Freedom, <http://stockholmprinciples.org>.

¹⁴¹ Rao, 2003.

¹⁴² Rao, 2003.

“smart mob”. Foreign players are eyeing the market for Internet infrastructure and e-commerce in some East Asian countries, but are finding it tough to deal with local regulations, operating environments and IPR protection.

Authorities in Thailand were the first to welcome a censorship policy introduced by Twitter, announcing they will work with the micro-blogging site to ensure any content posted online is in compliance with strict local laws.¹⁴³ Thailand's government already removes online content that is deemed derogatory or offensive towards the country's royalty (via defamation legislation known as the lese majeste laws) and has IT experts who search the Net for such material and have blocked hundreds of such sites. “Freedom of expression must not violate other people's rights or the laws in each country”, according to Thai minister Anudith Nakornthap¹⁴⁴. The government had previously asked Facebook to delete thousands of pages of material deemed ‘harmful’.

Some Asia-Pacific countries have generally open online environments, such as Australia and India, others have exercised some government control, such as China and Malaysia. There, too, the Internet is contributing to a democratisation of viewpoints. For instance, the Web-based news service Malaysiakini (Malaysia Now) has received numerous international awards for its investigative reporting. The site, launched in 1999 by Steven Gan and Premesh Chandran, aims to “test and push the boundaries of free speech and press freedom in Malaysia by providing credible and up-to-date news and analysis” and “to counter the culture of self-censorship in the mainstream media”. Malaysiakini has operated in an environment of harsh government restrictions on independent and pro-opposition print media.¹⁴⁵

“Activists, journalists and opposition groups expected rising Internet access in Malaysia over the past decade to create more room and hunger for political debate, but the promise they saw in “e-democracy” remains unfulfilled today”, according to media analyst Eric Loo.¹⁴⁶ Despite the government's assurance that the Internet will not be censored, it continues to control the medium through licensing bureaucracies, pricing structures, and application of libel and national security laws through its less-than-independent judiciary, according to Loo.

During a 100 day mourning period for the deceased North Korean ruler Kim Jong-Il, citizens in North Korea were reportedly banned by the government from using mobile phones, with warnings that those being caught would be treated as ‘war criminals’.¹⁴⁷

West Asian governments have been more forceful in controlling the Internet. In an effort to protect the Iranian people from “cultural invasion and threats” from the West, the Iranian government has been planning a private “Halal Internet”, referring to the alleged moral and spiritual purity of the contents allowed.¹⁴⁸

Is Internet Access A Human Right?

The United Nations Human Rights Council has examined the important question of whether Internet access is a human right. The Special Rapporteur maintains that restricting access completely will always be a breach of Article 19 of the International Covenant on Civil and Political Rights, the right to freedom of expression.

¹⁴³ The Independent (2012), <http://www.independent.co.uk/news/world/asia/thailand-backs-twitter-censorship-policy-6297296.html>.

¹⁴⁴ ibid

¹⁴⁵ Rao, 2003.

¹⁴⁶ Loo, Eric (2003) in Rao.

¹⁴⁷ Stewart-Smith, Hana (2012), <http://www.zdnet.com/blog/asia/north-korea-makes-cellphone-usage-a-8216war-crime-under-100-days-of-mourning/834>.

¹⁴⁸ Ershadi, Julie (2012), <http://reason.com/blog/2012/01/24/iranian-exiles-protest-halal-internet>.

More specifically, the special rapporteur on freedom of opinion and expression, Frank La Rue, declared in June 2011 that Internet access “had become an indispensable tool for realising a range of human rights” following a series of fact-finding missions in 2010 sponsored by George Soros’ Open Society Institute and the Swedish government. In October 2011, La Rue encouraged governments to protect the free expression rights of citizens, except in cases where freedom of expression violates the human rights of others through racism and hate speech.¹⁴⁹

Internet access is inseparable from freedom of expression and its cousin, freedom of access to information, according to rights activist Adam Wagner,¹⁵⁰ who also observes that Internet use may fall within Article 8 of the European Convention of Human Rights (ECHR) as well: the right to family and private life, since email, Skype, Facebook and Twitter are now essential tools of interaction between friends and family.

Defining Internet access as a human or civil right will make it difficult for governments to place restrictions on access or even shut it down entirely. However, the UK has blocked child pornography sites through ISPs since 1996. Cleanfeed site-blocking technology is intended to be used against foreign pirate sites by BT and other British ISPs.¹⁵¹

The UN Report accepts that in some scenarios Internet access will need to be restricted, for example in the case of sex offenders and terrorist suspects. Internet access in the UK will remain a “qualified” right, reflecting freedom of expression under Article 10 ECHR. That is, it can be restricted but only if that restriction is provided for by law and is necessary or proportionate in a democratic society.

Some Internet experts such as Vinton Cerf, co-creator of the TCP/IP protocol and currently Google’s Chief Internet Evangelist, argue that technology is an enabler of rights, not a right itself, and specific instances of technology (such as the Internet) need not be regarded as a right since the technology itself keeps changing.¹⁵² Cerf maintains that Internet access could be considered a civil right instead. Freedom of the press does not imply the government must give you one, which is a description of the situation by some observers; Internet access is just a more modern manifestation of the right to free speech, and the Internet is becoming like a utility, such as water or electricity.

In sum, human rights are inalienable, fundamental, and emergent from the fact of existing as a human being.¹⁵³ Civil rights are granted universally by a governing authority. To remove a civil right is to restrict a person from having the same things others may have; to remove a human right is to prevent them from being a human being. Laws, regulations and international guidelines, should be aimed at enshrining rights in their pure and timeless forms, not in derivative forms, however widespread and important those derivatives may be.

Human Rights in Internet Governance

Human rights have already been found to be indispensable for Internet Governance. But do existing human rights suffice or is there a need for new digital rights?

¹⁴⁹ See Frank La Rue, op. cit.

¹⁵⁰ Guardian (2012), <http://www.guardian.co.uk/law/2012/jan/11/is-internet-access-a-human-right?newsfeed=true>.

¹⁵¹ Financial Times (2012), <http://www.ft.com/intl/cms/s/0/04b98446-4112-11e1-b521-00144feab49a.html?ftcamp=rss#axzz1I3bRZVGZ>.

¹⁵² Daily Caller (2012), <http://dailycaller.com/2012/01/08/internet-access-not-a-human-right-says-father-of-the-internet>.

¹⁵³ Coldewey, Devin (2012), <http://techcrunch.com/2012/01/05/is-the-internet-a-human-right/>.

The WSIS documents show a holistic approach to human rights protection by referring to the Universal Declaration of Human Rights (UDHR) and the Vienna Declaration and expressly reaffirming the “universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms”.¹⁵⁴

The UDHR assembles all human rights, i.e. civil and political rights as well as economic, social and cultural rights under one normative roof. In its Art. 19, the UDHR also points out that there are also duties of the individual to the community. The general reference in the Geneva Declaration can be interpreted as a holistic approach, but also as a lack of agreement on the relevance of certain rights to the Internet. The exception is the right to freedom of expression, which is highlighted in the Geneva Declaration of Principles, however, qualified by reproducing Art. 29 UDHR in full thereafter, which refers to duties and possible limitations.¹⁵⁵ It further lays down that in this way an information society shall be promoted where human dignity is respected.¹⁵⁶ Under the heading “ethical dimension of the information society” the rights to personal privacy and to freedom of thought, conscience and religion are spelled out.¹⁵⁷

Further efforts to clarify the importance of human rights online come from civil society, which had already been active during WSIS. The Association for Progressive Communication (APC), with a global membership, took the initiative and in 2006 drafted a “APC Internet Rights Charter”,¹⁵⁸ which later served the Dynamic Coalition on Internet Rights and Principles as one of the bases on which to elaborate its Charter on Human Rights for the Internet. At various occasions calls have been made for international documents to provide a comprehensive approach to human rights for the Internet.¹⁵⁹ Before, there have been various more limited attempts, like the “Charter for Innovation, Creativity and Access to Knowledge”¹⁶⁰ or the Declaration of Madrid on Privacy Standards in the Internet of 2009, prepared by civil society.¹⁶¹ The discussion around SOPA and ACTA has stimulated this trend even more. However, the most comprehensive and elaborated approach is the already introduced draft Charter on Human Rights and Principles for the Internet of 2011.

Dimensions of Internet Rights: the APC Internet Rights Charter

It is becoming commonly accepted that the Internet is a global public space that must be open, accessible and affordable to all. APC, the world’s longest-running online progressive network founded in 1990, has drafted an Internet Rights Charter which should provide some good food for thought and action. It connects aspects such as governance, access, content, education, skills and recourse for protection.

The Charter is inspired by the Universal Declaration of Human Rights (1948), the International Covenant on Economic, Social and Cultural Rights (1976), the International Covenant on Civil and

¹⁵⁴ Geneva Declaration of Principles 2003, paras. 1, 3; Tunis Commitment 2005) and para. 2.

¹⁵⁵ See WSIS, Declaration of Principles, paras. 4 and 5, op. cit.

¹⁵⁶ Ibid., para. 5.

¹⁵⁷ Ibid., para. 58.

¹⁵⁸ See APC Internet Rights Charter, <http://www.apc.org/node/5677>. See also the substantive statement of APC before the Human Rights Council in Geneva on „Internet rights are human rights“, May 2011, <http://www.apc.org/en/node/11424>.

¹⁵⁹ See, for example, Mendoza, Nicolas. Metal, code, flesh: Why we need a „Rights of the Internet“ declaration, <http://www.aljazeera.com/indepth/opinion/2012/02/201228715322807.html>.

¹⁶⁰ Charter for Innovation, Creativity and Access to Knowledge 2.0.1. – Citizens’ and Artists’ Rights in the Digital Age, http://fcforum.net/charter_extended.

¹⁶¹ The Civil Society Madrid Privacy Declaration, Global Privacy Standards for a Global World, 03.11.2009, <http://thepublicvoice.org/madrid-declaration>.

Political Rights (1976) and the Convention of the Elimination of All Forms of Discrimination against Women (CEDAW, 1980). Components of the Charter are summarised in Table 6.

Table 6: APC Internet Rights Charter (2006)

Rights Theme	Components
1. Internet access for all	<ol style="list-style-type: none"> 1. Progressive development and social justice (guarding against reinforcement of existing inequalities) 2. The right to access to infrastructure 3. The right to the skills to use and shape the Internet 4. Inclusive design 5. The right to equal access for men and women 6. The right to affordable access 7. The right to access in the workplace 8. The right to public access 9. Cultural and linguistic diversity
2. Freedom of expression and association	<ol style="list-style-type: none"> 1. Protection from infringement by government and non-state actors 2. The right to freedom from censorship 3. The right to engage in online protest
3. Access to knowledge	<ol style="list-style-type: none"> 1. The right to access to knowledge 2. The right to freedom of information (eg. from government) 3. The right to access to publicly-funded information
4. Shared learning and creation	<ol style="list-style-type: none"> 1. The right to share, as well as protection of the interests of creators 2. The right to free and open source software (FOSS) 3. The right to open technological standards 4. The right to benefit from convergence and multi-media content
5. Privacy, surveillance and encryption	<ol style="list-style-type: none"> 1. The right to data protection; clear privacy policies 2. The right to freedom from surveillance 3. The right to use encryption
6. Governance of the Internet	<ol style="list-style-type: none"> 1. The right to multilateral democratic oversight of the Internet 2. The right to transparency and accessibility of governance decisions 3. The right to a decentralised, collaborative and interoperable Internet 4. The right to open architecture
7. Awareness, protection and realisation of rights	<ol style="list-style-type: none"> 1. The right to open standards 2. The right to Internet neutrality and the end-to-end principle 3. The right to the Internet as an integrated whole

	4. The right to rights protection, awareness and education
	5. The right to recourse when rights are violated

Source: APC¹⁶²

Impact of Multistakeholder Coalitions: The Internet Rights and Principles Coalition and its Draft Charter on Human Rights and Principles for the Internet

The Draft Charter of Human Rights and Principles for the Internet¹⁶³ follows the structure of the UDHR of 1948 and complements it, where the development of human rights has led to new or more specific human rights since, like in the case of the right to development, the human rights of women or the rights of the child. It follows a holistic approach, as indicated in the Geneva Declaration of Principles, which refers to the “universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms ... as enshrined in the Vienna Declaration”,¹⁶⁴ which is a reference to the Vienna Declaration and Plan of Action on Human Rights, the final document of the Vienna World Conference on Human Rights of 1993.¹⁶⁵

So, is there a need for new digital rights? The Special Rapporteur on Freedom of Expression, Frank La Rue, in his report of 2011¹⁶⁶ has confirmed that human rights which exist in the off-line world also apply online. This was also the approach of the draft Charter, which did not try to create new rights, but to apply existing human rights to the specific context of the Internet. It also identifies Internet policy principles, such as network neutrality, thus its name.

For example, it spells out a right to non-discrimination of marginalised groups with regard to Internet access, to the security of the Internet, to online protect, to the protection of the virtual personality or digital data protection, to education through and about the Internet, to the diversity of cultures and access to knowledge on the Internet, to freedom of exploitation and child abuse imagery, the accessibility of the Internet to people with disabilities, to online participation in public affairs, to legal remedies, fair trial and due process in actions involving the Internet, to multilingualism and pluralism on the Internet and to effective participation in Internet governance.

The only right, which might be considered new, is the right to access to the Internet, put as Article 1, which reads “*Everyone has the right to access, and make use of, the Internet. This right underpins all other rights in this Charter*”.¹⁶⁷ This right can be logically deduced from the need to have access to the Internet in order to realise all other human rights. However, there is a conceptual controversy as already referred to (Vint Cerf) and a reluctance of states and other actors as this right obviously cannot be fulfilled for everybody in a short time.

However, human rights do not always have to be implemented in full immediately. For example the International Covenant on Economic, Social and Cultural Rights follows an approach of progressive realisation. As indicated in its Art. 2, state parties are “to undertake steps, individually or through international associations and co-operation, ... to the maximum of its available

¹⁶² APC, <http://www.apc.org/en/node/5677/>.

¹⁶³ Internet Rights and Principles Coalition, Charter of Human Rights and Principles for the Internet, <http://irpcharter.org/charter>.

¹⁶⁴ Geneva Declaration, para. 3.

¹⁶⁵ See Benedek/Gregory/Kozma/Novak/Strohal/Theuermann (eds.) (2009). Global Standards – Local Action, 15 Years of Vienna World Conference on Human Rights, NWV/Intersentia, Vienna/Antwerp.

¹⁶⁶ Report of the Special Rapporteur, La Rue, Frank (2011). Op. cit.

¹⁶⁷ Op. cit, note 158.

resources, with a view to achieving progressively the full realization of the rights ...”. Accordingly, the human rights nature of a right to access is not at risk, because the right cannot be achieved at once.

In conclusion, the recognition of a human right to access would not force any actors into a violation of human rights, but it would strengthen the many commitments already made by states and business in particular to work towards their realisation. Anyway, as shown above, many states, also from the South, have already voluntarily made provisions in their law entitling their citizens to Internet access, which creates a trend towards the development of a customary human right to access. The recognition of the various Internet rights derived from international human rights instruments by interpretation is an ongoing process, which largely goes right by right and often happens in practice, but the law also moves in this direction.

What is thus important to note is that there is no need to develop new human rights for the Internet, but rather to apply the existing rights effectively to new online challenges. With the UDHR and the two key UN covenants, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, the international community has a firm universal basis for human rights protection online. The judgments of international and national courts will be of much relevance in this context¹⁶⁸ as are legal reforms like the review of the EU data protection law. In this context, it remains to be seen whether this reform will produce more than minimum standards, i.e. take best practices from member states into account.

Table 7: Rights contained in the draft Charter on Human Rights and Principles for the Internet (Draft 1.1., 2011)

1)	Access to the Internet a) Quality of service b) Freedom of choice of system and software use c) Ensuring digital inclusion d) Net neutrality and net equality
2)	Human Dignity
3)	Non-Discrimination in the Enjoyment of all Rights a) Equality of access b) Gender equality c) Marginalised groups and people with different needs
4)	Liberty and Security a) Protection against all forms of crime b) Security of the Internet
5)	Equality and Diversity on the Internet
6)	Development a) Poverty reduction and human development

¹⁶⁸ See, European Court of Human Rights, Internet: Case-law of the European Court of Human Rights, Research Division, Council of Europe/European Court of Human Rights, June 2011, http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf. These cases include K.U. v. Finland (No. 2872/02), 02.12.2008 (state duties to ensure human rights online); and Renaud v. France (No. 13290/07), judgment of 25.02.2010 (limits to state actions limiting freedom of expression online).

	b) Environmental sustainability
7)	Freedom of Opinion and Expression <ul style="list-style-type: none"> a) Right to Information b) Freedom of Online protest c) Freedom from prior censorship d) Freedom from illegal blocking and filtering
8)	Freedom of Religion and Belief
9)	Freedom of Assembly and Association <ul style="list-style-type: none"> a) Participation in Assembly and Association on the Internet b) Freedom to set up Online Communities and freedom of online protest
10)	Privacy <ul style="list-style-type: none"> a) National legislation on privacy b) Privacy policies and settings c) Standards of confidentiality and integrity of IT-Systems d) Protection of the virtual personality e) Right to anonymity and to use encryption f) Freedom from surveillance g) Freedom from defamation
11)	Data Protection <ul style="list-style-type: none"> a) Protection of Personal data b) Obligations of data collectors c) Minimum Standards on Use of Personal Data d) Monitoring data protection
12)	Education <ul style="list-style-type: none"> a) Education through the Internet b) Education about the Internet and Human Rights
13	Access to Knowledge and Culture <ul style="list-style-type: none"> a) Right to participate in the cultural life of the community b) Diversity of languages and cultures c) Right to use one's own language d) Freedom from Restrictions of Access to Knowledge by Licensing and Copyright e) Knowledge Commons and the Public Domain f) Free/Open Source Software and Open Standards
14	Children and Child Protection <ul style="list-style-type: none"> a) Right to benefit from the Internet b) Freedom from exploitation and child abuse imagery c) Right to have views heard d) Best interests of the Child
15	Work <ul style="list-style-type: none"> a) Respect for Workers' Rights b) Internet at the workplace
16	Participation in Public Affairs <ul style="list-style-type: none"> a) Right to equal access to electronic services

	b) Right to participate in electronic government
17	Consumer Protection
18	Health and Social Services Online a) Access to health-related content online
19	Legal Remedy and Fair Trial a) Right to a Legal Remedy b) Right to a Fair trial
20	Appropriate Social and International Order for the Internet a) Governance of the Internet for Human Rights b) Multilingualism and Pluralism on the Internet c) Effective Participation in Internet Governance
21	Duties and Responsibilities on the Internet a) Respect for the Rights of Others b) Responsibility of power holders
22	22) General Clauses a) Interdependence of all rights in the Charter b) Non-exhaustive nature of the Charter c) Interpretation of Rights and Freedoms of the Charter

Source: Internet Rights and Principles Coalition, Charter of Human Rights and Principles for the Internet, <http://irpcharter.org/charter/>

Various Principles for Internet Governance (and Human Rights)

In 2011, shared principles have evolved as an important tool to guide the evolution of Internet Governance. These principles engage issues of public morality and public interest, but have a less constraining impact than norms or rules. They help guide the normative development of Internet Governance by framing the normative development of the information society.

2011 saw the publication of a number of Internet Governance Principles by different states (such as the US),¹⁶⁹ groups of states (e.g. India, Brazil and South Africa, on behalf of the Group of 77; China, the Russian Federation, Tajikistan and Uzbekistan; the G8),¹⁷⁰ international and

¹⁶⁹ US President Barack Obama proposed 10 principles in his strategy paper in May 2011, see President of the United States of America, International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 10.

¹⁷⁰ India, Brazil and South Africa – on behalf of the Group of 77 – proposed to launch a new “inter-governmental working group [to] be established under the UN Commission on Science and Technology for Development”, IBSA Joint Statement, Open consultations on Enhanced Cooperation, New York, 14.12.2010, <http://www.un.int/india/2010/IBSA%20STATEMENT.pdf>; Letter dated 12.09.2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, 14.09.2011, A/66/359, <http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf>; G8 Declaration, Renewed Commitment for Freedom and Democracy, G8 Summit of Deauville, 26.-27.05.2011, <http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html>.

intergovernmental organisations (e.g. OECD, OSCE, NATO, EU, UNESCO)¹⁷¹ and non-state actors (e.g. Internet Rights and Principles Coalition).¹⁷² Whether termed ‘compact’, ‘commitment’ or ‘strategy’, the documents usually contained certain broadly phrased principles to guide the future development of Internet Governance. Often, these non-binding principles were passed, adopted or published in the forms of resolutions or declarations, such as the Declaration by the Committee of Ministers (of the Council of Europe) on Internet governance principles.¹⁷³ Most combine *rights* (developed in application of the Universal Declaration of Human Rights, as developed by international human rights law), and *principles* (deducted from the international legal order, promoted by multistakeholder declarations of principles and ultimately crystallised through practice) that they wish to see implemented in light of overarching policy goals.

