Asia-Europe Meeting

12th Informal ASEM Seminar on Human Rights

"Human Rights and Information and Communication Technology"

27-29 June 2012
Seoul, Republic of Korea

Human Rights and Information and Communication Technology

Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights

27 – 29 June 2012

Seoul, Republic of Korea

The Informal ASEM Seminar on Human Rights Series is a partnership between:

ASIA-EUROPE FOUNDATION

RAOUL WALLENBERG INSTITUTE OF HUMAN RIGHTS AND HUMANITARIAN LAW

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET EUROPÉENNES

DEPARTMENT OF FOREIGN AFFAIRS
REPUBLIKA NG PILIPINAS
PHILIPPINES

The 12th Informal ASEM Seminar on Human Rights was hosted by:

National Human Rights Commission of Korea

MINISTRY OF FOREIGN AFFAIRS
MOFA
외교부
Ministry of Foreign Affairs

Published by:
Asia-Europe Foundation
31 Heng Mui Keng Terrace
Singapore 119595

Designed and Printed by:
Xpress Print Ltd
No 1 Kallang Way 2A
Singapore 347495

ISBN: 978-981-07-5715-1

Human Rights and Information and Communication Technology, Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights

Copyright © 2013. All rights reserved. No part of this publication may be reproduced without the prior permission of the publishers.

Views expressed here do not necessarily reflect those of the co-organisers, publisher or editors of this volume.

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 (ASEF), the Raoul Wallenberg Institute, the French Ministry of Foreign Affairs, the Philippine Department of Foreign Affairs, the Korean Ministry of Foreign Affairs and the National Human Rights Commission of Korea.

Contents

Acknowledgements

Ambassador ZHANG Yan

Executive Director, Asia-Europe Foundation (ASEF)

The 12th Informal ASEM Seminar on Human Rights provided a timely platform for the discussion of the complex issues relating to information technology and human rights debate. It is hoped that the expert knowledge and experience shared by the participants over the course of the 3-day seminar in Seoul will reach a wider audience through the publication of this volume, and will contribute to the overall strengthening of human rights dialogue across the two regions. On behalf of the organisers I would like to express my deepest appreciation to those who facilitated the programme from start to finish.

Our thanks go firstly to the 120 seminar participants, who represented governments and civil society across Asia and Europe. Without their co-operation in sharing frankly and openly their diverse experiences in the field of human rights and information and communication technology, this dialogue and the resultant findings laid out in this publication would not have been possible. It is our sincere hope that connections made among the participants in Seoul provide the basis for continued strengthening of networks between the two regions.

Our profound appreciation goes to the seminar hosts, the Ministry of Foreign Affairs and Trade of the Republic of Korea (MOFAT) and the National Human Rights Commission of Korea (NHRCK) for their kind and generous hospitality. We would especially like to thank Second Vice Minister of Foreign Affairs, Mr. Kim Sung-han and the Chairman of the NHRCK, Mr. Byung-Chul Hyun for their welcome address. Also from MOFAT, thanks goes to Ambassador Kim Sam-hoon, Mr. Lee Wook-heon and Ms. Kim Boram for their cooperation and kind assistance during this Seminar.

As the local Seminar host, the NHRCK played such a vital role in the success of the Seminar. In particular, we would like to thank the Director General of Human Rights Education and Policy Bureau, Mr Seokmo An, and his colleagues, especially Mr Seok-Jun Ri, Mr Yunkul Jung and Mr Seunggi Hong for their tireless dedication to the preparation of the Seminar. We could not have coordinated this three-day Seminar without their kind support.

The informative addresses on information technology and human rights which were provided by our distinguished keynote speakers, Ms. Agnes Callamard and Mr. Pavan Duggal, set the tone of the whole seminar, and for this we are indebted.

We are deeply grateful to the two main seminar rapporteurs, Dr. Wolfgang Benedek and Dr. Madanmohan Rao who not only prepared a detailed and comprehensive Background Paper but also compiled the final Seminar Report for this publication. We are also deeply appreciative of the work of Dr. Dieter Zinnbauer and Dr. Delia Browne in capturing the discussions and proposals of their respective working groups. Thanks also go to Mr. Matthias C. Kettemann for his contribution to these documents.