Space does not allow for an in-depth discussion of the different collections of Internet Governance Principles,¹⁷⁴ but a comparative perspective allows us to draw the conclusion that all share certain commitments to Internet economy, Internet security and human rights protection on the Internet – albeit with different emphases. Comparing the different Internet Governance principles, we also find that the multistakeholder-based model of regime development has been accepted without exception. This is an important step in the evolution of the Internet Governance regime. Further, all declarations accept the architectural principles of the Internet, including its end-to-end nature.

Of course, the Principles also reflect the policies of the actor that published them. The OECD focus is on the economic dimension of the Internet, on the importance of innovation and of intellectual property rights. UNESCO focuses on the ethical dimension of the Internet, on its impact on culture and cultural diversity. The US, G8, and the Russia/China proposal highlight the importance of the role of states and of security in the future evolution of the Internet. For NATO, too, cyber security is a key element of the principles. The Council of Europe underlines the importance of human rights in the evolution of the Internet and lays down state duties regarding transboundary Internet traffic. But importantly, none of the principles discounts the importance of either security, economy or human rights in Internet Governance regime design.

States already confirmed in the OECD Seoul Declaration for the Future of the Internet Economy 2008¹⁷⁵ that they shared a vision of an Internet economy covering “the full range of our economic, social and cultural activities supported by the Internet and related information and communications technologies” and allowing states to improve the quality of life for all citizens. Ultimately, this is the goal of all Internet Governance guidelines and principles.

¹⁷¹ UNESCO, Code of Ethics for the Information Society, proposed by the Intergovernmental Council of the Information for All Programme (IFAP), 36 C/49, 10.10.2011, <http://goo.gl/nZ0lk>; OSCE, 8th South Caucasus Media Conference, Declaration: Pluralism and Internet governance, Tbilisi, Georgia, 20.-21.10.2011, <http://www.osce.org/fom/84371>; OECD Communiqué on Principles for Internet Policy Making, OECD High Level Meeting: The Internet Economy: Generating Innovation and Growth, 28.-29.06.2011, Paris, <http://www.oecd.org/dataoecd/40/21/48289796.pdf> (see already OECD, Seoul Declaration for the Future of the Internet Economy 2008, <http://www.oecd.org/dataoecd/49/28/40839436.pdf>); NATO; Vice-President of the European Commission Neelie Kroes, Internet Compact, <http://blogs.ec.europa.eu/neelie-kroes/i-propose-a-compact-for-the-internet/#more-671>.

¹⁷² Cf. Internet Rights and Principles Coalition, 10 Internet Rights and Principles, <http://internetrightsandprinciples.org>.

¹⁷³ Council of Europe, Declaration by the Committee of Ministers on Internet governance principles, adopted on 21 September 2011, <http://goo.gl/RxDWs>.

¹⁷⁴ Wolfgang, Kleinwächter (2011). A Constitutional Moment in the History of the Internet? – How Soft Law is Used to Regulate Cyberspace, *juridikum* 4/2011, 460-470.

¹⁷⁵ OECD Seoul Declaration for the Future of the Internet Economy 2008, <http://www.oecd.org/dataoecd/49/28/40839436.pdf>.

What is important for the immediate future, thus is to agree upon a common commitment regarding the values to be enshrined in the future evolution of Internet Governance as reflected in a fair relationship between the normative trajectories of enabling economic progress, providing for security and ensuring human rights. The principles that best meet this criterion will need to be operationalised.

Mainstreaming Human Rights in Internet Governance

The discussion of the Internet Governance Forum with its broad agenda proves that there is hardly any topic for which human rights do not play any role. Efforts to discuss human rights concerns at the IGF and other general fora so far showed that it is not always necessary to have human rights in the title in order to introduce human rights concerns. Sometimes very technical issues have led to vibrant human rights discussions, because of the social consequences of technological choices. Business and technology look for orientations to human rights as they are normally not interested to be blamed for human rights violations, as can be seen from the Global Network Initiative. States are under human rights obligations anyway. And civil society has a monitoring function it fulfills e.g. by producing reports on Internet freedom like the Global Information Society Watch (GIS Watch) report¹⁷⁶ or the Freedom House report on “Freedom of the Net”.¹⁷⁷

Consequently, the promotion, protection and fulfillment of human rights on the Internet has become an issue of “mainstreaming”,¹⁷⁸ i.e. of institutionalisation in the work of all actors involved in the Internet. This is best achieved by way of Human Rights Impact Assessments (HRIA), before new technologies or business models are launched and by constant monitoring of the social consequences of ICT usage. For this purpose, a multi-stakeholder approach is best, although it does not provide an excuse for any individual stakeholder to neglect their obligations. In practice, the community of users also serves as a review body, for example when users of Facebook or Google complain about disrespect of their privacy forcing the companies to change their policies.

Fragmentation of the Internet

Right from the early days of the Internet, there has been discussion of ‘fragmentation and the Net’. The first wave of debates were about media fragmentation, the second wave about infrastructure fragmentation, and the third wave about online fragmentation. In the domain of media studies, successive media have played a role in both fragmenting and uniting society. Print media in the form of newspapers first began to ‘unite’ societies, but the rise of niche special interest magazines fragmented the reader base.¹⁷⁹ Radio removed some of the adoption barriers that characterised print media, but television subsequently forced radio programming to cater to niche audiences. The popularity of the Internet also led some analysts to raise concerns about fragmentation of online users and their detachment from the ‘real’ world. Social networking from

¹⁷⁶ See, for example, Global Information Society Watch 2011, Internet Rights and Democratisation, Focus on freedom of expression and association online, edited by APC and the Humanist Institute for Cooperation with Developing Countries (Hivos), www.giswatch.org/.

¹⁷⁷ Freedom House, Freedom on the Net 2011, www.freedomhouse.org/report-types/freedom.net.

¹⁷⁸ On mainstreaming human rights in the work of the UN, see Oberleitner, Gerd, A Decade of Mainstreaming Human Rights in the UN: Achievements, Failures, Challenges, Netherlands Quarterly of Human Rights 26 (3) (2008), 359-390.

¹⁷⁹ Dosset, Michael (2011). Fighting History – Fragmentation and the Social Web, <http://letschatbusiness.net/2011/02/26/fighting-history-fragmentation-and-the-social-web/>.

the early days of email lists to the modern day Web 2.0 sites and services have, on the other hand, helped unite audiences around causes and interests.

The second wave of discussion around fragmentation and the Internet revolved around infrastructure and access. Some governments have been blocking access to overseas news sites and search engines. Other kinds of filtering are happening via IP addresses (eg. for video content access from countries other than the host country/region, eg. Spotify).¹⁸⁰ Before the introduction of an official .biz domain, an independent .biz had existed for six years — and for a time the two survived in parallel. And some countries have tested domain names in their own languages by routing those queries to their own root servers.¹⁸¹

The third wave of discussion around fragmentation revolves around the practice of companies like Facebook and Apple, who have come under criticism for creating ‘walled gardens’ that have their own rules for how third-party applications may run and how personal data are dealt with.

“You are trapped in a single store, rather than being on the open marketplace”, says Web inventor Tim Berners-Lee, referring to Apple iTunes.¹⁸² The tendency to create apps for smartphones rather than Web apps also creates “off the Web” worlds. “Many powerful social networking sites do not exchange profile services with each other, thus posing a threat to a ‘single, universal information space’ and potentially stifling future innovation. The goal of the Web is to serve humanity. We build it now so that those who come to it later will be able to create things that we cannot ourselves imagine”, Berners-Lee urges.

“As we saw in the 1990s with the America Online dial-up information system that gave you a restricted subset of the Web, these closed, “walled gardens”, no matter how pleasing, can never compete in diversity, richness and innovation with the mad, throbbing Web market outside their gates”, cautions Berners-Lee.¹⁸³

Fortunately, open source social networking services such as Friendica and the Diaspora Project have started to emerge as real alternatives to the ‘walled gardens’. “The new standard core language of the Web, HTML5 (still in draft and developed through open standards) encompasses a collection of new features to assist Web application authors. Described as the most dramatic evolution of Web standards in over a decade, these enhancements will enable the Web and, as a result, open source social networking services to flourish on mobile communications devices such as smart phones and tablets”, according to Julee Brouwer.¹⁸⁴

Net Neutrality

Net neutrality can be defined as a general principle requiring that all the informations are channelled through the networks without any discrimination. This has to do with technical (lack of capacity in peak periods for example), economic or commercial (pricing policy) considerations of Internet service providers who may choose to restrict or slow down access to certain contents or with legal obligations to block access to certain contents. It raises new concerns about measuring service quality and empowering regulators to impose minimal quality standards to operators or ISPs.

¹⁸⁰ The Economist, 2010, <http://www.economist.com/node/16941635>.

¹⁸¹ Minkel, J. R. (2006), <http://spectrum.ieee.org/computing/networks/could-the-internet-fragment>.

¹⁸² Metz, Cade (2010), http://www.theregister.co.uk/2010/11/20/berners_lee_says_facebook_a_thret_to_web/.

¹⁸³ Berners-Lee, Tim (2010). Long Live the Web: A Call for Continued Open Standards and Neutrality, <http://www.scientificamerican.com/article.cfm?id=long-live-the-web&print=yes>.

¹⁸⁴ Brouwer, Julee (2012), <http://networkconference.netstudies.org/2012/the-web-unspun-the-case-for-open-source-social-network-site-development-in-the-portable-communications-age/>.

Most European regulators have started to work on measuring and analysing the transparency of service quality and traffic management and on the definition of minimal service quality standards which Article 23 of the Universal Service Directive of the EU allows them to establish. If legislation on that topic has been proposed in a limited number of countries such as Italy or France or passed like in the Netherlands, the dominant approach is presently to privilege guidelines or co-regulation with operators and ISPs like in Germany or self-regulation like in UK. Thus, it is at the moment a hot issue in EU.

In the US, some cable TV companies have been considering whether to limit their Internet users to downloading only the company's mix of entertainment. France's HADOPI 1 law, created in 2009, allowed for disconnection of a household from the Internet for a year if someone in the household was alleged by a media company to have ripped off music or video. The provision allowing the user to be disconnected for a year has been cancelled by the Constitutional court¹⁸⁵. The HADOPI 2 law transferred the disconnecting power to the judge as a side sanction to a violation of IPRs (related to counterfeiting). The administrative body can only suspend the connection for one month maximum (which is the consequence of the necessity and proportionality principle applied to the constitutional freedom of expression), after two warnings addressed to the user.

UK's Digital Economy Act allowed the government to order an ISP to terminate the Internet connection of anyone who appears on a list of individuals suspected of copyright infringement. Such disconnection is a form of deprivation of liberty, argues Berners-Lee.¹⁸⁶

One of the Internet's founding principles is that every packet of data, regardless of its contents, should be treated the same way, and the best effort should always be made to forward it. "Allowing broadband carriers to control what people see and do online would fundamentally undermine the principles that have made the Internet such a success", said Vinton Cerf, co-inventor of the Internet's TCP/IP protocol.¹⁸⁷

Cited concerns of ISPs (wireline and wireless) have been rapid growth in file-sharing and video, and finite availability of spectrum. In broadband Internet markets where there is less competition (as in the US), Net neutrality is an important issue, but may be less of a concern where competition is greater and consumers have the choice to switch to another ISP that does not resort to Internet traffic filtering.

¹⁸⁵ See note 186.

¹⁸⁶ Berners-Lee, Tim (ibid.).

¹⁸⁷ The Economist (2010), <http://www.economist.com/node/16941635>.

III. Examples of Good Policies/Practices

Access to the Internet

Access to the Internet is crucial for benefiting from all of the opportunities connected with the Internet. As already mentioned earlier the importance of access to the Internet as an enabler of other human rights, and thus a right itself, has been proclaimed both by the UN Special Rapporteur on Freedom of Information and Expression as well as by the draft Charter on Human Rights and Principles for the Internet and others. The following will provide some more information on access to the Internet within the EU and some of its member states.

Legislative Approaches and Public Policies

Access to the Internet has become an emerging human right within the EU with a series of initiatives. Some of the most important steps are the European Directives, which provide for access to communications networks and services, including provisions for people with disabilities. According to these Directives, the EU is longing for achieving a Single European Information Space and an Inclusive Information Society. A fundamental precondition is that people are able to connect to the public communications network at a fixed location and at an affordable price without any constraints on the technical means. Accordingly, the EU member states should introduce in their national legislation the measures and the laws which comply with the provisions of the several European Directives, regulating various aspects of access and services.¹⁸⁸ The 2009 Directive also provides for implementing legislation upholding the rights of disabled end-users. Indirectly it is spelled out that people have a right to access to Internet.

Apart from the European Directives, some states have taken measures individually towards the recognition of the right to access to the Internet. Such states are Estonia, Greece, France, Finland and Spain.

In 2000, Estonia enacted the Telecommunications Act which provided for a universal service. The latter is a set of telecommunications services, and according to the Estonian Telecommunications Act, its universal service is “available and accessible to all subscribers who wish to have such access at a uniform price, regardless of their geographical location”.¹⁸⁹

¹⁸⁸ Directive 2002/19/EC of the European Parliament and of the Council of March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/20/EC (Authorisation Directive), Directive 2002/21/EC (Framework Directive), Directive 2002/22/EC (Universal Service Directive) and Directive 2002/58/EC (Directive on privacy and electronic communications), see Official Journal of the European Communities, 24.04.2002, p. 7, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0007:0007:EN:PDF>. In addition, Directive 2009/136/EC of the European Parliament and Council of 25.11.2009 amends a) Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, b) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and c) Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, see Official Journal of the European Communities, 18.12.2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF>.

¹⁸⁹ Estonian Telecommunications Act, Chapter 1, § 5, http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/estonia.htm.

Greece followed suit in 2001 with the amendment of its Constitution and the introduction of Article 5A which spells out the obligation of the state to facilitate the access to electronically transmitted information, the production, the exchange and the diffusion thereof.¹⁹⁰

In the case of France, the Constitutional Council with paragraph 12 of the relevant decision declared that “given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, the free communication of ideas and opinions enshrined in the Declaration of the Rights of Man and the Citizen of 1789 implied freedom to access such services”.¹⁹¹

In 2010, Finland amended its Communications Market Act with the provisions of Section 60 C declaring that broadband access is a basic right.¹⁹² Consequently, the universal service providers should provide every permanent residence and business office with access to a reasonably priced and high-quality connection.

In Spain ‘Act 2/11 of March 4, Sustainable Economy’ was the document which turned access to Internet into a right. Precisely, this Act added broadband access to its universal service and stated that ‘broadband connection at a speed of 1Mbit per second is to be provided through any technology’.¹⁹³

In Germany, a right to access as part of the right to the provision of the fundamentals of communication can be developed from two sources: first, the principle of the social state, which ensures everybody, in the jurisprudence of the German Constitutional Court, the “possibility to conduct relations with other people” and to “take part in the social, cultural and political life” of the state.¹⁹⁴ Second, Article 4 of the German Fundamental Law enshrines essential freedoms of communication which, in light of the emergence of the Internet, now encompass taking part in the communicative space through the Internet and thus presuppose access.

As can be seen from a recent study for OSCE, there are more countries in Europe, which have laws assuring access to the Internet.¹⁹⁵

However, despite the recognition of the right to access to the Internet (either by law or by jurisprudence) and the adoption of relevant policies and measures within the European Union, the Digital Divide still exists. Not everyone has access to Internet and Information Communications Technologies, let alone equal access. According to Internet World Stats, as of 31 December 2011, the levels of Internet penetration in the EU member states do range from 92,9

¹⁹⁰ Resolution of 06.04.2001 (G). In: Gazette A/17.04.2001 84, http://www.wipo.int/wipolex/en/text.jsp?file_id=224011#LinkTarget_3951.

¹⁹¹ Constitutional Council’s Decision No. 2009-580 of 10.06.2009, in the *Act Furthering the Diffusion and Protection of Creation on the Internet*, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf. The decision does not recognize access to internet as a fundamental right (a right for everybody to be connected) but says only that the restriction to the freedom of access to internet is a threat to the FOE.

¹⁹² Section 60 C, in: *Communications Market Act*, <http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf>.

¹⁹³ Boletín Oficial del Estado, ‘Disposiciones Generales: Ley 2/2011, de 4 de marzo, de Economía Sostenible’, documento BOE-A-2011-4117 in *Boletín Oficial del Estado*, No. 55, 05.03.2011, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-4117.

¹⁹⁴ German Constitutional Court (BVerfG), 1 BvL 1/09, judgment of 09.02.2010, para. 135.

¹⁹⁵ Organisation for Security and Cooperation in Europe (OSCE) (2011): The Office of the Representative on Freedom of the Media, Report on Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating states. Vienna. <http://www.osce.org/fom/80723>.

% for Sweden and 91,4 % for Luxembourg as the highest to 39,2 % for Romania and 46,9 % for Greece as the lowest ones.¹⁹⁶

The EU is working on overcoming these gaps in Internet penetration and, more generally, to bridging the Digital Divide.¹⁹⁷ Summing up, access to Internet and consequently to ICTs constitutes an emerging legal right and should be protected and promoted.

Digital Divide and Human Rights

In a survey of 27,000 people in 26 countries conducted for the BBC in 2010, 87 percent of users thought Internet access should be a “fundamental right of all people”.¹⁹⁸ Yet, more than two-thirds of the world’s population does not have access to the Internet and many of those do only have low speed access.

In addition to the growing democratisation of discourse spurred by the Internet in Asia, the explosion of wireless technologies opens up new opportunities for bridging the “last mile” problem of traditional telephony and thus narrowing the digital divide.

“A whole new development paradigm will be unleashed in the next few years in Asia”, according to Yoshio Utsumi, former secretary general of the International Telecommunications Union (ITU Telecom Asia 2002 summit, Hong Kong).¹⁹⁹ In many developing countries of Asia, the penetration of cellphones has already exceeded the penetration of landlines (Cambodia was the first country in the world to cross this threshold, in 1983).

A lot of data that is critically needed by the masses is in the public domain, and a number of technologies are emerging that can help bridge the critical “last mile” problem such as WLANs and satellite. But regulatory obstacles are holding back services like WiFi (wireless fidelity networks) and VoIP (Voice over Internet Protocol) in many developing countries of Asia, observes Heather Hudson, telecom professor at San Francisco State University.²⁰⁰

Universal access goals are also becoming moving targets, evolving from basic landline connectivity and wireless access to Internet and then broadband. Developing nations of Asia should prioritise these services and target user organisations such as healthcare, libraries, NGOs, schools and governments.

“Technology is moving in the right direction. Human brokers – for instance, for operating telecentres and providing wireless access on a shared basis – are very important in this regard for developing nations”, advises Hudson.

For developing countries, mobile media are the most important ICTs to date.²⁰¹ Mobile media have potential to bridge the digital divide in developing countries. Jonathan Donner²⁰² provides a detailed research review of how mobile media adoption and usage in developing countries

¹⁹⁶ Internet World Stats, Internet Penetration in Europe, <http://www.internetworldstats.com/stats4.htm>.

¹⁹⁷ European Commission Information Society, ‘European Broadband: Investing in Digitally Driven Growth’. In: *Europa*, http://ec.europa.eu/information_society/activities/broadband/index_en.htm.

¹⁹⁸ Elsayed-Ali, Sherif (2012), <http://www.egyptindependent.com/node/601891>.

¹⁹⁹ Techsparks: “Asia: Centre of the World's Wireless Explosion” <http://www.techsparks.com/Asia-Centre-of-the-World-Wireless-Explosion.html>

²⁰⁰ Rao (2003).

²⁰¹ Chen, Yi-Fan (2012). Mobile Theories and Frameworks. In: Bruck, Peter and Rao, Madanmohan (2012), *Global Mobile*. New Jersey: InfoToday Books.

²⁰² Donner, J. (2008). Research approaches to mobile use in the developing world: A review of the literature. *The Information Society: An International Journal*, 24, 140-159.

whereas Heather Horst and Daniel Miller²⁰³ and Nicholas Sullivan²⁰⁴ study how mobile media help the poor in developing countries.

Digital divide policies and projects are now included as part of wider action plans to harness ICT to benefit economies and societies. Development initiatives are now moving beyond top-down approaches and involve local partners and the business community. The private sector has slowly spread technology to middle income groups, and they now see the developing world and underserved populations as viable markets that require targeted products. Governments are realising the need to step beyond short-term demands of their constituencies, and provide a coherent, long-term plan for prosperity and effective ICT integration, along with a legal and regulatory framework that foster ICT use. All three trends need to be accelerated in order to bridge the divides with practical applications of technology and sound policy-making.

Citizen Expression: Smartphones and Digital Journalism

Thanks to a combination of mobile Internet and powerful photo/audio/video features, smartphones offer simple yet unobtrusive ways to record and edit video and audio, and deliver easily from the field, according to Stephen Quinn.²⁰⁵ They make it possible to film in places where camera crews are banned. Citizen journalism and crowdsourcing reporting are mushrooming because the technology is so easy to use and so common.

The Internet-enabled mobile phone is the latest in a series of technologies that journalists have embraced as newsgathering tools. Earlier examples include shorthand, the telegraph, the typewriter, the digital tape recorder, satellite phones and store-and-forward options on laptops for filing video from the field. But Internet-enabled phones are unique, and herald a new era in newsgathering and ability to circumvent the constraints of traditional broadcasting and restrictions of media regulations.

For the first time in 2011 the number of smartphones sold worldwide was higher than the number of personal computers. At least 85 per cent of new handsets can access the web, and by early 2012 at least 1.2 billion people were surfing the web from their mobile.

On 6 March 2012, the UK's Channel 4 News broadcast video secretly filmed by a Syrian hospital employee with his mobile phone, after severe fighting in Homs. A French photojournalist had smuggled the covert footage out of Syria. The mobile phone is also useful in situations where journalists' traditional cameras are confiscated.

The August 2011 riots in the United Kingdom provided countless examples of citizens using mobile phones to record the violence. One of the sites that received most attention during the riots was Citizenside (<http://www.citizenside.com>), a global citizen journalism site founded in 2006. The site says its goal is to create "the largest online community of amateur and independent reporters, where everyone can share their vision of the news by uploading photos and videos for fellow reporters to see". In November 2007, Agence France-Presse, the world's third-largest news agency, and the IAM company, became shareholders in the Citizenside agency (formerly Scooplive). The service created its own iPhone app and it is available from the iTunes store for free. The app is simple to use. Once installed, people can send photographs and video to Citizenside with a single click. As the site says: "Film news events from right inside the app, and send them to Citizenside in a single click".

²⁰³ Horst, H. and Miller, D. (2006). *The cell phone: An anthropology of communication*. New York, NY: Berg.

²⁰⁴ Sullivan, N. P. (2007). *You can hear me now: How microloans and cell phones are connecting the world's poor to the global economy*. San Francisco, CA: Jossey-Bass.

²⁰⁵ Quinn, Stephen. *Mobile Journalism*. In: Bruck, Peter and Rao, Madanmohan (2013-forthcoming), *Global Mobile: Scenarios and Strategies*. New Jersey: InfoToday/Perseus Publishing.

The UK's first dedicated citizen journalism news portal, The-Latest.com (<http://www.the-latest.com>), published numerous photographs and video of the riots, mostly taken with mobile devices. The riots started in the suburb of Tottenham. A search for "Tottenham" on Flickr.com shows scores of pages of pictures of the destruction in the streets. Some of the most vivid photographs were taken with the iPhone application Instagram (<http://instagr.am>).

Meporter, a location-based iPhone app for reporting local news, works by sharing geo-located text, photos and videos. It has a presence in the UK, US, China, Japan, Spain, and Italy. The application lets people write, photograph and video local news as it occurs.

The most prolific creators of mobile phone video are people aged under 30. In most countries in Asia, apart from Japan and South Korea, huge sections of the population are young. In Cambodia, half of the country's population is aged under 20. In Indonesia, 27 per cent of the population is younger than 14; in Malaysia it is 29 per cent. In the Middle East, more than 60 per cent of the population is aged under 25.²⁰⁶ This suggests opportunities for media organisations and freelancers who want to create sites for young mobile journalists.

Mobile phones are thus useful tools for social change agents and activists during the phases of research, engagement and participation. The tactical use of mobile phones can save lives during natural disasters, enable activists to monitor illegal logging, facilitate fundraising for NGOs, and help citizens report corruption and sign petitions. In this regard, mobile phones have been described as "people's media".²⁰⁷ The Tactical Technology Collective has documented a range of such examples of mobile activism: Ushahidi (documenting violence in Kenya), TXTpower (consumer rights group in the Philippines), International Centre for Accelerated Development (election monitoring in Nigeria), Women of Uganda Network (activism against gender violence), and Amnesty International Netherlands (signature campaign against torture).

Democracy Online: Information of, and Participation by, the Public

The Internet created new opportunities for the information and participation of the public which can be seen in the fast growth of the numbers of bloggers around the world, in the emergence of a new form of citizen journalism, reporting from every corner of the world and new instruments of democracy, for example e-voting, e-participation, e-government and e-democracy. NGOs which traditionally have been concerned with freedom of expression of the media and the situation of journalists now are concerned with bloggers and freedom of expression through the Internet.²⁰⁸

The purpose is the enlarged participation and involvement of citizens in public life and decision-making processes at all levels. In this way a more inclusive democracy based on wide public debates and larger scrutiny of decision-making processes should be achieved, which is part of the public service value of the Internet.²⁰⁹

The Council of Europe has also been active in this field as can be seen from his recommendation on electronic democracy (e-democracy) of 2009.²¹⁰ It also has worked out together with the Association for Progressive Communications and the United Nations Economic Commission for

²⁰⁶ Quinn, *ibid.*

²⁰⁷ Bahague, Rick and Banks, Ken (2008). *Mobiles in a Box: Tools and Tactics for Mobile Advocacy*, <http://mobiles.tacticaltech.org>.

²⁰⁸ E.g. Reporters without Borders, *Enemies of the Internet Report 2012*, <http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html>.

²⁰⁹ Council of Europe Recommendation CM/Rec(2007)/16 of 07.11.2007.

²¹⁰ Council of Europe Recommendation CM/Rec(2009)/1 on Electronic Democracy (e-democracy) of 18.02.2009.

Europe, which has been responsible for the Aarhus Convention on Information, Participation and Transparency in Environmental Decision-Making, a Code of Good Practice on Information, Participation and Transparency in Internet Governance.²¹¹ In this way the principles of e-democracy could also be applied to Internet governance itself.

Participation by all stakeholders is essential for the legitimacy of Internet Governance arrangements. To ensure the participation of individuals in the process is therefore an important task. But the long discussion on enhancing the democratic legitimacy of the UN by installing a UN Parliamentary Assembly²¹² has shown, it is still very difficult to organise individuals meaningfully beyond national organisational structures.

SOPA, PIPA, ACTA and beyond

Recent legislative efforts to fight violations of Intellectual Property Rights (IPRs) through increases of state competences to control user behaviour, both on a national and an international level, have led to a backlash from large parts of the Internet community. Proposed bills in the US – such as Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA) – led to an international mobilisation via the Internet, to real-life demonstrations and to virtual solidarity blackouts by some of the world's most-visited websites such as Wikipedia in January 2012. Other opponents included a range of Internet companies and human rights groups including Google, Yahoo, Wikipedia, Craigslist, Facebook, Twitter, LinkedIn, eBay, AOL, Mozilla, Reddit, Tumblr, Etsy, Zynga, EFF, ACLU, Human Rights Watch and Electronic Frontiers Australia (EFA).

They criticised the massive penalties and the criminalisation of activities such as uploading video clips of friends singing copyrighted songs that could be read into the language of the IPR protection bills.²¹³ In Asia, opponents to SOPA/PIPA emerged in a range of countries including Cambodia, on grounds that they would hinder Internet progress and limit online access to information in developing countries where the Internet can play an even more important role in the knowledge movement.²¹⁴ These protests resulted in the withdrawal of the controversial legislation before their adoption,²¹⁵ but they have not concluded the debate. The critique now is focused on the Cyber Intelligence Sharing and Protection Act (CISPA) before the US Congress, which is regarded as a major threat to freedom of expression and online privacy in the name of fighting cyber crime. Both the government and private companies would be authorized to monitor communications, and close down or block access to websites.²¹⁶

With the Anti-Counterfeiting Trade Agreement (ACTA), the debate on how to protect IRPs while ensuring Internet freedom was internationalised. ACTA²¹⁷ is an international trade agreement between the EU and non-EU states, including Japan, US and Canada, that aims to ensure the effective international enforcement of certain intellectual property rights. Conceived as a

²¹¹ See Code of Good Practice on Information, Participation and Transparency in Internet Governance (October 2010), <http://www.apc.org/en/node/11199>.

²¹² See Giving World's Citizens a Voice, Campaign for a United Nations Parliamentary Assembly (UNPA), <http://en.unpacampaign.org/index.php>.

²¹³ Sydney Morning Herald (2012), <http://www.smh.com.au/opinion/politics/planned-us-antipiracy-laws-a-draconian-mess-20120118-1q5z0.html>.

²¹⁴ VOA (2012), <http://www.voanews.com/khmer-english/news/US-Internet-Piracy-Bills-Find-Little-Support-in-Cambodia-137766413.html>.

²¹⁵ RT Network (2012), <http://rt.com/news/poland-acta-protest-anonymous-823/>.

²¹⁶ See Reporters without Borders, Draconian cyber security bill would lead to Internet Surveillance and censorship, Press Release of 06.04.2012.

²¹⁷ Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, Brussels, 23.08.2011, Doc. Nr. 12196/11, <http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf>.

complement to the WTO Agreement on Trade-Related Aspects of Intellectual Property (TRIPS),²¹⁸ it provides state parties with a number of obligations to be implemented into national law, notably with regard to effective enforcement of “any act of infringement of intellectual property rights” under ACTA.²¹⁹

The negotiations on ACTA started in June 2008 and were concluded in 2010. On 16 December 2011, member states authorised the Commission to sign ACTA, and agreed to sign and ratify it themselves. As this national ratification process started, civil society opposition grew. After some EU member states, with Poland in the lead, stopped plans for ratification, and demonstrations erupted in European capitals, the European Commission decided to ask the Court of Justice of the European Union for an advisory opinion on the consistency of ACTA with the Fundamental Rights Charter and other primary law-based fundamental rights guarantees on EU level.²²⁰

Though some of the more fierce criticism is misplaced, the vague wording (e.g. references to “fundamental principles such as freedom of expression, fair process, and privacy”²²¹ instead of ‘fundamental *rights*’) should invite critique, as should the high level of state autonomy in implementing surveillance in execution of ACTA.²²² Second, the protection of these rights is left to states, without ACTA providing for specific human or fundamental rights guarantees. Third, a number of provisions introduced in reaction to civil society protest already in 2008, such as the *de minimis* provision of Art. 14 (2) ACTA, are worded in a way that allows state parties to exclude application of ACTA,²²³ but again leaves this to states to decide.

The dynamics of the international mobilisation against ACTA and the success that these groups had is an interesting case study in international norm-making in the Internet age. Citizens in a number of (mainly European) countries protested against the government signing an international agreement which they considered to be tantamount to opening the door to Internet censorship. ACTA aims to protect copyright owners from online piracy and counterfeiting, but opponents branded it as an attack on civil liberties as it allows states to introduce intrusive measures, such as controls of digital devices at borders, and provides an argument for states should the wish to stronger police use activity by ISPs.

The European Parliament has also taken a very critical attitude on the Anti-Counterfeiting Trade Agreement (ACTA),²²⁴ negotiated by the European Commission largely without its participation

²¹⁸ Agreement on Trade-Related Aspects of Intellectual Property contained in Annex 1C to the WTO Marrakesh Agreement Establishing the World Trade Organization, 15.04.1994.

²¹⁹ Cf. Article 6 ACTA.

²²⁰ Cf. Statement by Commissioner Karel De Gucht on ACTA, 22.02.2012, <http://trade.ec.europa.eu/doclib/press/index.cfm?id=778>. He expresses the Commission’s opinion that “ACTA will change nothing about how we use the internet and social websites today – since it does not introduce any new rules. ACTA only helps to enforce what is already law today”.

²²¹ Article 27 (2), (3) and (4) ACTA.

²²² For a more comprehensive critique, see Opinion of European Academics on ACTA, http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opinion_110211_DH2.pdf. They do not, however, raise the question of the involvement of other stakeholders. See further Michael Geist, Assessing ACTA: My Appearance Before the European Parliament INTA Workshop on ACTA, 01.03.2012, <http://www.michaelgeist.ca/content/view/6350/125>.

²²³ Article 14 ACTA: Small Consignments and Personal Luggage

1. Each Party shall include in the application of this Section goods of a commercial nature sent in small consignments.

2. A Party may exclude from the application of this Section small quantities of goods of non-commercial nature contained in travellers' personal luggage.

²²⁴ Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, Brussels, 23.08.2011, Doc. Nr. 12196/11, <http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf>.

although it is the one to ratify the agreement in the end.²²⁵ Fears were expressed that copyright obligations could be given higher rank than human rights although the competent Commissioner for justice and fundamental rights clarified that the free access to the Internet and freedom of expression were rights which must not be restricted because of authors' rights.²²⁶

One lesson from ACTA is that a public outcry can lead to states rethinking the ratification of a treaty with a bearing on Internet rights. A further, important lesson for states is that the exclusion of civil society in the drafting process can seriously endanger the success of the international normative project. This bridges the gap to the argument for a multistakeholder approach to normative attempts to govern (aspects of) the Internet.

However, the critique of ACTA should not be interpreted as requesting the abolition of copyright altogether. Author's rights are human rights too. It is rather about the present system of protection which is considered not in line with requirements in the time of the internet. Accordingly, new business models are needed to find a new balance between freedom of expression and information and intellectual property rights.

225 Cf. European Parliament Resolution of 24.11.2010 on the Anti-Counterfeiting Trade Agreement (ACTA), P7_TA(2010)0432. But see European Commission, Transparency. ACTA is not a "secret" agreement, <http://ec.europa.eu/trade/tackling-unfair-trade/acta/transparency>.

226 Reding, Viviane (2012). Statement by Viviane Reding, Vice-President of the European Commission and EU Commissioner for Justice, Fundamental Rights and Citizenship, on freedom of expression and information via the Internet, attempts to block websites „three-strikes-law“, and ACTA, http://ec.europa.eu/commission_2010-2014/reding/pdf/quote_statement_en.pdf (13.02.2012) as well as directive 2009/136/EG (25.11.2009).

IV. ICT/Human Rights Issues for Working Groups

A. Freedom of Expression on the Internet

Cybercensorship and Press Freedom

A number of watchdog organisations now track restrictions on freedom of expression around the world (traditional and online), on a regular basis.²²⁷

As decades-old authoritarian regimes crumbled or eased their grip in countries such as Egypt, Tunisia and Libya, freedom of the press gained precarious new footholds in 2011, according to Freedom House's annual survey of freedom of the press around the world.²²⁸ For the first time in eight years, global media freedom showed no overall decline. Freedom House found that 40.5 percent of the world's peoples live in a "not free" media environment, while 45 percent had a "partly free" press and just 14.5 live in counties with a "free press".²²⁹

Countries like Syria have cracked down on ordinary citizens and journalists alike, imposing a blackout on any independent, non-state sponsored reporting, barring foreign reporters from entering the country, and even detaining and attacking journalists who try to cover protests against his oppressive regime. Britain was marked down slightly in the press freedom index for riot-related press restrictions, and legal "super-injunctions" that bar the media from reporting the very existence of an injunction against coverage of celebrities and wealthy individuals.

Reporters Sans Frontiers routinely publishes the global Map of Cybercensorship and tracks attacks as well as protective measures regarding journalists, such as criminal charges against a journalist who posted spy video of a politician online, new criminal code posing a threat to fundamental journalistic principles, new guidelines instructing police to respect and protect journalists, and breaches of freedom of information during elections.

Environmental activists and healthcare reporters have been arrested in some Asian countries, and some European countries are proposing bills allowing monitoring of all phone calls, text messages, emails and other electronic communications. In more positive developments, some Asian bloggers have won "Reporters Without Borders" category awards, and moves by telecom authorities to block Web sites have been checked by courts.

Reporters San Frontiers (RSF) also held a World Day Against Cyber Censorship (on 12 March 2011) to rally everyone in support of a single Internet without restrictions and accessible to all. "Never have so many countries been affected by some form of online censorship, whether arrests or harassment of netizens, online surveillance, website blocking or the adoption of repressive Internet laws", according to RSF.²³⁰ Hundreds of Netizens around the world are currently detained for expressing their views freely online. World Day Against Cyber Censorship is intended to pay tribute to them and their fight for Internet freedom.

Cyberactivism to Protect Freedom of Expression

One of the interesting developments accompanying the diffusion of the Internet is the use of the Internet itself to campaign against online censorship. For instance, a number of Web sites have

²²⁷ Reporters Sans Frontiers, <http://march12.rsf.org/en/#ccmap>.

²²⁸ YNet News (2012), <http://www.ynetnews.com/articles/0,7340,L-4223280,00.html>.

²²⁹ Relief Web: <http://reliefweb.int/node/497932>.

²³⁰ Reporters Without Borders, <http://march12.rsf.org/en/>.

been set up to protest against government-proposed Internet restrictions in countries like India, and many activist organisations use email campaigns and social media to advocate for a more open Net.

“Not since the institutionalisation of the postal service have we seen a communication development in society that can give power to individuals like this”, observe McCaughey and Ayers.²³¹ Forms of online activism can be either Internet-enhanced (eg. coordination of physical activities) or Internet-based (situated entirely online). Another categorisation of online activism is: awareness/advocacy (Web, email, encrypted documents), organisation/mobilisation (eg. “armchair activism” or “slacktivism” - online petitions and signature campaigns; lists of rallies and meeting places) and action/reaction (eg. “hacktivism” – taking down or defacing a Web site). Online activist equivalents of real-life strikes and boycotts have also emerged, eg. the “blackout” of Web sites such as Wikipedia for 24 hours to protest against SOPA.

Activist organisations are now using the Internet not just in “physical world” causes like environmental protection but also for purely online causes like free speech online, eg. Electronic Frontier Foundation. The Internet itself is emerging as a powerful recruiting tool for activist organisations. Organisations such as the global Association for Progressive Communications have been creating networks of like-minded NGOs around the world to support use of online tools in social movements.

Over the decades since its founding in 1961, Amnesty International’s tool portfolio has evolved from Gestetner machines and faxes to Webcasts and email campaigns. Challenges arise in managing the vast quantities of archived information via a user-friendly interface, and ensuring that sensitive information does not end up in the hands of repressive governments. “Ultimately, ICTs have become an integral part of Amnesty International’s strategy and commitment to the respect of international human rights”, according to Joanne Lebert, author of “ICTs and Human Rights Advocacy”.

Online Whistleblowing and Freedom of Expression

In some countries, whistleblowers who have exposed human rights violations have been imprisoned or placed under house arrest for years. Thanks to the global Internet, their cases have been made public much faster than before, and online campaigns have been launched to secure their release. Exiles can also use the Internet and online communities to continue to exert an influence back home.²³²

The controversial rise to prominence of whistleblowing site WikiLeaks in 2010-2011 has revealed new perspectives on online whistleblowing as freedom of expression. Many NGOs, academics and thought leaders consider government actions against Wikileaks as human rights violations. “Respect for freedom of expression and access to information means that any government is obliged to refrain from taking action against whistle-blowing sites and the individuals behind them. Taking legal action against WikiLeaks personnel or informers is a breach of responsibility to protect freedom of expression and civil rights”, according to the Association for Progressive Communications.²³³ A site like WikiLeaks can play a vital role in aiding the fight against corruption in governments and corporations.

APC has also expressed concern over actions taken by private companies such as EveryDNS.net which disabled the domain name system services for WikiLeaks.org, Amazon which repealed web

²³¹ McCaughey, Martha and Ayers, Michael (2003). *Cyberactivism: Online Activism in Theory and Practice*. New York: Routledge.

²³² Glanville, Jo (2012), <http://www.guardian.co.uk/commentisfree/2012/may/04/chen-guangcheng-exile>.