Thanks to the knowledge and skilful facilitation of Mr. Rolf Ring, Mr. Al Alegre, Mr. Kavi Chongkittavorn and Mr. Paul Keller, the Seminar discussions proved to be particularly fruitful. The topic of human rights is sensitive and challenging, and we greatly appreciate their work in balancing the diversity of opinion within the working groups.

We would like to express sincere gratitude to our partners, the French Ministry of Foreign and European Affairs, the Raoul Wallenberg Institute, and the Department of Foreign Affairs of the Philippines. The insight and advice of our partners, coupled with the input of the members of our Steering Committee, ensured a strong and relevant seminar programme. We have to note the contributions of our former colleagues at the Asia-Europe Foundation: Ambassador Michel Filhol, Ms. Sol Iglesias, Ms. Anjeli Narandran and Mr. Christopher Massey who all contributed to the 12th Seminar.

Finally, we thank the Seminar's secretariat staff at the Asia-Europe Foundation (ASEF): Mr Thierry Schwarz, Ms Ratna Mathai-Luke, Ms Grace Foo and Ms Xue Linyan. Their hard work and diligence brought this Seminar from the planning stages, through execution, to the ultimate publication of this volume.

Preface

Mr Thierry SCHWARZ
Director for Intellectual Exchange, Asia-Europe Foundation (ASEF)

The Informal ASEM Seminar On Human Rights Series

The Asia-Europe Meeting (ASEM) brings together 49 Asian and European countries as well as the European Commission (EC) and the ASEAN Secretariat. The ASEM process aims at strengthening interaction and mutual understanding between the two regions and at promoting cooperation leading to sustainable economic and social development. It's an informal process of dialogue and cooperation among partners on all issues of common interest to Asia and Europe.

The biennial ASEM Summit meeting is held alternately in Asia and Europe and is the highest level of decision-making in the process, featuring the Heads of States or Heads of Governments, the President of the European Commission, accompanying ministers and other stakeholders. A total of nine Summit meetings have been held in the cities of Bangkok (1996), London (1998), Seoul (2000), Copenhagen (2002), Hanoi (2004), Helsinki (2006), Beijing (2008), Brussels (2010) and Vientiane (2012).

At the first meeting of ASEM Foreign Ministers in Singapore in 1997, Sweden and France offered to organize informal seminars on human rights to be held within the ASEM framework. In 2011, the Philippines joined ASEF, Sweden and France as a co-organiser of the Seminar series.

The series employs the following formula:

- A balanced representation between civil society participants from Asia and Europe (invited by the organisers) and official representatives (nominated by the 51 ASEM members) in each Seminar;
- Closed-door debates to allow free and direct exchanges of views; and,
- A set of recommendations, elaborated collectively to be sent to the relevant institutions in ASEM countries as an informal contribution to the official Asia-Europe dialogue.

The experience of the first twelve seminars has proven the usefulness of the chosen formula: a climate of confidence and mutual understanding, in accordance with the ASEM spirit, has grown stronger throughout this process.

The 12th Informal ASEM Human Rights seminar on Human Rights and Information and Communication Technology was attended by 120 participants representing 42 ASEM partners, including delegates from national regulatory authorities, technology promotion bodies, diplomats, human rights activists and internet experts, to discuss the complex relationship between information technology and human rights, and to share their own knowledge and experiences on the topic.

Human Rights and Information And Communication Technology: An Overview Of This Volume

This volume contains the proceedings of the Seminar. In addition to the official opening speeches made by the host and the organisers, it includes the keynote speeches of Ms. Agnes Callamard (Executive Director, ARTICLE19) and Mr. Pavan Duggal (Advocate, Supreme Court of India and President Founder of Cyberlaw Asia) who in introducing the Seminar topic, highlighted current issues (for example, the arrest and extradition of Richard O'Dwyer, the British founder of an online movie search engine, for copyright violations in the US) which raised pertinent questions regarding the governance, access and the role of different stakeholders in navigating the complex relationship between human rights and ICTs.