²³³ APC, <http://www.apc.org/en/pubs/briefs/wikileaks-human-rights-whistleblowers-under-attack>.

hosting services and Paypal which restricted access to WikiLeaks' account to prevent supporters from donating money.²³⁴

Article 19 joined free speech activists in a letter supporting Wikileaks and defending the right to publish leaked information in the public interest. "We assert that the right to publish is equal to, and the consequence of, the citizen's right to know. While we believe in personal privacy and accept a need for confidentiality, we hold that disclosure in the public interest is paramount. Liberty, accountability and true democratic choice can only be guaranteed by rigorous scrutiny", according to a statement by Article 19, International Federation of Journalists, and Reporters Without Borders.²³⁵

The WikiLeaks episodes have raised many issues related to freedom of expression, freedom of information, the profession of journalism, national security, privacy and ethical practices. Recognising this importance of online whistleblowing, UNESCO recently organised the conference "The Media World after WikiLeaks and News of the World".²³⁶ Journalists and citizens face challenges in dealing with the massive explosion of primary source data made available on the Internet. The global nature of the Net poses new challenges for international and domestic law related to privacy, national security, public order and Internet freedom. It also raises questions whether whistleblowing sites are 'partners' or 'intermediaries' of media – or media in their own right; and whether 'citizen journalists' need to follow the professional guidelines and ethics of their mainstream counterparts.²³⁷

Whistleblowers have fundamental rights consistent with the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Social Economic and Cultural Rights (ICESCR) and, constitutional protection in some democratic countries. While secrets are compatible with, justified, or even required under a democracy, keeping the public aware of the nation's agenda is vital for accountability between the state and civil society, according to James Von Geldern and Ezequiel Jimenez.²³⁸

Balancing Freedom of Expression and Hate Speech

Challenges can arise in balancing freedom of expression with freedom from discrimination, i.e. protecting free debate while not condoning hate speech, or promoting liberty without guaranteeing security. In the US, the government can restrict free speech except only if necessary to prevent imminent physical harm, while European courts are not so insistent on a tight causal link between speech and violence.²³⁹

Banning religious insult may not be the right approach since government officials are often not theological experts, and protests against such perceived offenses are held more for political reasons by opportunist parties. Governments such as those of Singapore protect a culture of

²³⁴ APC, <http://www.apc.org/en/pubs/briefs/apc-says-stand-wikileaks-stand-freedom-information>.

²³⁵ Article 19, <http://www.article19.org/resources.php/resource/1755/en/supporting-freedom-of-speech-and-wikileaks>.

²³⁶ UNESCO, <http://www.unesco.org/new/en/communication-and-information/events/calendar-of-events/events-websites/the-media-world-after-wikileaks-and-news-of-the-world/>.

²³⁷ Inform, <http://inform.wordpress.com/2011/02/02/news-freedom-of-information-in-the-wikileaks-era-is-the-whistleblowing-site-doing-more-harm-than-good-asks-panel-judith-townend/>.

²³⁸ Von Geldern, James and Jimenez, Ezequiel, http://macalester.academia.edu/EzequielJimenez/Papers/1036694/Diplomatic_Scandals_Leaks_and_Secrets_The_Case_of_Wikileaks.

²³⁹ Cherian, George (2011). Why Hate Speech Does Not Always Require the Red Card, http://www.straitstimes.com/BreakingNews/Singapore/Story/STIStory_740765.html.

tolerance and arrest 'hatemongers' on the Net, though some politicians also advocate that breaches be handled through mediation instead of government intervention.²⁴⁰

It is recommended that religion, spirituality and philosophy should be open to debate, and concepts like 'defamation' not be extended to a religion – while at the same time working towards a culture peace between religions. Practices like blasphemy are better dealt with by community initiatives, and not converted into censorship via criminal code. Instruments such as CERD (Convention on the Elimination of All Forms of Racial Discrimination) are better suited to deal with stereotyping of religions.²⁴¹ While there are unfortunately some problems with inter-religious relations between countries, censorship of the Internet is not a progressive solution.

One of the online services which unfortunately is becoming a victim of hate speech is anonymous access services, as well as anonymous postings on news sites. Anonymity on the Internet has been one way of providing a conduit for expression for activists living under repressive political climates. But some newspapers and social media sites, for instance, are announcing that anonymous online comments on their sites will no longer be allowed since they may be exploited as forums for hate speech and racism.²⁴²

However, the impact of hateful and cruel content online should not be ignored or underestimated, especially in cases where it has spurred hateful actions or even suicides. A balance should be struck between freedom of expression and its likely consequences, between rights and costs (in terms of human lives lost or harmed).²⁴³ The Internet has a double-edged sword characteristic for children: providing many opportunities for learning while exposing children to potentially negative content. From the point of view of child safety, the Internet has negative aspects such as violent games, pornography, hate sites, and predators.²⁴⁴

Legislative approaches in countries such as the US have been the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (Neighborhood Act). Solutions such as Internet filters have been proposed (eg. Cyber Patrol, Net Nanny, Cyber Snoop), though they have their limitations. There has also been concern about hate speech in game communities, i.e. in-game chats that marginalise different groups: Muslims, African Americans, gays, and women. Online game communities should work towards creating a more welcoming and sensitive environment for players of every stripe.²⁴⁵

In sum, free speech advocates should not merely say that the Internet is 'uncontrollable' and hate speech bans on the Internet are therefore 'ineffective', but propose ways of dealing with hate propaganda. Education, community vigilance and grassroots forums are some proposed solutions.

²⁴⁰ Wong, Gillian. Singapore Jails Bloggers for Racist Speech, <http://forums.yellowworld.org/archive/index.php?t-26498.html>.

²⁴¹ Cherian, George (2012). A conversation with UN Special Rapporteur Frank La Rue, <http://hatespin.weebly.com/la-rue.html>.

²⁴² Gross, Josh Gross. Newspapers Begin Move to Eliminate Anonymous Comments, <http://www.boiseweekly.com/CityDesk/archives/2011/08/31/newspapers-begin-move-to-eliminate-anonymous-comments>.

²⁴³ Cohen-Almagor, Raphael. Countering Hate on the Internet, <http://ojs.ubvu.vu.nl/alf/article/view/138/264>.

²⁴⁴ Cho, Chang-Hoan and Cheon, Hongsik John. Children's exposure to negative Internet content: effects of family context, http://findarticles.com/p/articles/mi_m6836/is_4_49/ai_n25120984/.

²⁴⁵ Tan, Philip (2011). Hate Speech in Game Communities, http://gambit.mit.edu/updates/2011/03/hate_speech_in_game_communitie.php.

European Support to Freedom of Expression Worldwide

Several European countries and the European regional organization Council of Europe, the European Union and OSCE have supported international action to promote freedom of expression in Europe and worldwide. The Council of Europe has adopted numerous pertinent resolutions and decisions starting from the Committee of Ministers Declaration on freedom of Communication on the Internet in 2003 to the Declaration on Measures to Promote Respect of Article 10 of the European Convention on Human Rights of 2011.²⁴⁶ The European Court of Human Rights has already developed a significant case law around the internet.²⁴⁷ The OSCE Representative on Freedom of the Media also engages into "Internet Freedom"²⁴⁸ in the 56 countries belonging to the OSCE and the European Union is likewise committed.²⁴⁹ Among European states, Sweden has taken a lead in promoting freedom of expression on the internet, which is visible in its support to the UN Special Rapporteur on Freedom of Opinion and Expression, when preparing its pertinent report, by hosting the European Dialogue on Internet Governance (EuroDIG) in June 2012 and relevant initiatives in the UN Human Rights Council, but also towards ICT companies.²⁵⁰ This can be considered as examples of good practice in the struggle for human rights in the Internet.

B. Privacy

Protection of Privacy and Data Protection

One area, where the effect of the new ICTs on human rights is strongly felt, is the area of privacy and data protection, raising the issue whether this has led to a (re)definition of the human right to privacy with regard to the information society.

The Data Retention Directive of the European Union and ACTA, as well as SOPA, PIPA and CISPA (Cyber Intelligence Sharing and Protection Act) together with new policies of Facebook and Google, which want to make better use of the data of their users for commercial purposes, have recently stimulated a new public debate on the protection of privacy and data protection. Although it could be argued that in particular the young generation is less concerned with privacy today because it is openly sharing a lot of information on itself through the Internet,²⁵¹ the new technical possibilities have created new threats to the privacy of the individual, which is eroded both from the state collecting more and more data about its citizens and by connecting them as well as from the side of business, which is commercialising the data it is legally or sometimes even illegally collecting. The decreasing costs of storage allowing of more data collection and the increased use of ever more sophisticated data mining tools thus combine to endanger privacy as never before. For example, Google has informed users that it intends to match all the data of the users of its different services, obviously for the purpose of selling profiles of the preferences of its users, which has led to an uproar in civil society circles.

Other concerns relate to privacy at the workplace, where according to laws and court decisions employers must not read personal e-mail of their staff²⁵² and with regard to privacy of consumers

²⁴⁶ See Kettemann (2011). Op. cit.

²⁴⁷ See European Court of Human Rights, Internet: Case-law of the European Court of Human Rights, Council of Europe, Strasbourg, June 2011.

²⁴⁸ OSCE Representative of the Media, Internet Freedom, Why it Matters, www.osce.org/fom.

²⁴⁹ See European Parliament resolution on freedom of expression on the internet of 06.07.2006.

²⁵⁰ Government Offices of Sweden, Enhancing Internet Freedom and Human Rights Through Responsible Business Practices, Ministry for Foreign Affairs, Stockholm 2012.

²⁵¹ Though this is due mainly to changing notions of privacy. Cf. Rössler, Beate (2004), *The Value of Privacy*, Cambridge: Polity.

²⁵² Cf. Privacy Rights Clearinghouse, Fact Sheet 7: Workplace Privacy and Employee Monitoring, <http://www.privacyrights.org/fs/fs7-work.htm#4a>.

data in general, which has recently been addressed by a publication of the White House on a possible “Consumer Privacy Bill of Rights”.²⁵³

However, privacy, issues can also be raised by activities of hackers or digital activists, who make private data available on the Internet for what they consider as public interest as demonstrated by “Anonymous”, or whistle blower websites like “Wikileaks” or “Openleaks”.

International Legal Regulations Governing Privacy and Data Protection

The protection of privacy and data protection are human rights contained in several international human rights conventions and in national law. On the global level Art. 12 of the Universal Declaration on Human Rights protects the right to privacy as does Art. 17 of the International Convention on Civil and Political Rights. On the regional level, the European Convention on Human Rights in Art. 8 protects the right to family life and privacy subject to certain limitations in the public interest. With regard to the European Union, Art. 7 of the EU Charter on Fundamental Rights recognises the right to privacy and Art. 8 the right to protection of personal data. This comprehensive provision also requires that data must only be processed in a bona fide way for determined purposes and with the consent of the person concerned or on a legitimate basis foreseen by law. Every person has the right to be informed about any data collected on her and to seek the correction of such data. It also foresees the supervision of these obligations by an independent authority.

Over time a number of specialised legal instruments have been adopted with regard to the protection of privacy and data protection, which are partly relevant beyond Europe like the OECD-Guidelines on Protection of Privacy and Transborder Flows of Personal Data of 1980 or the Council of Europe Convention for the Protection of Individuals with regard to automatic processing of personal data of 1981 and the European Data Protection Directive of 1995. The European Union has an independent European Data Protection Supervisor. The European E-Commerce directive is also relevant as it spells out the obligations and rights states need to implement for those involved in e-commerce. As already reported above, a revision of the data protection rules is currently underway in the EU and the European Commission has made proposals for a new directive and a new regulation in this respect.²⁵⁴

On the international level, the issue of privacy in the Internet has attracted particular attention in the recent years. Examples of documents outlining the challenges and providing for standards to overcome them include the Madrid Privacy Declaration adopted in 2009 and the “Rome Memorandum” on Privacy in Social Network Services.²⁵⁵ The Madrid Privacy Declaration notes with alarm the dramatic expansion of secret and unaccountable surveillance and also that new strategies to pursue copyright and unlawful content investigations are posing substantial threats to communications privacy, intellectual freedom and due process of law. It shows itself concerned also with the fact that some corporations are acquiring vast amounts of personal data without independent oversight. It sees a danger of fusion of data between the public and private sectors and warns that failure to safeguard privacy may jeopardize associated freedoms including the freedom of expression. It therefore requests support for independent data protection authorities

²⁵³ See White House, Consumer Data Privacy in a Network World, <http://www.whitehouse.gov/sites/defaults/files/privacy-final.pdf>. See also the publication of the “Federal Trade Commission on “Protecting Consumers in an Era of Rapid Change”, <http://www.ftc.gov/os/2012/03/120326/privacyreport.pdf>.

²⁵⁴ See supra, at p. 38.

²⁵⁵ International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services - „Rome Memorandum“ – of 04.03.2008. This Working Group was initiated by data protection commissioners from different countries in order to improve privacy and data protection in telecommunications and media; see <http://www.berlin-privacy-group.org>.

and for genuine privacy enhancing techniques. It requests countries to ensure that individuals are promptly notified when their personal information is improperly disclosed or used in a manner inconsistent with the states goal of collection and calls for the establishment of a new international framework for privacy protection with the full participation of civil society, based on the rule of law and respect for fundamental human rights.²⁵⁶

It might be true that the Western concepts of privacy are more individualistic than Asian or African communal traditions, but this does not mean that they are inappropriate in the African or Asian context.²⁵⁷ This can be seen, for example, from the regional consultations meetings, the Special Rapporteur on the Freedom of Opinion and Expression, Frank La Rue, had in preparing his report for 2011, which had a focus on freedom of expression and the Internet, including also issues of privacy and data protection in this context. The report on the consultations finds that the main problem is that many people are unaware of their privacy rights. The perception of privacy being a Western concept, alien to Asia and not in line with local values was considered by local participants as a convenient myth, while surveillance practices and data mining proliferate in the absence of adequate legal protection of citizens.²⁵⁸

Therefore, the various challenges to the right to privacy outlined in this chapter are very much the same in the North and in the South and are also discussed in a very similar way as could be seen during the Arab spring. States, generally, are more keen to emphasise duties and limitations as can already be seen from the Geneva Declaration of WSIS I in 2003, where para. 4, which emphasises the right to freedom of opinion and expression and participation in the Information Society, corresponding to Art. 19 UDHR, is immediately followed by the full text of Art. 29 UDHR, reaffirming duties to the community and possible limitations (para. 5).

As part of the right to the protection of personal data, the Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data already foresees “the right that such data be processed fairly and securely for specified purposes on a legitimate basis only, and that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data which have been processed without right”.

Some larger violations of data protection also fall under the European Convention on Cybercrime, For example, the intentional access to, interception of, and interference with computer data without the right to do so is a punishable offense.²⁵⁹ Special provisions exist with regard to the protection of personal health data including the right to be informed of, and the consent or not to any collection in processing of such data.²⁶⁰

The Parliamentary Assembly of the Council of Europe in 2011 has adopted a resolution and a recommendation in respect of privacy on the Internet: In its resolution, which was prepared by a multi-stakeholder process at the Internet Governance Forum 2010 in Vilnius, nine general principles for the protection of privacy and personal data in the ICT environment were identified, among them the obligation of states to provide an adequate legal framework for such protection against interference by public authorities as well as by private individuals and entities and the right of everyone to be able to control the use of their personal data by others including the right

²⁵⁶ Ibid.

²⁵⁷ Compare, for this debate, Tim Unwin, ICTs, Citizens, and the State: Moral Philosophy and Development Practices. In: Electronic Journal on Information Systems in Developing Countries (2010), 44, 1, 13.

²⁵⁸ See Freedom of Expression and the Internet, Report from Regional Consultation Meetings Convened by Demos, Lisa Horner on behalf of Global Partners and Associates, March 2011, <http://www.mediapolicy.org/Demos-FoE-Internet>.

²⁵⁹ See Arts. 2-4 of the Council of Europe Convention on Cybercrime of 2001.

²⁶⁰ See European Convention on Human Rights and Biomedicine and Additional Protocol to this Convention concerning Genetic Testing for Health Purposes of 1997.

to know and rectify as well as to erase them from ICT systems and networks, the principle of prior consent regarding the use of personal data can be subsequently withdrawn at any time and the right to be informed of a concrete commercial exploitation in advance.²⁶¹

A higher level of protection shall be provided for private images, personal data of minors or persons with mental or psychological disabilities, personal ethnic data, personal medical, health or sexual data, and biometric or genetic data. Periods should be specified beyond which such data shall no longer be kept or used. Public and private entities which collect, store or process personal data should be obliged to reduce the amount of such data to the absolute minimum necessary. Personal data should be deleted when they are outdated or unused. The random collection and storage of personal data should be avoided. Everyone should have an effective remedy against an unlawful interference with his or her right to protection of privacy and personal data before domestic courts.²⁶²

Accordingly, the concerns about privacy and data protection have increased in the recent years in Europe, the United States and also globally although it might be true that in certain circumstances in some African or Asian states the concern for privacy may be seen as less relevant than the economic gains expected from increased data usage, storage and mining. A case in point is the introduction, in India, of a “universal identity number” (UID) to be tied to biometric markers, which are supported widely even amid data protection and privacy concerns.²⁶³

Data Retention and Exchange for Anti-Terrorist and Security Purposes

Major inroads into the right to privacy and data protection have been made as a result of the so-called “war against terrorism”.²⁶⁴ For example, the Data Retention Directive of the EU²⁶⁵ or the Passenger Name Record Agreement between the European Union and the United States and other data exchange agreements were largely inspired by security concerns.²⁶⁶ There is the issue of so-called “deep packet inspection” (DPI), which allows to analyse data packets for network security or copyrights purposes, but is also used for censorship, for example by key word filtering.²⁶⁷ On the other side there is little information how useful the collection of so many data has been in the end while there are a number of reports that data actually collected could not be processed in a proper way in order to prevent attacks. There is a need for a balance between security and privacy, which builds on the principle of proportionality in applying possible restrictions, while maintaining an open Internet.²⁶⁸

In this context, the Special Rapporteur on the Right to Freedom of Expression noted insufficient or inadequate data protection laws in many states and increased pressures by states on private

²⁶¹ See Council of Europe, Parliamentary Assembly, Res. 1843 (2011).

²⁶² Ibid.

²⁶³ The Economist, Identifying a billion Indians, 27.01.2011, <http://www.economist.com/node/18010459>.

²⁶⁴ Cf. Benedek, Wolfgang (2004). Human Security and Prevention of Terrorism. In: Benedek, Wolfgang and Yotopoulos-Marangopoulos, Alice (eds.), Anti-Terrorist Measures and Human Rights, Leiden/Boston, Nijhoff, 171-184.

²⁶⁵ Op. cit.

²⁶⁶ Cf. Nino, Michele (2010). The protection of personal data in the fight against terrorism. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon, Utrecht Law Review, Vol. 6, Issue 1 (January) 2010, <http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/115/115>.

²⁶⁷ See Wagner, Ben. Deep Packet Inspection and Internet Censorship: International Convergence on an “Integrated Technology of Control”. In: Advocacy, Global Voices Online, <http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf>.

²⁶⁸ See European Parliament, Study on Information and Communication Technology and Human Rights, by Horner, Lisa, et al on behalf of Global Partners (2010), 41 et seq.; EXPO/B/DROI/2009/24.

actors to provide information of their users. Cloud computing services requiring the storage of information at third sites also have to adhere to strict data protection guarantees.²⁶⁹

With regard to limitations, it might be noted that the ICCPR, different from the European Convention on Human Rights, does not foresee any grounds for restrictions on privacy whereas restrictions are possible for freedom of expression grounds, including for the respect of the rights and reputation of others and in the public interest.

As a recent European example, the “Communication Development Capability Programme”, proposed by the UK Government, which should give the police access to e-mail and social media traffic data of individuals to investigate serious crime and terrorism has been criticised by civil liberties organisations. Also a spokesperson for the European Commission has commented that it might potentially be incompatible with the right to privacy. Another bill, the “Draft Online Safety Bill” would force Online Service Providers to block pornographic sites, if the user over 18 has not actively opted in by informing the ISP of his consent to subscribe to a service that includes pornographic images.²⁷⁰

Informational Self-Determination and Virtual Personality

The right to informational self-determination and the protection of the virtual personality are at the basis of all privacy and data protection regarding the Internet. For example, the protection of the virtual personality, according to the draft Charter on Human Rights and Principles for the Internet requires that digital signatures, usernames, passwords, PIN- and TAN-codes must not be used or changed by others without the consent of the owner. Standards of confidentiality and integrity of IT systems need to protect the right to privacy. The draft Charter also identifies the freedom from surveillance according to which everyone has the freedom to communicate without arbitrary surveillance or interception (including behavioral tracking, profiling, or cyber-stalking) or the threat of surveillance and interception. Furthermore every individual has the right to communicate anonymously on the Internet and to use encryption technology for that purpose. Obviously, governments are not all too happy with that provision. The right to digital data protection according to the draft Charter contains a number of obligations of data collectors in particular regarding transparency of the use of that personal data, whereas the individual must maintain the right to exercise control over its personal data. For this purpose minimum standards are proposed like that data collectors have an obligation to seek the active consent and notify people when their information has been forwarded to third parties, abused, lost or stolen.²⁷¹

New Challenges to Privacy from Technology

There are new challenges to privacy which come from technological developments like cloud computing and the Internet of Things with its objects that communicate via RFID chips. Most of these have not as yet been resolved in a satisfactory way. Growing concerns relate to governmental demands for data from Internet Service Providers (ISPs) and so-called “data-mining” undertaken by business as well as by security services. Special protection needs relate to the privacy of children and minors against cyber-bullying, grooming, sexting etc.

²⁶⁹ Report by the Special Rapporteur on Freedom of Opinion and Expression, La Rue, Frank, UNGA-Doc. A/HRC/17/27 of 16.05.2011, paras. 53 et seq.

²⁷⁰ EDRI (European Digital Rights) – gram newsletter – Number 10.7 of 11.04.2012.

²⁷¹ See Internet Rights and Principles Coalition, Draft Charter of Human Rights and Principles for the Internet, <http://internetrightsandprinciples.org/node/367>.

Some of the challenges to privacy, which have the potential to substantially alter the behaviour of Internet users is **location privacy**. Increasingly, mobile networks and smart phone applications allows users to communicate their location to others – and the police to find them. While allowing police access to location data in real time (or to location data records) in cases of serious crimes is essential for public safety, misuses can lead to human rights violations. Access to location data records needs to be tightly controlled and requests from police should pass through independent judges and, ideally, be submitted a stringent necessity test.

The increased use of **video surveillance** (CCTC) partly precedes the Internet. But services such as YouTube and the Google Street View have substantially enlarged the availability of audiovisual recordings and the human rights challenges involved. In several states, Google Street View has been stopped because of privacy concerns. In a recent case Google has been fined US \$ 25.000 for impeding US investigations in its Street View Project by the Federal Communications Commission.²⁷² In others, individuals can request their property to be less clearly visible. This request mirrors those of states that have requested to have their military installations blocked out. Google Maps also uses old imagery or imagery reduced in resolution of certain conflict zones, including Sri Lanka, Israel and Afghanistan.²⁷³

As the example of India's biometrical ID number scheme has shown, collecting **biometrical information** can have serious human rights implications. At the same time, biometrics-based security documents allow for safe and easy travel and communication. Here again, a balance has to be struck between the responsibilities of the state and private companies collecting the data and its usage in conformity with the right to privacy.

New Conceptions of Privacy?

The right to privacy which was originally conceptualised as privacy of letters as the classical form of correspondence gains a different meaning in cyberspace. What some people consider private, that is: meant only for a limited audience, no longer actually is private in the Internet. The dissonance between what is meant to be private but is actually available for all the world to see has not yet been fully incorporated in the modes of thinking of the young generation. A large symposium in Austria looking at the development of the information society from different angles has been entitled "Goodbye Privacy?"²⁷⁴ Freedom of expression is linked to privacy in various ways because it covers also the private expression.

Generally, the question can be asked whether we observe an erosion of privacy or rather a new awareness for privacy concerns. The Declaration of Principles of the World Summit on the Information Society largely neglected privacy concerns as privacy is mentioned only in the context of confidence and security in the use of information and communication technology. However, during the Internet Governance Forum privacy is regularly discussed together with data protection in the context of security and openness, but also as a cross-cutting issue. There is also a Dynamic Coalition on Privacy animated by NGOs focusing on privacy like the Electronic Privacy Information Center (EPIC) or Privacy International.²⁷⁵ As already indicated, the Global Network Initiative has as one of its main concerns the protection of privacy and did develop pertinent principles and guidelines. However, in view of recent decisions of Google it can be questioned to what extent these principles and guidelines are observed in their own practice. It is clear that the human rights to privacy and data protection often seem to stand in the way for Internet companies of a

²⁷² See the Guardian of 17.04.2012.

²⁷³ Cf. Geens, Stefan. Google Earth conspiracy watch – Sri Lanka war edition, <http://ogleearth.com/2012/03/google-earth-conspiracy-watch-sri-lanka-war-edition/>.

²⁷⁴ See for the documentation <http://thenextlayer.org/GoodbyePrivacy>.

²⁷⁵ See Electronic Privacy Information Center, www.epic.org and <https://www.privacyinternational.org>; See also its "PrivAsia Project", which conducts research on privacy and security, builds capacity for local organisations and briefs policy makers of several Asian countries on privacy and technology policy issues.

more commercial use of their customer's data. It is only logical therefore that the various recommendations and guidelines of the Council of Europe like the guidelines regarding human rights and search engines²⁷⁶ or social networks²⁷⁷ also contain privacy concerns.

Individuals navigating on the Internet are usually addressed as "users". They should rather be empowered as "participants" in the building of human rights-based, people-centred, development-oriented information society for all, in particular regarding their rights, including privacy rights. The improvement of "user's rights" is a major concern of the Council of Europe's newly established "Committee of Experts on Rights of Internet Users" which is to assist in the implementation of the Council of Europe Internet Governance Strategy related to maximising rights and freedoms of Internet users.²⁷⁸

Remedies Against Violations of Privacy

The obligation of states is to protect against violations of privacy and data protection both from the state and private companies. For this purpose companies can be forced to observe certain privacy policies and provide privacy settings which are easy to handle. This raises the question of self-regulation as it is the practice mainly in the United States or state regulation, which is rather the European approach or co-regulation as it is proposed by the recommendations of the Council of Europe.

Recently, the European Commissioner for Justice and Human Rights, Viviane Reding, has called for a new "gold standard in data protection".²⁷⁹ The background to this call is the divergence between US privacy principles and EU privacy law. The cooperation in mutual data transfer since 2001 has shown that a common denominator and common legal standards are urgently needed.

Interestingly, Commissioner Reding also requested that the new data protection law of the European Union should include a "right to forget", a right that is inherently difficult to implement. A right to delete has also been requested in the scientific debate.²⁸⁰ Furthermore, Commissioner Reding also came out in support to the principle of explicit prior consent as a requirement for personal data processing. According to her, the revised data protection laws should also apply to cloud computing, i.e. storage of data in a cloud, which can be anywhere.²⁸¹ Companies need to respect the rules on privacy and data protection, and states must provide quick, effective remedies for violations, in keeping with the principles of due process and fair trial. A human rights-sensitive approach to data protection also requires special means of protection of children and minors. Users must have full control over their data, in particular their privacy settings. Encryption should be allowed. In this way, the confidence of the users in ICTs can be preserved.

²⁷⁶ See Draft Recommendation CM/Rec. (2012) 3 of the Committee of Ministers on the protection of human rights with regard to search engines, adopted on 04.04.2012, [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2012\)3&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)3&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383).

²⁷⁷ See Draft Recommendation (CM/Rec. (2012) 4) of the Committee of Ministers on the protection of human rights with regard to social networking services, adopted on 04.04.2012, [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2012\)4&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)4&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383).

²⁷⁸ See Council of Europe Internet Governance Strategy 2012-2015, op. cit.

²⁷⁹ Reding, Viviane (2012). Speech for the EU-Conference: Privacy and Protection of Personal Data, Washington/Brussels, 19.03.2012, speech/12/...

²⁸⁰ See Mayr-Schönberg. „Delete“, supra note.

²⁸¹ Reding, Viviane (2011). Explicit prior consent needed for personal data processing, 08.11.2011, <http://www.out-law.com/en/articles/2011/november/explicit-prior-consent-needed-for-personal-data-processing-eu-commissioner-says/>.

Accordingly, there is a need to sharpen existing standards and to enforce them in practice by independent institutions, like data protection authorities or the courts. Social networks and business in general must show that they are serious about self-regulation. However, states or the European Union which need to respond to the demands of users too, have to provide an appropriate legal framework and ensure that a recourse to legal remedies exists in cases of self-regulatory 'market failure'.

Privacy Rules for Social Networks

With regard to social networks, the challenge is what data about users should be publicly available. For example, should also mobile phone numbers or home addresses appear on profiles? Should it be upon the companies to decide this? Should companies be forced to stop their users from oversharing? Already now companies face the challenge that transmission of personal user data to advertising companies may be illegal. There is also the question whether making user location data generally available to others should not be restricted. In any case users have to be made aware of what happens with their data in particular if there are any data losses. The settings need to be privacy friendly and at least the account has to be easy to delete. There should be full transparency on data retention and on targeting and selling profile information. If users delete data, this data must also be deleted from the companies' servers. All companies that store user data (and that is practically all companies active on the Internet) need to hire or consult with privacy officers who ensure that their business practices do not violate data protection laws.

Facebook Europe is confronted with a complaint by an Austrian student, Max Schrems, who challenged the privacy policy of Google Europe at its seat in Ireland with some limited success.²⁸² After an important deadline for Facebook to change some of its policies, he is now planning to use the European Commission to enquire into Facebook's data usage practices.²⁸³ Facebook had already made improvements to privacy settings in August 2011 giving users more control over their privacy.²⁸⁴

There is also a dialogue by the German voluntary self-control mechanism for multimedia service providers with several social networks including Google+, Facebook and LinkedIn towards a new code which should improved data protection for users, in particular the youth.²⁸⁵

Data Privacy in Asia

Asia Pacific Privacy Authorities (APPA)²⁸⁶ is the principal forum for privacy authorities in the Asia Pacific Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. APPA convenes twice a year, discussing permanent agenda items like jurisdictional reports from each delegation and an initiative-sharing roundtable. Topical issues canvassed by forums have included privacy and security, cross-jurisdictional law enforcement in the Pacific Rim, privacy legislation amendments, cryptography and personal data privacy. APPA was formerly known as PANZA and PANZA+ (Privacy Agencies of New Zealand and Australia plus Hong Kong and Korea).

²⁸² Cf. the initiative Europe v. Facebook, <http://europe-v-facebook.org/EN/en.html>.

²⁸³ Cf. Ibid.

²⁸⁴ See Facebook Changes Privacy Options, BBC News Technology, 23.08.2011, <http://www.bbc.co.uk/news/technology-14633427>.

²⁸⁵ Heise Online, 06.04.2012.

²⁸⁶ <http://www.privacy.gov.au/aboutus/international/appa>

Graham Greenleaf²⁸⁷ surveys data privacy legislation developments across Asia, terms of strength of protection provided by each law: existence of a data protection authority (DPA); ability of individuals to obtain financial compensation; data export prohibitions; and data breach notification requirements.

In 2009 there were seven jurisdictions in the region which had enacted data privacy laws (New Zealand; Hong Kong; Taiwan; Australia; South Korea; Japan; Macau), later joined by India and Malaysia. Australia, Japan, and South Korea first introduced data protection laws covering the public sector. Korea's 2001 Act was strengthened beyond in 2004 in relation to data breaches and data exports; its Data Protection Act of 2011 regulates all data processors, public and private, by one Act. It also covers representative lawsuits by consumer organisations, consent for collection and use of sensitive data, notification to data subjects of the source of personal data, and Privacy Impact Assessments (PIAs) for data protection in the public sector.

Japan has had an Act on the protection of personal information held by public sector agencies since 1988; a separate Act covered the private sector in 2003. But Japan has one of the weakest data privacy laws in Asia, according to Greenleaf²⁸⁸. In China, the Amendment to the Criminal Law of the PRC (February 2009) criminalises a wide range of disclosures of personal information. Data privacy provisions have also been included in sectors like medical records, insurance, and credit reporting.

India's IT Act 2000 was amended in 2008 to include data privacy regimes. There are also rules on data exports in the context of outsourcing contracts. Enforcement of complaints is through a Cyber Appellate Tribunal (CAT). There are also proposals for a Data Protection Authority of India (DPAI) and provisions for freedom from surveillance, and protection of personal data.

In Southeast Asia, Singapore has announced its intention to introduce a private sector Bill in 2012, and legislation drafts are at early stages in Thailand, Philippines, and Indonesia. Asia's data privacy measures seem to be influenced by The European Union's privacy Directive and OECD Privacy Guidelines. The APEC Privacy Framework has also come up with some principles, and serves as a forum for data privacy discussion for some member countries (which do not include countries such as India).

Some Conclusions

In conclusion there is a need to (re-)conceptualise privacy as empowerment – as returning the power of what happens with personal data to the people to whom the data belongs. Increasing data awareness is a first step. Information, transparency and accountability regarding privacy and data protection is an obligation for both the state and business although the responsibilities differ in the implementation. The general baseline should be the “do no harm-principle”. The Ruggie Framework and principles could be meaningfully applied also in this context. Human rights as the right to privacy and data protection are not only obligations of states but also of private entities and citizens. The empowerment of the users should encompass decisions on the privacy settings and the use of their data. This is part of their right to informational self-determination and their freedom of choice.

If these rights and principles are not respected by governments or business this has a chilling effect on the use of ICTs and results in a loss of confidence detrimental to the Internet. Therefore self-restraint is needed by business and the state together with clear rules. Strong independent monitoring authorities are to ensure the implementation of these rules as self-regulation is not

²⁸⁷ Greenleaf, Graham (2011). Asia-Pacific Data Privacy: 2011, Year of Revolution?, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1914212.

²⁸⁸ *ibid*

enough. A multi-stakeholder approach has proven useful in identifying the problems and developing solutions. In order to allow users to make full use of their rights awareness-raising is necessary through digital education on all levels.

C. Digital Divide and Sustainable Development

Freedom of expression and access to ICTs should be properly seen in the context of broader goals of human development, codified by the United Nations' Millennium Development Goals framework and the national ICT goals set by the World Summit on the Information Society. Freedom of expression in traditional and online media actively helps in cultural preservation and promotion, reporting on environmental abuse by corporate and government agencies, campaigning against practices and products which harm health, and in peaceful negotiation during times of crisis and conflict.

Eight major megatrend areas can be identified in development discourse.²⁸⁹ For each of them, ICT4D can make contributions – some valuable, some indirect. Table 7 summarises key challenges in each of these trend domains, and how ICT4D factors into this dynamic. For instance, ICTs can enable the citizen on the street to participate in environmental quality monitoring systems and report on pollution via smartphones. More direct and valuable impacts of ICTs have been in creating ICT industries (eg. the 'Chindia' effect, or the rise of hardware and software services industries in China and India), preservation of cultural artefacts online, and healthcare applications of ICTs.

Table 8: Development Megatrends and the Role of Digital Media

Dimension	Active forces, challenges	Digital media responses
Environment	Global warming	ICTs for monitoring and optimising use of electricity in buildings; SMS/smartphone based citizen alert systems to report pollution
Safety	Natural/man-made disasters	Hybrid satellite/Internet/SMS alert systems for tsunami warnings
Habitat	Urbanisation	Telecentres, ICT-based/powered work for urban workers (eg. BPO), broadband connections for rich-media applications
Health	Diseases: AIDS, bird flu, malaria, etc.	Portals for AIDS awareness/mobilisation campaigns, mobile alert systems during disease outbreaks
Livelihood	Poverty	Web sites promoting sales/exports of handicrafts made by marginalised communities
Peace	Terrorism	Online forums promoting peaceful resolution of crises, alternative news sites with balanced coverage of international developments

²⁸⁹ Rao, Madanmohan (2009). ICT4D: Learnings and Best Practices. Singapore: AMIC.

Employment	Globalisation, informatisation	IT-enabled services for offshoring and outsourcing; capacity building for e-business; creation of domestic ICT industries
Culture	Media monopolies, audience fragmentation	Alternative news sites, free expression, community media, cultural archives online, community preservation of culture via ICTs

Source: Rao (2009)²⁹⁰

A notable trend is the increasing presence of ICTs in formulating global development agendas and development indicators. The United Nations' eight Millennium Development Goals (MDGs) have become widely-used benchmarks for development programs around the world, and a number of analysts have looked at ICT4D contributions and indicators within the MDG context.

Table 9: MDGs and ICT Indicators

	MDG	ICT4D Indicators
1	Eradicate extreme hunger and poverty	ICT initiatives directly targeted at poverty elimination, poverty-reduction strategies that include ICTs
2	Achieve universal primary education	ICT access in schools, percentage of teachers trained in ICTs, learning materials in digital form in local languages
3	Promote gender equality and empower women	ICT literacy among girls, role of women in ICT policymaking, availability of training of female workers in ICTs
4	Reduce child mortality	Campaigns to sensitise population via ICTs, ICT usage in health institutions, health sector allotments in national ICT plans
5	Improve maternal health	
6	Combat HIV/AIDS, malaria and other diseases	
7	Ensure environmental sustainability	Education/awareness campaigns using ICTs, ICT initiatives to reduce consumption of energy, water and other essential resources
8	Develop a global partnership for development	Number of companies and people employed in ICT sector, number of web pages in local languages, ICT penetration, competitiveness of local markets

Source: Rao (2009)²⁹¹

In some areas, ICTs are making significant contribution: such as higher education, healthcare services, and occupational advancement. In others, ICTs have a less direct role: poverty eradication on a large scale and rapid pace, or reduced child mortality (see Table 8).

The ITU's World Summit on the Information Society (I and II) marked the first formulation of global goals set by the international community, in ICT areas ranging from basic connectivity to e-

²⁹⁰ Rao, Madanmohan (2009). Ibid.

²⁹¹ Rao, Madanmohan (2009). ICT4D: Learnings and Best Practices. Singapore: AMIC.

government. Table 9 summarises the WSIS targets, along with ICT indicators for each. These targets and indicators will increasingly be used by the ICT community to benchmark and measure their progress. For instance, the World Bank's Information and Communications for Development 2006 report used these WSIS targets to compare and contrast ICT progress in countries around the world.

Table 10: WSIS Targets and ICT4D Indicators

	ICT Target	Sample indicators
1	Connect villages with ICTs and establish community access points	Percentage of villages with landline/mobile access, public Internet access points per 100 inhabitants
2	Connect universities, college, schools with ICTs	Percentage of schools with PCs/broadband Internet, students per computer
3	Connect scientific and research centres with ICTs	Availability of national research/education network, broadband connectivity
4	Connect public libraries, cultural centres, museums, post offices, and archives with ICTs	Percentage of institutions online, percentage of institutions providing public Internet access
5	Connect hospitals and health centres with ICTs	Percentage of institutions online, percentage with public Website-based services
6	Connect local and central government departments, establish Web sites and email addresses	Percentage of departments with Web sites and email, percentage of existing public services available online, number of new services online
7	Adapt all school curricula to meet the challenges of the Information Society	Inclusion of ICT in primary as well as secondary school curricula
8	Ensure that all of the world's population has access to television and radio access	Percentage of households covered by radio/TV signal, households with radio/TV sets
9	Encourage the development of content; technical platforms for all world languages on the Internet	Percentage share of Internet hosts, percentage of local sites in top 50 Web sites
10	Ensure that more than half the world's population have access to ICTs within their reach	Percentage of population with 2G mobile network, 3G network; online households

Source: Rao (2009)²⁹²

²⁹² Rao, Madanmohan (2009). ICT4D: Learnings and Best Practices. Singapore: AMIC.

D. Right to Cultural Diversity on the Internet

The Vision of WSIS

The Internet is a well of social and cultural knowledge, of practices, of languages, of symbols, icons and memes. At the same time, the dynamics of cultural discourse allow for the domination of specific cultures and languages. For historical and practical reasons, the English language and US cultural practices have dominated in the Internet for some time.

The common vision of the World Summit on the Information Society (WSIS) was an Information Society, where everyone can share information and knowledge and individuals, communities and peoples do achieve their full potential, including minorities and indigenous peoples. **Cultural and linguistic diversity** is given particular attention and includes cultural identity and the promotion of a dialogue between cultures and civilizations. For the purpose of linguistic diversity the creation of local content is crucial. Digitalisation should help pursuing the cultural heritage. Similar to the Vienna World Conference on Human Rights, which has called for human rights for all, the WSIS called for an information society for all (and recalled the outcomes of the Vienna World Conference).²⁹³

We find “foster[ing] and respect[ing] cultural diversity” as one of the key principles of the information society in the Geneva Declaration of Principles (para. 19). This commitment is echoed also in the Tunis documents. But it is the Geneva Declaration that explicitly underscores that cultural diversity is a “common heritage of humankind” and that information society should therefore “be founded on and stimulate respect for cultural identity, cultural and linguistic diversity, traditions and religions, and foster dialogue among cultures and civilizations”.²⁹⁴

An important part of preserving and enhancing cultural diversity, including linguistic diversity online, is the **creation, dissemination and preservation of content in different languages**. From an Internet that knew only Latin characters (actually: US-ASCII characters) we have come a long way to an Internet of internationalised domain names that brings the Internet closer to home to the billions of non-English speakers who can now access domain names in different scripts and in their own language.²⁹⁵

But the problem for cultural diversity lies deeper. An overwhelming part of the Internet is still produced and consumed in English, though social media have started to invigorate smaller languages as well. In the Geneva Declaration we read that the development of local content is so important because it “will encourage social and economic development and will stimulate participation of all stakeholders, including people living in rural, remote and marginal areas”.²⁹⁶ **Promoting local content** is indeed an important aspect of increasing diversity online and creating a sense of content-ownership and cultural pride in the Internet-based representation of cultural practices.