The Background Paper is the preliminary annotation to the 12th Seminar. It was prepared by Dr. Wolfgang Benedek, Director of the Institute of International Law and International Relations of the University of Graz, and of the European Training and Research Centre for Human Rights and Democracy of the University of Graz, Austria, and Dr. Madanmohan Rao, Research advisor at the Asian Media Information and Communication Centre (AMIC) and Editor of The Asia-Pacific Internet Handbook. The Seminar Report, co-written by Dr. Benedek and Dr. Rao, as well as the two other Working Group rapporteurs, Dr. Dieter Zinnbauer and Dr. Delia Browne, constitutes the fundamental part of this publication, together with the Background Paper. These papers provide an introductory overview of the key issues discussed in

each of the Working Groups as well as the essence of discussions and debates that took place in them. The working groups addressed the following topics:

1) Freedom of Expression
2) Right to Privacy
3) Digital Divide, and
4) Right to the Cultural Enjoyment of the Internet

Among the key messages raised at the Seminar the following ones were deemed of particular relevance:

- The safeguards that exist for human rights protection should be equally applied online. Government restrictions on ICT usage should be provided by law and pursue specific public welfare interests;

- Governments need to ensure that the public interest balance is maintained and recognised in domestic IP legislation and international treaties and agreements. The rights of users and public institutions – and the fundamental rights and freedoms such as freedom of expression, right to information, right to privacy – should be positively affirmed.

- Digital education and capacity-building about the appropriate use of new media is needed for all citizens and communities. In particular, States should ensure that technology tools and ICT skills education are available in as many minority, ethnic and indigenous languages as possible

The volume ends with concluding remarks from two of the co-organising partners, Ambassador Olof Ehrenkrona, Political Ambassador and Senior Advisor to the Minister for Foreign Affairs (on behalf of the Raoul Wallenberg Institute), and Mr Frédéric Tiberghien, Representative of the Ministry of Foreign and European Affairs of France, who summarise the discussions.

Opening Speech

Professor Byung-Chul HYUN
Chairperson, National Human Rights Commission of Korea
(Opening Speech on behalf of the National Human Rights Commission of Korea)

Dear ladies and gentleman, I'm glad to see you.

My name is Byung Chul Hyun, and I am the chairperson of the National Human Rights Commission of Korea.

Firstly, I would like to thank and welcome all of you who came to attend to the 12th Informal ASEM Seminar on Human Rights. Especially thank you for to those who came from abroad to represent their home countries, their fields of study, and civil societies of Asia and Europe.

Also I would like to welcome and thank all our domestic guests who came from various government branches, diverse specialised areas, and civil society in Korea. Starting today, we are going to proceed the three-day seminar regarding "Human Rights and Information Communication Technology" in order to communicate and cooperate with each other and reaffirm the universal value of human rights.

As we all know, recent developments in Information Communication Technology devices have brought us from an analog world to, a modern digital world, and have changed our life-styles in various aspects.

Now we are living in a world where everyone can have access to the internet ubiquitously, communicate regardless of time and space, generate a personal opinions on international issues, and produce and consume contents no irrespective of who they are.

While so many of us are benefitting from modern developments of Information Technology (IT), the astronomical speed in which IT is developing also means that various problems are also rapidly rising such as leakage of personal information, 'Big Brother' and Surveillance Society, SNS and the issue of freedom of expression.

In fact, leakage of personal data due to hacking; monitoring through CCTV; violation of the right to personality due to excessive freedom of expression in cyber space; disconnection of access to internet via IT gadgets; digital divide; and the issue of copyrights derived from the production and duplication of contents are the challenges that we must resolve as we live in a digital world.

The Republic of Korea (ROK) is known as one of the IT advanced countries, and thus ROK also faces the strong demand for standardised criteria for human rights in IT field.