According to the Tunis Agenda **multilingualism** regarding domain names, e-mail addresses and content is one of the priorities in the quest to overcome the linguistic (and thus the digital) divide.²⁹⁷ Linguistic diversity thus equals empowerment and facilitates local content-production and the transfer of existing cultural heritage via ICTs to the memory space of the Internet.

²⁹³ See WSIS I, Geneva Declaration of Principles, op. cit.

²⁹⁴ Geneva Declaration of Principles, paras. 52.

²⁹⁵ Cf. ICANN, Internationalized Domain Names, <http://www.icann.org/en/resources/idn>.

²⁹⁶ Geneva Declaration of Principles, para. 53.

²⁹⁷ Compare WSIS II, Tunis Agenda for the Information Society, op. cit.

The right to cultural diversity belongs especially to minority populations, marginalised groups and indigenous people. ICTs can be harnessed to help overcome both the intrastate digital divide by representing indigenous cultural practices online and by preserving and promoting indigenous knowledge.²⁹⁸ The commitment of the International community also encompasses promoting the capacity of indigenous peoples to develop content in their own languages²⁹⁹ and thus contribute to a more diversified Internet. To achieve this, states and NGOs need to cooperate with indigenous peoples and traditional communities and make sure that they have the tools to “use and benefit from the use of their traditional knowledge in the information society”.³⁰⁰

In the **Internet Governance Forum**, the part of the WSIS agenda related to cultural and linguistic diversity was further discussed as one of the 4 (and later 5) main areas of debate. This was based on the firm commitment that, apart from English and the Latin alphabet other languages and scripts should be given more attention, inter alia by providing for the technological basis for Internationalized Domain Names (IDN) and developing content in other languages. At the IGF in Athens in 2006 the point was made that some 90 % of the world’s 6.000 languages were not represented on the internet. Domain names, at that time, could only be displayed in a few alphabets.³⁰¹

In the IGF the discussion was continued in several multi-stakeholder workshops on realising a multilingual Internet and Internationalized Domain Names (IDNs) and a Dynamic Coalition on Linguistic Diversity was established. The linkages between diversity and access were also a focal point, like the special needs of minorities, indigenous people, migrants, and issues of gender as well as the problem of literacy. It was at the Sharm El Sheikh session of the IGF in 2009, when ICANN announced that for country-code Top-Level-Domains (ccTLDs) non-Latin characters could now also be approved and Egypt filed the first application for a ccTLD in Arabic.³⁰²

Opportunities and Threats from Cultural and Linguistic Diversity

Obviously, the opportunities created by the Internet are enormous. For example, people speaking a minority language but scattered all over the world can communicate more easily through the Internet, their language can more easily be preserved. The opportunities also relate to sharing music and other expressions of culture from around the world. However, there are also threats to diversity as the fact that most content is in English may lead to the neglect and further marginalization of other languages.

Access to the Internet means access to education and capacity-building, which also has a cultural impact. It has also opened new opportunities for religions and churches to present their beliefs and to communicate with their followers, which can strengthen cultural identity and diversity.

The Internet allows for unprecedented tools to **preserve cultural heritage** through digitalization. This is, as the Geneva Declaration puts it, a “crucial component of identity and self-understanding of individuals that links a community to its past”.³⁰³ Through the Internet, harnessing and preserving cultural heritage for the future has become much easier. One example

²⁹⁸ Cf. Ibid., para. 23 d).

²⁹⁹ Ibid., para. 23 k).

³⁰⁰ Ibid., para. 23 l).

³⁰¹ See Proceedings of the first IGF in Athens. In: Doria, Avri and Kleinwächter, Wolfgang (2008), Internet Governance Forum (IGF), The First Two Years, UNESCO 2008, 167 et seq.

³⁰² See Xue, Hong. Diversity: Achieving an Internet that is Really for All. In: William J. Drake (Ed.), Internet Governance: Creating Opportunities for All, The Fourth Internet Governance Forum in Sharm El Sheikh, Egypt, 15.-18.11.2009, United Nations 2010, 25-33.

³⁰³ Ibid., para. 54.

is the Google Art Project³⁰⁴ that has started to digitalise collections of museums from around the world, making them both accessible free of charge and preserving them for the future.

At the same time, digitalisation of cultural content is not without risks. The choice of what content to digitalise is often politically motivated, commercially conditioned or can be culturally conditioned. International law needs to guide the international community in promoting a discrimination-free and intellectual development-oriented process of promoting digitalisation of cultural content. This is echoed by the Geneva Plan of Action which calls on states to develop policies and laws to ensure that “libraries, archives, museums and other cultural institutions can play their full role of content - including traditional knowledge - providers in the Information Society”.³⁰⁵

Regional Initiatives for Cultural Promotion and Diversity

The South Asian Association for Regional Cooperation (SAARC) set up a Cultural Centre in Sri Lanka as a regional centre to promote cultural cooperation in order to bring the people of South Asia closer and to project the distinct identity of South Asia. The SAARC Agenda for Culture launched the SAARC Website on Culture (www.saarcculture.org) and addressed digital initiatives such as digitisation of regional tangible and intangible cultural heritage details; development of archives employing state of the art digital technology; and creation of links with websites of relevant inter-governmental institutions’ on culture.

The issue of cultural diversity in the Asia Pacific was also addressed at the Ministerial Forum of the Asia Pacific region³⁰⁶ (9-11 May 2012, Dhaka: <http://culdivminforum.gov.bd>), which was supported by UNESCO's International Fund for Cultural Diversity. The Dhaka Declaration was signed by ministers and representatives from 33 out of 44 countries of the region. The salient features of the Dhaka declaration emphasise linking culture to development endeavours; urgent need for collective political will to ensure cultural cooperation for sustained human resource development; developing a platform for cross-sector dialogue and cooperation with the civil society to ensure active participation of myriad voices in the policy-making and implementation processes.

In 2008, the Asia-Europe Meeting initiated the online platform culture360.org to use new technologies for enhancing information sharing and cultural understanding, in keeping with the spirit of the UNESCO Convention on the Diversity of Cultural Expressions (especially Article 12). The portal collects information, data and best practices on the diversity of cultural expressions (Ramona Laczko David, 2010).³⁰⁷ Cultural practitioners take part in bi-regional cooperation, exchange information on projects, and collaborate on new initiatives. Over 800 organisations in Asia and Europe have been linked via culture360.org, and ASEM Cultural Ministries have been encouraged to link culture360.org to their own websites.

Relevant Legal Instruments

According to Art. 15 of the UN Convention on Economic Social and Cultural Rights everyone has the **right to take part in cultural life, to enjoy the benefits of scientific progress** and its applications and to benefit from the protection of the moral and material interests resulting from any

³⁰⁴ Google Art Project, <http://www.googleartproject.com>.

³⁰⁵ Geneva Plan of Action, para. 23 b).

³⁰⁶ The Daily Star, Bangladesh (2012). Cultural diversity declaration, <http://www.thedailystar.net/newDesign/news-details.php?nid=233851>.

³⁰⁷ German Commission for UNESCO/Asia-Europe Foundation (2010). Mapping Cultural Diversity – Good Practices from Around the Globe, http://www.unesco.it/_files/DIVERSITAculturale/Publication_DUK.pdf.

scientific, literary or artistic production of which he is the author. This includes intellectual property rights like the copyright. While the controversies related to these provisions will be dealt with later, it is important to point out that the first two rights can be related, i.e. the enjoyment of the benefits from scientific progress can be instrumental for the right to take part in cultural life.

UNESCO in 2001 has adopted a “Universal Declaration on Cultural Diversity”, which is based on cultural diversity as the common heritage of humanity. The defense of cultural diversity is presented as an “ethical imperative, inseparable from human rights”.³⁰⁸ The Convention emphasises the relevance of the respect for human rights and fundamental freedoms, such as freedom of expression, information and communication for cultural expression. The Convention recognises that cultural diversity is manifested through a variety of cultural expressions, whatever the means of technology used, which also includes Internet technology. The Action Plan for the implementation of the Declaration calls for the greater mastery of ICT (“digital literacy”) and the promotion of linguistic diversity in cyberspace.³⁰⁹ In the follow up to WSIS, UNESCO focused on cultural heritage and diversity of languages including indigenous languages.

An important international instrument to protect and promote diversity of cultural expressions is the UNESCO “Convention on the Protection and Promotion of the Diversity of Cultural Expression” of 2005 which, by 2012, has 121 states and the EU as parties.³¹⁰ The Convention notes that globalisation and ICT development has offered “unprecedented conditions for enhanced interaction between cultures”, but also challenges cultural diversity, especially in view of risks stemming from imbalances between rich and poor countries. Art. 12 d) of the Convention calls for promotion of the use of ICTs to enhance information sharing and cultural understanding, and foster the diversity of cultural expressions. Similarly, Art. 14 b) and c) highlight the potential of ICTs for capacity-building through the exchange of information, experience and expertise, and technology transfer.

Elements of the Right to Cultural Enjoyment on the Internet

The draft Charter on Human Rights and Principles for the Internet by the Dynamic Coalition of Internet Rights and Principles addresses several aspects of the cultural enjoyment on the Internet related to Art. 27 UDHR, i.e. the right to participate in the cultural life of the community, the right to access to quality and diverse information as well as different cultural content, the realization of culture and linguistic diversity on the Internet in all forms (e.g. text, images and sound), technological innovation to promote diversity on the Internet and the protection and promotion of indigenous knowledge online. In addition, there is a right to use one’s own language to create, disseminate, and share information and knowledge through the Internet, while special attention should be given to promote access for minority languages. This includes use of domain names, software, services, content in minority languages and scripts.³¹¹

Cultural diversity has been proclaimed as a new principle, if not already an **emerging right** mainly in the context of media and globalisation.³¹² The discussion on an audiovisual exception to the obligations of the General Agreement on Trade in Services (GATS) of the WTO in the 1990s was continued in the first decade of the new millennium with a debate on cultural diversity in cyberspace and with regard to culturally diverse expressions by and through online media. One major concern was and is the preservation of cultural identities and cultural pluralism. Such

³⁰⁸ See Arts. 1 and 4 of the Declaration, <http://unesdoc.unesco.org/images/0012/001271/127160m.pdf>.

³⁰⁹ Ibid.

³¹⁰ UNESCO, Convention on the Protection and Promotion of the Diversity of Cultural Expressions, Paris, 20.10.2005, <http://unesdoc.unesco.org/images/0014/001429/142919e.pdf>.

³¹¹ Compare draft Charter on Human Rights and Principles for the Internet, op. cit.

³¹² See Meigs, Divina Frau (2011). Media matters in the cultural contradictions of the „information-society“ – Towards a human rights-based governance, Council of Europe Publications 2011, 189 et seq.

identity is a prerequisite for a cultural dialogue on an equal level. Accordingly, the UNESCO Convention on Cultural Diversity of 2005 allows states to derogate GATS-obligations for the purpose of protection of cultural diversity.

The European Union is also involved in such activities, through the European Cultural Foundation, Culture Action Europe or the Rainbow Platform on Inter-Cultural Dialogue.³¹³ In 2006 the European Commission adopted a Recommendation on Digitization and Online Accessibility of Cultural Material to preserve Europe's cultural heritage and make it better available.³¹⁴

Furthermore, the Internet and social media can be used to preserve the world's endangered languages. In the world today, there are over 6,000 languages spoken; some villages of Africa, Asia, and South America only speak dialects with fewer than 1,000 speakers of that language per village (Meagan Lunn, 2012).³¹⁵ For example, Vasi-vari is a language spoken by the Vasi tribe in a few villages in the Prasun Valley, Afghanistan. Only 1,000 people are said to have this as a first language and is considered to be the least spoken of the Nuristani languages.

Modernisation and globalisation have often been the enemies of traditional and local cultures, but modern day social media sites like YouTube, Facebook and Twitter as well as mobile communication methods like SMS can preserve the content of some of the endangered languages and nurture communities speaking these languages. It has been predicted that by 2100 that half of the 7,000 endangered languages spoken globally will disappear.

Civil society has been very active in fighting against what some perceive as trends to endanger free access to cultural expressions.³¹⁶ Disorganized phenomena such as Anonymous have emerged that reflect the zeitgeist of the Internet age and, according to Yochai Benkler, should not be perceived as security threats but rather as evidence of the "openness and uncertainty that have made the Internet home to so much innovation, expression, and creativity".³¹⁷

Balancing Open Access and Compensation Models

In order for cultural diversity to be ensured the rights of authors have to be protected. This has become one of the thorniest issues of Internet Governance. The public reaction to anti-piracy laws in the US Congress – SOPA and PIPA – and the discussion in Europe and beyond on the consequences of ACTA for private users have evidenced clearly a dissonance between the user base and the traditional normative approaches of states and the interests of content management companies.

The central dissonance is that between the claim that knowledge is free and access to knowledge should be free too and that of the owners of intellectual property rights (IPRs) who are supposed to earn their living from them³¹⁸ or to benefit from an exclusivity during a certain period to

³¹³ Ibid., at 209.

³¹⁴ See European Commission, Recommendation on the Digitization and Online Accessibility of Cultural Material and Digital Preservation of 24.08.2006, O.J. L 236 of 31.08.2006.

³¹⁵ Lunn, Meagan (2012). Social Media to Preserve Endangered Languages, <http://www.koreaittimes.com/story/19919/social-media-preserve-endangered-languages>.

³¹⁶ Cf. Gross, Michael Joseph (2012). World War 3.0, Vanity Fair, May 2012, <http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking.print>.

³¹⁷ Benkler, Yochai (2012). Hacks of Valor. Why Anonymous Is Not a Threat to National Security, 04.04.2012, Foreign Affairs, <http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor?page=show>.

³¹⁸ The rights of authors emerged and were first recognised in France in the eighteenth century after a long crusade leaded by author de Beaumarchais. The authors wanted to be able to earn their living through their own intellectual work and no longer depend on royal pensions irregularly given to "courtisans" (in that respect, the author IPR was also linked with freedom of expression). Benefiting of a new right of property,

amortize the cost of their creation or of their discovery, having made them public and thus accessible to everybody.

The need for balancing Access to Knowledge (A2K) and compensation is both anchored in, and can be termed in, human rights terminology. Article 27 of the Universal Declaration of Human Rights gives everyone the right “freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits” (para. 1) and, in para. 2, gives everyone the right to “to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author”.

A2K proponents thus rely on para. 1 of Art 27, while opponents focus on the “material interests” protection clause of para. 2. How both can be balanced with a view to furthering access to knowledge can be seen in the Access to Knowledge Treaty which was drafted in 2005.³¹⁹ It suggests reframing the way patents are granted and IP is protected worldwide, including through the Berne Convention and TRIPS.³²⁰ Further it introduces the notion of “knowledge commons”, that knowledge that should be available to everyone.

However, a globally accepted approach to ensuring diversity and free use of cultural expressions on the one hand and promoting diversity by protecting cultural expressions on the other hand, remains elusive. One possible avenue to bridge the dissonance and ensure for free access to commons is the “creative commons licensing” system,³²¹ which allows creators of materials to share these while retaining certain rights. There are also considerations on new models to compensate author’s rights, i.e. by a levy on hard discs or on Internet connectivity.

The explosion of content on the Internet creates opportunities for content creators, aggregators, researchers and other intermediaries, eg. new sources of revenue and visibility for publishers, business models for search engines. New forms of content and information have also been emerged, ranging from blogs and microblogs to location data and mashups. Some copyright owners and Internet companies have also cooperated to ensure free access to cultural heritage.³²²

Internet publishing also creates new challenges, via increased plagiarism, copying without accreditation or payment, compensation for online versions of content originally created for print/broadcast media, reference formats and longevity for academic research, linking and

the authors whose books were largely sold could live with the revenue of their work. The most controversial problem in IPR remains to determine the duration of the period of exclusivity. In the case of author's right, France recognises also the heirs' IPR, which can be considered strange given the aim of that right (after the author's death, there is no longer any need to ensure him with a revenue.

³¹⁹ Access to Knowledge Treaty (2005), http://www.cptech.org/a2k/a2k_treaty_may9.pdf.

³²⁰ Generally speaking, IPR are divided in at least two categories, author's and artistic copyright and patent rights. Even if one could have expected software (mainly produced within large industrial firms) would have fallen in the patent rights category, they are protected as an author right. Under Article 2 of the Berne Convention (09.09.1886, revised in 1971 and 1979) and specially Articles 9 and 10 of TRIPS, software is protected as litterature works under the regime of the Berne Convention. Article 2 of the IPWO (Geneva, 20.12.1996) also foresees that the software are protected as litterature works in the meaning of article 2 of the Berne Convention. The European Directives 91/250/EEC and 2001/29/EC develop the legal regime of software in the frame of the common market and of the information society. But the protection of software is a limited one according to the jurisprudence of the ECJ (decisions C-5/08, 16.07.2009, C-393/09, 22.12.2010 and C-406/10, 02.05.2012) and deserves a lot of flexibility to the user. Moreover, under many software domestic legislations, the user benefiting from a license can adapt and improve the software. "Free software" is also subject to IPR but respects four freedoms defined by the Free Software Foundation (freedom of use for any use; freedom of study and of adaptation to everybody's needs; freedom of diffusion; freedom of modification).

³²¹ Creative Commons, <http://creativecommons.org/licenses>.

³²² Google Art Project, <http://www.googleartproject.com>.

framing external content, rights and duties of commercial aggregators, authorised and 'unauthorised' translations, 'screenscraping' and archiving, and content ownership and access after mergers and acquisitions between content creating companies.

"While in the analog world, life was sans copyright law; in the digital world, life is subject to copyright law. Every single act triggers the law of copyright. Every single use is either subject to a license or illegal, unless deemed to be "fair use". The emergence of digital technologies has thus radically increased the domain of copyright law", according to Lawrence Lessig.³²³ The hardware, software and architecture of the Internet ('code') are the most significant form of law in cyberspace, and "it is up to lawyers, policymakers, and especially citizens to decide what values that code embodies".

Lessig³²⁴ advocates that enormous opportunities await those who view art as a resource to be shared openly via digital media rather than a community to be hoarded. The 'read-write' culture of mobile social media should not be criminalised, but nurtured for the next generation of the creative community to emerge.

Activist David Bollier³²⁵ uses the term 'viral spiral' to refer to the open access movement based on decentralised creativity, collaborative intelligence, and cheap and easy sharing. Free and open-source software, Creative Commons licenses, Wikipedia, remix music, video mashups, peer production, open science, open education, and even open business are some incarnations of the "sharing economy".

Shutting down large scale commercial piracy can reward content creators and protects their intellectual property rights, but the 'law of unintended consequences' can lead to legitimate businesses (such as a web site or an ISP) liable for the presence of illegitimate content on their site.³²⁶ Sites like Dropbox, YouTube and Facebook as well as emerging 'cloud' computing and hosting providers can be shutdown under proposed laws like SOPA and PIPA simply for unintentionally hosting content deemed 'pirated'. Heavy-handed approaches run the risk of 'overkill' of creative sites.

Another set of challenges emerges in the realm of parody, satire, compilations, and tagged content. For instance, Pinterest, a virtual pinboard or scrapbook, allows users to collect and organise their favourite images and ideas.³²⁷ The company says that it believes that it is protected under the safe harbour of the US Digital Millennium Copyright Act. The site also claims it drives traffic back to other Web sites and thus does not hurt them. The site, which was launched in 2009, has over 10 million users.

Some search engines, caching services and news indexing services have also been threatened with lawsuits. The Associated Press has filed a copyright lawsuit against news indexing engine Meltwater, calling it a 'modern-day clipping service'.³²⁸ For a fee, Meltwater enables clients to search news stories for mentions of keywords and to receive email digests. US courts have treated search engines and clipping services differently in regard to copyright law.

³²³ Lessig, Lawrence (2006). Code. Version 2.0, New York: Basic Books, <http://codev2.cc>.

³²⁴ Lessig, Lawrence (2008). Remix: Making Art and Commerce Thrive in the Hybrid Economy. New York: The Penguin Press.

³²⁵ Bollier, David (2009). How the Commoners Built a Digital Republic of Their Own. The New Press.

³²⁶ Harzog, Bernd (2012). SOPA and PIPA, <http://www.virtualizationpractice.com/the-sopa-and-pipa-kerfluffle-14272/>.

³²⁷ Tsukayama, Hayley (2012). Pinterest addresses copyright concerns, http://www.washingtonpost.com/business/technology/pinterest-addresses-copyright-concerns/2012/03/15/gIQAijAFES_story.html.

³²⁸ Myers, Steve (2012). Meltwater says AP's copyright lawsuit threatens all search engines, <http://www.poynter.org/latest-news/mediawire/171382/meltwater-says-aps-copyright-lawsuit-threatens-all-search-engines/#more-171382>.

“The Internet will create a world where there is much more art, much more culture, much more learning and knowledge, according to Robin Gross,³²⁹ executive director of IP Justice. Outdated business models from the analog era should ‘not stifle and chill’ the digital world of the Internet.”

In response, some alternative compensation systems for digital media have been proposed by researchers such as John Palfrey, co-director of the Berkman Centre for Internet & Society. “The present crisis in digital media, increasingly a global phenomenon, calls for the consideration and rigorous analysis of alternatives to those schemes”, according to Palfrey.³³⁰ A new system should be designed in which the creators and producers of digital content will be compensated by industry and governments in proportion to the frequency with which their products are consumed, with revenue being raised through taxes on consumer electronic devices and Internet access. The revenue would be shared with content creators, government agencies and infrastructure providers. Such a new system can be created by mandate, or a voluntary partnership between all stakeholders. Challenges can arise in “free riding” by non-participants, inflation of figures by ‘gaming’ the system, and respecting consumer privacy.

³²⁹ The 2012 Internet Society Global INET, http://www.elon.edu/e-web/predictions/isoc_20th_2012/intellectual_property_innovation.xhtml.

³³⁰ Palfrey, John (2012). “Alternative Compensation Systems for Digital Media”, <http://blogs.law.harvard.edu/palfrey/alternative-compensation-systems-for-digital-media/>.

V. General Conclusions, Open Questions and Future Challenges

Ethics and Human Rights as Universal Standards

Cyberspace is a social space in need of basic rules. Among those rules the emerging law of the Internet human rights have a crucial role to play. They respond to the calls for a computer ethics and information ethics, and an ethics of e-governance,³³¹ in particular with regard to the roles of states and business, but also the individual and civil society. According to the WSIS, these are to act together in a multi-stakeholder approach, when it comes to Internet governance issues. In practice, the issue mainly is about balancing of interests between the different stakeholders, like the balance between freedom of expression or privacy and security or the balance between access to knowledge and intellectual property rights. Human rights as interpreted for the purposes of the information society can inform decisions in such conflicts, while the balancing outcomes are also the result of a political process, in which all actors are involved. For example, the right to access to knowledge is a particular concern of the South, but it is assisted by Northern NGOs and new political forces like the “piracy parties” and large parts of international civil society in this respect. Accordingly, there are less North-South issues than issues about the future rules governing the information society, which are being discussed in the multi-stakeholder forum of the IGF as well in regional fora. The conceptual differences sometimes disguise the economic interest behind. With regard to human rights, it is less as a matter of a Western, individualist approach vs. a Southern community-oriented approach, which in practice can hardly be found, than of a holistic approach, based on the universality and indivisibility of all human rights, as the two World Conferences on Human Rights in Teheran 1968 and in Vienna 1993 have concluded.

No New Digital Rights, but Right to Access

It could be shown that there is hardly any need to design new digital rights and get them accepted as human rights, but rather to apply the existing human rights to the issues raised by the Information Society, according to the principle that “human rights applying offline also apply online”. However, there is a need to interpret human rights when applying them to issues of the Internet in an appropriate way as they had to be interpreted to apply to the electronic media when those emerged. From the right to the full enjoyment of all human rights, a right to access to the Internet can be concluded, which is to be achieved in a progressive way.

New Challenges and Human Rights

New challenges are posed by new technological innovations like the “Internet of Things”, tags to communicate with each other, or by cloud computing, which raises issues of privacy protection in a new context. Privacy and data protection together with freedom of expression are very much in the forefront of ongoing discussions, which shows the relevance of human rights.

For example, the right to anonymity as part of the right to privacy has been heavily debated as is the right to delete personal data or “a right to die” in the Internet. In the first case, it is the state who wants to have some control over traffic data, if not content while in the second it is also business, which is hesitant to give the user full autonomy and informational self-determination. Many states want to restrict data privacy for the sake of so called “cyber-security”, they want the

³³¹ Compare Unwin, Tim (2010). ICTs, Citizens and the State: Moral Philosophy and Development Practices, *Electronic Journal on Information Systems in Developing Countries*, 44, 1, 1-16.

identity of the user to allow for governmental surveillance. This would arguably be the end of privacy.

Free speech advocacy organisation Article 19 (www.article19.org) believes that increasing the profile of the human rights perspective in debates on intellectual property is essential to protecting freedom of expression, particularly in the digital ecosystem. The Expert Meeting on Freedom of Expression and Intellectual Property Rights, organised by Article 19 in 2011, advocated the use of the phrase “information society service providers”³³² as an umbrella phrase that includes search engines, advertisers, payment services. The Meeting also identified philosophical foundations of differing views of copyright protections, in particular the difference between the US (incentivise creation) and European (natural rights) approach. Intellectual property protection was also identified as a geographic concentration of wealth issues (eg. Hollywood) as much as a moral issue.

The Future of Internet Governance

Of crucial importance for the future governance of the Internet could be the World Conference on International Telecommunications (WCIT) of the International Telecommunication Union (ITU) in Dubai in December 2012, which will discuss the future ITU role and rules, and where no multi-stakeholder approach applies.³³³ This could also affect the rules of Internet governance and the proposals by Russia, China and others for a code of conduct to improve global information security also point in the direction of more state control over the Internet. Therefore, the issue of the future of an open Internet in which all human rights of users are respected is at stake. In an Op-ed to the New York Times and International Herald Tribune Google’s Chief Internet Evangelist Vint Cerf has warned that the decisions in Dubai could put government hand-cuffs on the Net.³³⁴

States may rightly be concerned about increasing levels of cybercrime or glorification of terrorism on the net, about hacktivism like Anonymous or various cyber-intrusions up to cyber war. However, cyberspace, as has been shown in the first part, has been created as an opened space and there are technological limits to governmental control over it. As the Egyptian blackout has shown, restrictions on the Internet can have a chilling effect on the economy, which is increasingly based on ICTs and the Internet. Again, the issue is finding the right balance of security and openness, taking the legitimate interests of all stakeholders into account. The wave of sets of principles may be an indicator of increased efforts to find such a balance.

A ‘Principled Approach’ to Internet Governance

2011 was the important year for the development of principles guiding Internet Governance. 2012 has partly been the year of their operationalisation. The international community has to ask itself which goals it wishes to pursue with which means. The WSIS documents have committed the international community to a people-centred, development-oriented information society that is based on human rights and international law. This must continue to be the goal of all regulation.

2012 will be an important year for the protection of human rights on the Internet. The 2012 session of the UN Human Rights Council has discussed the role of freedom of expression on the Internet, itself a catalyst for other human rights. The IGF 2012 in Baku and the ITU conference in

³³² Centre for Internet and Society (2012). Report on Expert Meeting on Freedom of Expression and Intellectual Property Rights, <http://cis-india.org/a2k/freedom-of-expression-and-ipr-meeting>.

³³³ See World War 3.0, op. cit.

³³⁴ Cerf, Vinton (2012). Keep the Internet Open, New York Times and International Herald Tribune of 25.05.2012.

December 2012 both have to consider the role of Internet Governance Principles and how they can be translated into practice.³³⁵

Interaction of States and Non-State Actors in the Future Regulatory Framework

The information society and the framework introduced to regulate it, Internet Governance, is characterised by the multi-stakeholder approach. This approach is both effective and legitimate and has led to important normative developments. What is essential for Internet Governance to work is that states and non-state actors face each other on an equal level. The Internet has provided us with innovative opportunities of e-government and e-governance. Now, it is important to ensure that e-participation by all in the processes of Internet Governance is ensured.

Which Instruments and Which Actors Will Regulate Online Behaviour Most Effectively?

The Internet Governance regime has shown how self-regulatory models can effectively secure human rights through stakeholder-based regulatory efforts. If no outside security constraints forbid it, self-regulation is in fact the optimal solution to the challenges of Internet Governance. If self-regulation is not practicable, co-regulation should be the regulatory approach envisaged next. In both cases, however, recourse to traditional state structures of law enforcement must be provided in order to ensure the rule of law and the protection of human rights in cases of regulatory failure.

Another important aspect of regulating behaviour online is awareness-raising. Originally, the Internet has been governed effectively by nothing more than social norms. There can be no stepping back to simpler times, but individuals should develop an ethical approach to Internet usage, as they should have to life. When using ICTs individuals are not divested of their human rights, but rather have the responsibility to assert their own rights and respect and protect the rights of others.

Instead of trying to strengthening their grip over users, states should rather be concerned with creating more awareness, of providing cyber-education or digital education in order to allow their citizens to make best user fit for economic progress and development.

The Road Ahead: Emerging Technologies

Technology turns anyone with a modern mobile phone into a cameraman – and international broadcaster.³³⁶ Sites like Ustream, Bambuser and Livestream allow users to upload videos taken from mobile phones, and activists will be able to use ‘drone cameraplanes’ one day.

The debate over free speech and the Internet is becoming increasingly politicised, with the US administration actively supporting the construction of detours around Internet censors in repressive environments. More than \$ 70 million worth of grants have reportedly been issued to nongovernmental organisations developing technologies to assist activists inside repressive countries to stay connected, regardless of government efforts to keep them silent.³³⁷ The

³³⁵ Cf. Kettemann, Matthias C. (2012). The Power of Principles: Reassessing the Internet Governance Principle Hype, Jusletter IT, 29.02.2012, www.jusletter-it.eu.

³³⁶ The Economist (2012), <http://www.economist.com/node/21542748>.

³³⁷ Crawford, Jamie (2012), <http://security.blogs.cnn.com/2012/01/30/the-unseen-global-revolution/>.

programme has evolved from circumventing government Internet firewalls to developing mobile-based technologies such as mesh networks that can be used on cell phones and other portable devices that are much more difficult to monitor. (At the same time, the US government itself has taken action against whistleblowing sites such as Wikileaks!)

The rise of digital expression and mobile activism has opened up new research frontiers in the psychology and culture of digital media. By enabling social connection, mobile technologies tap into the biologically-based drive for social contact. Digital tools like the Internet have given us global awareness, but it is mobiles that give people the control to be personal.³³⁸

Mobiles have helped create a 'place out of place' or interspace that allow users to be physically in one location but mentally elsewhere. Mobile Internet is challenging the meaning of public spaces and social norms for interaction. Digital tools provide the ability to offload lower-value cognitive tasks focus more on creativity, analysis, and problem solving. Digital platforms and mobile social networks are changing individual expectations about opportunities and impacts of activism.

From the alphabet and writing in Ancient Greece to Gutenberg's printing press, and now with the Internet and its mobile incarnation, media innovations continue to undermine existing political structures, redefine social capital, create new divisions, and challenge individual beliefs and assumptions. In less than 20 years, the Internet has set a new standard by for communications that concurrently enhance autonomy and collaboration (e.g., Harp, Bachmann, Rosas-Moreno and Loke, 2010;³³⁹ Harris, 2004;³⁴⁰ Howard, A. L., 2010;³⁴¹ Howard, P. H., 2004;³⁴² Kellner and Share, 2007;³⁴³ Winston, 1998³⁴⁴).

Smart mobs, as first identified by Howard Rheingold,³⁴⁵ are mobile, technologically-mediated self-organising social groups. But as the prevalence of technology-enabled collective actions grows, there are variations among different types of 'mobs' based on duration, focus, implementation and purpose.³⁴⁶

With the convergence of Internet and mobile, tools like Ushahidi have emerged, which offer an open source platform available to developers to create crowdsourced solutions for crisis information. Initially developed to report post-election violence in Kenya in 2008, it is now used for everything from managing snow removal in New York City to reports of gender violence in Pakistan.

Technology innovators have driven a dizzying pace of digital media evolution over the past three decades, and the next wave is powered by developments in embedded chips and hybrid

³³⁸ Pamela Rutledge: Psychology of Mobile. In: Bruck, Peter and Rao, Madanmohan (2013-forthcoming), Global Mobile: Scenarios and Strategies. New Jersey: InfoToday/Perseus Publishing.

³³⁹ Harp, D.; Bachmann, I.; Rosas-Moreno; T. C. and Loke, J. (2010). Wave of Hope: African American Youth Use Media and Engage More Civically, Politically Than Whites. The Howard Journal of Communications, 21 (3), 224-246.

³⁴⁰ Harris, R. J. (2004). A Cognitive Psychology of Mass Communication (4th ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

³⁴¹ Howard, A. L. (2010). Engaging the City: Civic Participation and Teaching Urban History. Journal of Urban History, 36 (1), 42-55.

³⁴² Howard, P. H. (2004). Society Online: The Internet in context. Thousand Oaks, CA: Sage Publications.

³⁴³ Kellner, D. and Share, J. (2007). Critical Media Literacy, Democracy, and the Reconstruction of Education. In: Macedo, D. and Steinberg, S. R. (eds.), Media literacy: A reader, 3-23. New York: Peter Lang.

³⁴⁴ Winston, B. (1998). Media Technology and Society: A History: From the Telegraph to the Internet. London: Routledge.

³⁴⁵ Rheingold, H. (2002). Smart Mobs. Cambridge, U.K.: Perseus Books.

³⁴⁶ Kindberg, T.; Bardram, J.; Buttrich, S.; Esbensen, M.; Houben, S.; Khaled, R. and Tabard, A. (2011). Mesh Mobs: Virtually Augmented Crowds. Copenhagen: IT University of Copenhagen.

networks. Physicist Michio Kaku³⁴⁷ interviews over 300 of the world's top scientists to present a fascinating view of what the next 100 years of inventions and their impacts may look like.

Just as many computer pioneers from two to three decades ago predicted some of what we are witnessing today in the world of mobile Internet devices and the accompanying socio-political impacts, so also many scientists and labs today are able to make educated guesses about emerging technological innovations. These include Internet-enabled glasses, wireless safety chips embedded in clothes and automobiles, and nanotechnology devices (see Table 11).

Table 11: Technology Evolution for the 21st Century

Technology category	Near Future (present to 2030)	Mid-Century (2030 to 2070)	Far Future (2070 to 2110)
Computing	<ul style="list-style-type: none"> - Internet-enabled glasses, contact lenses - Driverless cars - Four-wall screens - Flexible electronic paper - Safety chips in clothes 	<ul style="list-style-type: none"> - End of Moore's Law - Ubiquitous augmented reality - Universal translators - Holographic Internet 	<ul style="list-style-type: none"> - Machine control by thought (telekinesis) - Portable brain scans - Photographing dreams - Mind reading
Artificial Intelligence	<ul style="list-style-type: none"> - Expert systems in healthcare 	<ul style="list-style-type: none"> - Modular robots - Robot surgeons and cooks 	<ul style="list-style-type: none"> - Conscious machines - Human mergers with robots
Medicine	<ul style="list-style-type: none"> - Genomic medicine - Cloning; stem cells 	<ul style="list-style-type: none"> - Gene therapy - Designer children 	<ul style="list-style-type: none"> - Reversing aging - Resurrecting extinct life forms - Creating new life forms
Nano-technology	<ul style="list-style-type: none"> - Nanocars in our bodies - DNA chips - Quantum computers 	<ul style="list-style-type: none"> - Shape shifting 	<ul style="list-style-type: none"> - The Replicator
Energy	<ul style="list-style-type: none"> - Solar/hydrogen economy - Electric cars 	<ul style="list-style-type: none"> - Global warming and flooding - Nuclear fusion power 	<ul style="list-style-type: none"> - Magnetic cars and trains

Source: Adapted from Michio Kaku³⁴⁸

³⁴⁷ Kaku, Michio (2011). *Physics of the Future: The Inventions That Will Transform Our Lives*. New York: Penguin Books.

³⁴⁸ Kaku, Michio (2011). *Physics of the Future: The Inventions That Will Transform Our Lives*. New York: Penguin Books.

Such innovations have interesting implications for digital expression. For instance, almost all the literature and developments on freedom of expression assume that it is humans who are gathering and disseminating information. However, this can change in the not-so-distant future with robots and 'drone aircraft' taking on the role of reporting in dangerous situations or banned zones!

Another key assumption of the ICT era is that rules like Moore's Law, according to which memory capacity and processing speed are doubling roughly every two years will continue to hold for the coming decades. This will continually driving down the price of tools like smartphones and thus increase citizen access to digital media, creatively disrupt existing industries, and provide the growth engine for the entire IT industry which in turn powers much of the 21st century capitalist economy. However, as scientists like Kaku explain, Moore's Law will cease to hold perhaps by 2030, thus raising serious challenges to the ICT industry while also forcing it to further explore alternatives such as quantum computing or bio-computing.

Questions related to Chapters I-IV

These questions arise from the preceding review of the relevant issues and supplement those already identified by the seminar's organisers.

Questions related to Chapter I:

1. Should the Internet be considered as a (global) public good and what consequences would follow from such approach?
2. What can be understood by the 'public service value' of the Internet?
3. What are the main new opportunities, what are the new risks flowing from the Internet in the fields of economy, society, crime, etc.?
4. How can we balance freedom and openness of the Internet against the responsibility of states to provide security?
5. How to deal with hate speech or terrorist propaganda on the Internet in a human rights sensitive way?
6. Which restrictions of contents on the Internet are justified by the protection of minors?
7. When is the Internet an enabler, when a threat to human rights?
8. How are definitions of what is private and public changing with the advent of social media?
9. How are mobile communications introducing new notions of what is private, eg. location of the user?
10. What are metrics and measures which can be used to compare public service and open access models in different countries and regions around the world?
11. What are the features of the Internet and mobiles which make them work in favour of the 'masses,' and what are the features (like or unlike) which can turn them in favour of the ruler?
12. What are some emerging trends in encryption and authentication which can work in favour of user privacy, and how should governments deal with them?

Questions related to Chapter II:

1. What is the purpose of Internet Governance and can it be implemented?
2. What means of regulation – self-regulation, co-regulation or regulation by the public authorities – is most effective and legitimate?
3. What should be the role of ICANN in Internet Governance; What the role of the IGF and of ITU?
4. What are the benefits and problems related to a multistakeholder approach?
5. Should the IGF become responsible for drawing up recommendations or producing reports?
6. What should be the role of governments in Internet Governance; how can we use the framework of the United Nations effectively?
7. What should be the role of events and organisations at the regional level in Internet Governance?
8. What are the differences in Internet Governance approaches and between European and Asia?
9. What are the responsibilities of the different stakeholders for Internet Governance in general and human rights in particular?
10. Are there legitimate limitations of human rights in the information society for cultural reasons?
11. What is the role of human rights in Internet Governance and which human rights are the most crucial?

12. Does the Charter on Human Rights and Principles for the Internet provide a good basis in this respect?
13. Is there a need for new digital rights?
14. What is the role of principles for Internet Governance and which principles can be agreed upon?
15. What are the emerging trends in M2M (machine-to-machine) connectivity in the world of IPv6? What implications does this have for surveillance networks by governments?
16. What are the approaches for Internet governance within sub-continental frameworks (eg. ASEAN in Southeast Asia)?
17. How can regional Internet cooperation go beyond infrastructure (eg. backbone network design) to cultural issues (eg. language) and governance?

Questions related to Chapter III:

1. Is there a right to access to the Internet and how can it be best realised?
2. What are examples of good practice?
3. How can the Internet be used to strengthen democracy and an empowering discourse? What are the opportunities and risks involved?
4. What are the main issues of consumer protection on the Internet?
5. How to strengthen the rights of users?
6. How should Internet users think of themselves as not just consumers but citizens (eg. engage in socio-political empowerment and not just business)?
7. How does Internet access relate to telecom access, postal service access, and educational access as a government responsibility and citizen right?
8. What comparative frameworks can be used for assessing performance of different countries over time, in terms of Internet access?
9. How has the mobile Internet added new notions of democratic and ubiquitous citizen expression?
10. What new dimensions of media does broadband Internet bring to the expressive power of citizen?
11. How does the rise of citizen journalism and mobile journalism modify existing rights of the traditional media (eg. freedom of the press)?
12. How can new forms of 'publishing' on the Internet such as microblogging (eg via Twitter) be protected by existing copyright regimes?
13. What acceptable use guidelines and ethical principles apply to user-generated content?
14. How can open access coexist with traditional publishing?

Questions related to Chapter IV (Working Groups A-D):

A. Freedom of Expression

1. What existing mass media provisions for freedom of expression need to be extended to digital media?
2. What existing provisions for freedom of digital expression need to be extended to successive waves of ICTs like mobile access?
3. What challenges do global ICTs like the Internet pose for national hate speech regulations?
4. What challenges do anti-terrorism laws pose for freedom of expression, and how can a balance be maintained?
5. How can freedom of expression be protected across different regulatory domains in the face of convergence, ie. telecom regulation, broadcast media regulation, print regulation?
6. What new commercial forces pose challenges to freedom of expression, eg. the power of social networking sites like Facebook and Twitter?

7. How can existing advocacy groups leverage ICTs to increase awareness about freedom of expression and mobile citizens around the world?
8. What are the opportunities and challenges posed by 'armchair activism' on the Internet, to democratic processes?
9. What are the rights and responsibilities of whistleblowing sites and activists on the Internet? What opportunities do they open up for pro-democratic and openness advocates, and what challenges do they pose for diplomats and traditional media? How has existing and emerging jurisprudence helped to resolve these issues?
10. Sensor-based networks open up opportunities for governments and companies to engage in widespread surveillance of citizens. What challenges do these pose for free-speech and privacy advocates?

B. Privacy and Data Protection

1. What are the main challenges for the human right to privacy and data protection in the context of the Internet?
2. Should there be a global standard for privacy and data protection or should regional or cultural aspects be taken into account?
3. Are the international or European regulations going beyond national standards or are they rather a minimum standard? Has the Internet led to new conceptions of privacy?
4. Are the orientations presented by the European Commission in order to revise the European Data Protection Directive of 1995 satisfactory in terms of HR protection?
5. What are the main principles for the protection of privacy and personal data in an ICT environment?
6. Do the nine principles contained in the resolution of the Parliamentary Assembly of the Council of Europe form a sound basis for data protection and for privacy in general?
7. What are the challenges to privacy stemming from the use of social networks and how to address them?
8. What exceptions or limitations are legitimate to the right to privacy and data protection, in particular for security purposes?
9. What are the main remedies against violations of privacy and data protection and against which actors can they be addressed?
10. What rights to consumers have with respect to protecting their location and communication data from abuse by operators?
11. What rights to citizens have with respect to protecting their location and communication data from abuse by governments?
12. How can governments protect citizens from threats like terrorism, via interception of mobile messages from terrorists – while also not tramping on citizen privacy?
13. What new consumer forums are emerging in the arena of mobile data protection, and how are they linking together internationally?
14. What new tools and technologies are emerging in the area of mobile encryption, and how do they affect the privacy v/s security debate?

C. Digital Divide and Sustainable Development

1. What divides are successive waves of digital media closing – and opening? Eg. narrowband and broadband?
2. What kinds of rights ride on digital access and how can the rights divide be reduced for those without such access?
3. How can provisions for access to digital content and services by marginalised and under-served communities be enhanced? Eg. W3C and access to differently abled users.
4. How can national ICT industries work with policymakers to bridge the digital divide?
5. How can provisions be made to ensure that rural and under-served communities get adequate access to ICTs?

6. How effective have Universal Service Obligations and Funds been to bridge the digital divide in remote areas?
7. How does the fragmentation of the Internet create new kinds of divides and how can these be overcome?
8. How can definitions of the digital divide be extended beyond just Internet/mobile access, to content and services such as e-health and m-learning?
9. What kinds of progressive legislations and policies are being passed by governments to ensure that digital access is a basic right?

D. Cultural Diversity on the Internet

1. What are the elements and the main concerns regarding cultural diversity?
2. What are the opportunities and threats involved?
3. Has the vision of the WSIS (at least partly) come true?
4. What are the elements of a possible right to cultural enjoyment on the Internet?
5. How to achieve multi-lingualism and more local content on the Internet?
6. How to take the needs of minority populations, indigenous or marginalised groups better into account?
7. What can be the role of UNESCO, the IGF or regional efforts to achieve the rights to cultural enjoyment on the Internet?
8. How can linguistic diversity on the Internet go beyond IDNS to actual content promotion and preservation policies, especially for endangered languages?
9. How does the Internet promote globalisation and homogenisation while also supporting localisation and local content generation?
10. What new measures and frameworks will emerge to compare online cultural strengths and performances of different countries?
11. How can emerging platforms like mobile Internet promote cultural diversity, eg. via message greetings and proverbs in endangered languages?

Acronyms

ACTA	Anti-Counterfeiting Trade Agreement
AoC	Affirmation of Commitments
APC	Association for Progressive Communication
ASEM	Asia Europe Meeting
ASO	Address Supporting Organization
CCNSO	Country Code Name Supporting Organisation
CCPR	Human Rights Committee
CCTV	Closed Circuit Television
CISPA	Cyber Intelligence Sharing and Protection Act
DNS	Domain Name System
DoC	Department of Commerce
DPI	Deep Packet Inspection
ECHR	European Convention of Human Rights
ECJ	Court of Justice of the European Union
ECtHR	European Court of Human Rights
EuroDIG	European Dialogue on Internet Governance
G8	Group of Eight
GA	General Assembly
GAC	Governmental Advisory Council
GIS Watch	Global Information Society Watch
GNSO	Generic Names Supporting Organisation
HRIA	Human Rights Impact Assessments
IANA	Internet Assigned Numbers Authority
IBSA	India, Brazil and South Africa
ICANN	International Association of Assigned Names and Numbers
IG	Internet Governance
IGC	Internet Governance Caucus
IGF	Internet Governance Forum
IRP	Internet Rights and Principles Coalition
IRT	International Telecommunication Regulations
ISPs	Internet Service Providers
ITU	International Telecommunications Union
MAG	Multistakeholder Advisory Group
MNCs	multinational corporations
MoU	Memorandum of Understanding
MPEPIL	Max Planck Encyclopedia of Public International Law
NGOs	Non-governmental Organizations
NTIA	National Telecommunications and Information Administration
NWICO	New World Information and Communication Order
OECD	Organization for Economic Cooperation and Development
ONI	Open Net(work) Initiative
PIPA	Protect IP Act
RFC	Request for Comments
RFID	Radio-Frequency Identification
SOPA	Stop Online Piracy Act
TRIPS	WTO Agreement on Trade-Related Aspects of Intellectual Property
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organisation

WCIT-12	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WSIS	World Summit on Information Society
WTO	World Trade Organization

Selected Bibliography

Books

Benedek, Wolfgang; Bauer, Veronika and Kettemann, Matthias C. (eds.) (2008). Internet Governance and the Information Society: Global Perspectives and European Dimensions, Utrecht: Eleven, 31-49.

Bollier, David (2009). How the Commoners Built a Digital Republic of Their Own. The New Press.

Bruck, Peter and Rao, Madanmohan (2013-forthcoming). Global Mobile: Scenarios and Strategies. New Jersey: InfoToday/Perseus Publishing.

Castells, Manuel (2000), The Information Society: Economy, Society and Culture. Vol. 1, The Rise of the Network Society, 2nd ed., Oxford: Blackwell, originally published in 1996.

Elsayed-Ali, Sherif (2012), <http://www.egyptindependent.com/node/601891>.

Fidler, Roger (1997). Mediamorphosis: Understanding New Media. California: Pine Forge Press.

Frederick, Howard (1993). Global Communications and International Relations. Belmont, California: Wadsworth Publishing Company.

Gan, Steven; Gomez, James and Johannsen, Uwe (2003). Asian Cyberactivism: Freedom of Expression and Media Censorship. Bangkok: Friedrich Naumann Foundation.

Horst, H. and Miller, D. (2006). The cell phone: An anthropology of communication. New York, NY: Berg.

Howard, P. H. (2004). Society Online: The Internet in context. Thousand Oaks, CA: Sage Publications.

Jørgensen, Frank Rikke (2006). Human Rights in the Global Information Society, Cambridge, MA: MIT Press, <http://mitpress.mit.edu/catalog/item/default.asp?tttype=2&tid=10872>.

Kaku, Michio (2011). Physics of the Future: The Inventions That Will Transform Our Lives. New York: Penguin Books.

Kindberg, T.; Bardram, J.; Buttrich, S.; Esbensen, M.; Houben, S.; Khaled, R. and Tabard, A. (2011). Mesh Mobs: Virtually Augmented Crowds. Copenhagen: IT University of Copenhagen.

Kulesza, Joanna (2012). International Internet Law, London: Routledge.

Kurbalija, Jovan (2010). An Introduction to Internet Governance, 4th ed.

Lessig, Lawrence (2008). Remix: Making Art and Commerce Thrive in the Hybrid Economy. New York: The Penguin Press.

Lessig, Lawrence, Code (2006). Version 2.0, New York: Basic Books, <http://codev2.cc>.

MacKinnon, Rebecca (2012). Consent of the Networked. The Worldwide Struggle for Internet Freedom, New York: Basic Books, <http://consentofthenetworked.com>.

Malcolm, Jeremy (2008). Multi-Stakeholder Governance and the Internet Governance Forum, Perth: Terminus Press.

Mayer-Schönberger, Viktor (2009). Delete. The Virtue of Forgetting in the Digital Age, Princeton University Press.

McCaughey, Martha and Ayers, Michael (2003). Cyberactivism: Online Activism in Theory and Practice. New York: Routledge.

McDonald, QC.; John, Ross Crail and Clive, Johns (2009). The Law of Freedom of Information, 2nd edition, Oxford University Press.

Morozov, Evgeny (2011). The Net Delusion - How not to Liberate the World, London: Allen Lane, <http://netdelusion.com>.

Post, David G. (2012). In Search of Jefferson's Moose. Notes on the State of Cyberspace, New York: Oxford University Press, <http://ukcatalogue.oup.com/product/9780199858217.do>.

Rao, Madanmohan (2009). ICT4D: Learnings and Best Practices. Singapore: AMIC.

Rao, Madanmohan (2003). News Media and New Media: The Asia-Pacific Internet Handbook. Singapore: Eastern Universities Press.

Rheingold, H. (2002). Smart Mobs. Cambridge, U.K.: Perseus Books.

Seneviratne, Kalinga and Yeo, Lay Hwee (2011). Balancing Civil Rights and National Security. Singapore: AMIC and European Union Centre in Singapore.

Sullivan, N. P. (2007). You can hear me now: How microloans and cell phones are connecting the world's poor to the global economy. San Francisco, CA: Jossey-Bass.

Winston, B. (1998). Media Technology and Society: A History: From the Telegraph to the Internet. London: Routledge.

Zeff, David (2002). China Dawn: The Story of a Technology and Business Revolution. New York: Harper Business.

Articles

Bahague, Rick and Banks, Ken (2008). Mobiles in a Box: Tools and Tactics for Mobile Advocacy, <http://mobiles.tacticaltech.org>.

Benedek, Wolfgang (2008). Internet Governance and Human Rights. In: Benedek, Wolfgang; Bauer, Veronika and Kettemann, Matthias C. (eds.) (2008). Internet Governance and the Information Society: Global Perspectives and European Dimensions, Utrecht: Eleven, 31-49.

Benedek, Wolfgang (2011). Multi-Stakeholderism in the Development of International Law. In: Fastenrath, Ulrich; Geiger, Rudolf; Khan, Daniel-Erasmus; Paulus, Andreas; von Schorlemer, Sabine and Vedder, Christoph (eds.). From Bilateralism to Community Interest. Essays in Honour of Bruno Simma, Oxford: Oxford University Press, 201-210.

Coldewey, Devin (2012), <http://techcrunch.com/2012/01/05/is-the-internet-a-human-right/>.

Crawford, Jamie (2012), <http://security.blogs.cnn.com/2012/01/30/the-unseen-global-revolution/>.

Daily Caller (2012), <http://dailycaller.com/2012/01/08/internet-access-not-a-human-right-says-father-of-the-internet/>.

Donner, J. (2008). Research approaches to mobile use in the developing world: A review of the literature. *The Information Society: An International Journal*, 24, 140-159.

Downing, John (1989). Computers for Political Change: PeaceNet and Public Data Access. *Journal of Communication*, Summer 1989.

Ershadi, Julie (2012), <http://reason.com/blog/2012/01/24/iranian-exiles-protest-halal-internet>.

Financial Times (2012), <http://www.ft.com/intl/cms/s/0/04b98446-4112-11e1-b521-00144feab49a.html?ftcamp=rss#axzz1I3bRZVGZ>.

German Commission for UNESCO/Asia-Europe Foundation (2010). Mapping Cultural Diversity – Good Practices from Around the Globe, http://www.unesco.it/_filesDIVERSITAculturale/Publication_DUK.pdf.

Greenleaf, Graham (2011). Asia-Pacific Data Privacy: 2011, Year of Revolution?, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1914212.

Guardian (2012), <http://www.guardian.co.uk/law/2012/jan/11/is-internet-access-a-human-right?newsfeed=true>.

Hamelink, Cees (1990). Information Imbalance: Core and Periphery. In: *Questioning the Media: A Critical Introduction*, by Downing, John; Mohammadi, Ali and Sreberny-Mohammadi, Annabelle (eds). Newbury Park, California: Sage.

Harp, D.; Bachmann, I.; Rosas-Moreno, T. C. and Loke, J. (2010). Wave of Hope: African American Youth Use Media and Engage More Civically, Politically Than Whites. *The Howard Journal of Communications*, 21 (3), 224-246.

Harzog, Bernd (2012). SOPA and PIPA, <http://www.virtualizationpractice.com/the-sopa-and-pipa-kerfluffle-14272/>.

Harris, R. J. (2004). *A Cognitive Psychology of Mass Communication* (4th ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Howard, A. L. (2010). Engaging the City: Civic Participation and Teaching Urban History. *Journal of Urban History*, 36 (1), 42-55.

Human Rights First (2012), <http://www.humanrightsfirst.org/2012/01/30/learning-from-egypts-internet-and-cellphone-shutdown/>.

Kellner, D. and Share, J. (2007). Critical Media Literacy, Democracy, and the Reconstruction of Education. In: Macedo, D. and Steinberg, S. R. (eds.), *Media literacy: A reader* (3-23). New York: Peter Lang.

Kettemann, Matthias C. (2010). Ensuring Human Rights Online: An Appraisal of Selected Council of Europe Initiatives in the Information Society Sector in 2010. In: Benedek, Wolfgang; Benoît-

Rohmer, Florence; Karl, Wolfram and Nowak, Manfred (eds.), European Yearbook on Human Rights 2010, Vienna: Neuer Wissenschaftlicher Verlag, 461-482.

Kleinwächter, Wolfgang (2011). Towards an Improvement of the IGF: Eight proposals for an enhanced role of the IGF, 14.03.2011, http://www.unctad.info/upload/CSTD-IGF/Contributions/M1/Wolfgang_Kleinwachter.pdf.

Kleinwächter, Wolfgang. Internet principle hype: how softlaw is used to regulate the Internet, dotnxt, <http://news.dot-nxt.com/2011/07/27/internet-principle-hype-anon>.

Lunn, Meagan (2012). Social Media to Preserve Endangered Languages, <http://www.koreaittimes.com/story/19919/social-media-preserve-endangered-languages>.

McIver, William and Birdsall, William (2002). Technological Evolution and the Right to Communicate: The Implications for Electronic Democracy. Euricom Colloquium: Electronic Networks & Democracy, Nijmegen, The Netherlands.

Murphy, Brian (1994). Addressing Crises Through New Channels In The Psot-NWICO Era: Alternative News Agencies, And The Computer Networks Of Non-Governmental Organizations. Journal of International Communication, Vol. 1, No. 1, 1994.

Myers, Steve (2012). Meltwater says AP's copyright lawsuit threatens all search engines, <http://www.poynter.org/latest-news/mediawire/171382/meltwater-says-aps-copyright-lawsuit-threatens-all-search-engines/#more-171382>.

National Post (2012), <http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine/>.

Palfrey, John (2012). "Alternative Compensation Systems for Digital Media", <http://blogs.law.harvard.edu/palfrey/alternative-compensation-systems-for-digital-media/>.

Rafaeli, Sheizaf and LaRose, Robert (1993). Electronic Bulletin Boards and "Public Goods" Explanations of Collaborative Mass Media. Communication Research, Vol. 20, No. 2, April 1993.

RT Network (2012), <http://rt.com/news/poland-acta-protest-anonymous-823/>.

Southwood, Russell (2011), <http://www.apc.org/en/node/12433/>.

Stewart-Smith, Hana (2012), <http://www.zdnet.com/blog/asia/north-korea-makes-cellphone-usage-a-8216war-crime-under-100-days-of-mourning/834>.

Sydney Morning Herald (2012), <http://www.smh.com.au/opinion/politics/planned-us-antipiracy-laws-a-draconian-mess-20120118-1q5z0.html>.

The Economist (2012), <http://www.economist.com/node/21542748>.

The Independent (2012), <http://www.independent.co.uk/news/world/asia/thailand-backs-twitter-censorship-policy-6297296.html>.

Tsukayama, Hayley (2012). Pinterest addresses copyright concerns, http://www.washingtonpost.com/business/technology/pinterest-addresses-copyright-concerns/2012/03/15/gIQAijAFES_story.html.

Weber, Rolf H. (2010). New Sovereignty Concepts in the Age of Internet, Journal of Internet Law, August 2010, 12-20.

Weber, Rolf H. (2011). Shift of legislative power and multi-stakeholder governance, *International Journal of Public Law and Policy* 1, 4-22.

VOA (2012), <http://www.voanews.com/khmer-english/news/US-Internet-Piracy-Bills-Find-Little-Support-in-Cambodia-137766413.html>.

YNet News (2012), <http://www.ynetnews.com/articles/0,7340,L-4223280,00.html>. Reporters Sans Frontiers <http://en.rsfs.org/>.

Documents on Internet Governance

Centre for Law and Democracy, *A Truly World-Wide Web: Assessing the Internet from the Perspective of Human Rights*, Halifax, Canada, April 2012, <http://www.law-democracy.org/wp-content/uploads/2012/04/final-Internet.pdf>.

Council of Europe, Declaration by the Committee of Ministers on Internet governance principles, adopted on 21.09.2011, <http://goo.gl/RxDWs>.

G8 Declaration, Renewed Commitment for Freedom and Democracy, G8 Summit of Deauville, 26.-27.05.2011, <http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html>.

IBSA Joint Statement, Open consultations on Enhanced Cooperation, New York, 14.12.2010, <http://www.un.int/india/2010/IBSA%20STATEMENT.pdf>.

Internet Rights and Principles Coalition, 10 Internet Rights and Principles, <http://internetrightsandprinciples.org>.

Internet Rights and Principles Coalition, Charter of Human Rights and Principles for the Internet, <http://internetrightsandprinciples.org/node/367>.

Letter dated 12.09.2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, 14.09.2011, A/66/359.

OECD Communiqué on Principles for Internet Policy Making, OECD High Level Meeting: The Internet Economy: Generating Innovation and Growth, 28.-29.06.2011, Paris, <http://www.oecd.org/dataoecd/40/21/48289796.pdf>.

OSCE, 8th South Caucasus Media Conference, Declaration: Pluralism and Internet governance, Tbilisi, Georgia, 20.-21.10.2011, <http://www.osce.org/fom/84371>.

President of the United States of America, *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Report of the Working Group on Internet Governance (2005), <http://www.wgig.org/docs/WGIGREPORT.pdf>.

Reporters without Borders, Enemies of the Internet, Report (2012), <http://march12.rsf.org/en/#ccenemies>.

Secretary of State Hillary Rodham Clinton, Internet Rights and Wrong: Choices and Challenges in a Networked World, George Washington University, Washington, D.C., 15.02.2011, <http://www.state.gov/secretary/rm/2011/02/156619.htm>.

The 2012 Internet Society Global INET, http://www.elon.edu/e-web/predictions/isoc_20th_2012/intellectual_property_innovation.xhtml.

UN, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/17/27 of 26.04.2011.

UNESCO, Code of Ethics for the Information Society, proposed by the Intergovernmental Council of the Information for All Programme (IFAP), 36 C/49, 10.10.2011, <http://goo.gl/nZ0Ik>.

Vice-President of the European Commission Neelie Kroes, Internet Compact, <http://blogs.ec.europa.eu/neelie-kroes/i-propose-a-compact-for-the-internet/#more-671>.

World Summit on the Information Society (WSIS), Geneva Declaration of Principles, WSIS-03/GENEVA/DOC/4-E of 12.12.2003.

World Summit on the Information Society (WSIS), Geneva Plan of Action, WSIS-03/GENEVA/DOC/0005 of 12.12.2003.

World Summit on the Information Society (WSIS), Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E of 18.11.2005.

World Summit on the Information Society (WSIS), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18.11.2005.