During this Informal ASEM Seminar for Human Rights, the participants from the ASEM countries will together discuss all these problems in relation to human rights - especially the fact that everyone has the right to enjoy the benefits from the advancement of technology, as stated under the UDHR, ICCPR, and ICESCR.

Thus, I wish that ASEM members including ROK will share their experiences and concerns as well as discuss this pending issue thoroughly with experts of the field from all over the world.

Through this event, I wish we can identify the cause and find appropriate resolutions to each problem of each field such as the right to privacy, the digital divide, and the right to enjoyment of culture on the internet.

Lastly, I would like to express my heart-felt gratitude to ASEF and Ministry of Foreign Affairs and Trade of Korea for their support and special attention for this seminar.

NHRCK will do its best to support and assist this seminar to conclude it with a meaningful result.

Once again, thank you everyone who came to this place and wish you the best. Thank you.

Opening Speech

Mr KIM Sung-han
Second Vice Minister, Ministry of Foreign Affairs
(Opening Speech on behalf of the Host, Republic of Korea)

Distinguished participants and guests from home and abroad,

I am indeed honoured to make an opening speech here today and, on behalf of the Korean Government, I would like to extend a wholehearted welcome to all of the participants from the 48 ASEM members.

On the occasion of the first meeting of ASEM Foreign Ministers in Singapore in February 1997, member countries, such as Sweden and France, suggested that informal seminars on human rights be held within the ASEM framework. Since then, the Informal ASEM Seminar on Human Rights has indeed played a valuable role in promoting mutual understanding and cooperation between Asia and Europe.

I am delighted that such a meaningful seminar is being held in Seoul, the Republic of Korea. And I would like to express my deep appreciation to the staff of the Asia-Europe Foundation and National Human Rights Commission of Korea for their hard work, and to the co-sponsors of the seminar – the governments of Sweden, France and the Philippines.

As the relationship between human rights and ICT is attracting more and more attention, the holding of this seminar is indeed most timely. As you may well know, given the impact of ICT on human rights, we might say that it is a kind of double-edged sword. On the one hand, ICT offers us new opportunities and benefits; ones that humankind has never previously enjoyed. On the other hand, the digital divide brings with it an ever increasing gap between the 'haves' and the 'have-nots'.

The task that we now face is to expand the opportunities and benefits provided by ICT and to address the various challenges we face in the information society through determined action.

We believe that ensuring freedom of expression on the Internet is vital in further enhancing the universality of human rights and promoting democracy. In order to protect and promote the right to freedom of expression on the Internet, the Republic of Korea, with its world class Internet infrastructure, is constantly striving to build an Internet which allows for the free exchange of information in a safe environment which people can trust.

At the same time, in order to bridge the digital divide, the Korean Government has been exerting efforts to provide personal computers and technical assistance to developing countries. It has been working on making the Internet more accessible to the less privileged, who remain shut out from the benefits of high-tech information and communication technologies.

I hope that these experiences gained by Korea may serve as a useful basis for discussions among ASEM member countries, under the theme of "Human Rights and Information and Communication Technology."

Throughout history, opportunities created by revolutionary technologies have often brought daunting challenges. However, humanity has succeeded in finding ways to make full use of the positive sides of technology while mitigating its bad. I firmly believe that, in the face of the new challenges such as the restriction on freedom of expression and the digital divide, as we unite in our efforts among ASEM member countries, we too, as has been the case in the past, can overcome the obstacles before us and triumph.

I would like to bring my remarks to a close by expressing once again my sincere wish that this seminar will serve as a valuable opportunity to explore ways to forge strong bonds of cooperation in the fields of ICT and human rights within the ASEM framework. And I would like to wish you a most pleasant and rewarding stay.

Thank you.

Opening Speech

Ambassador Rosario G. MANALO
Foreign Affairs Advisor, Department of Foreign Affairs, Philippines
(Opening Speech on behalf of the Organisers)

Excellencies, Ladies and Gentlemen, distinguished guests,

On behalf of the co-organisers and the Philippine Government, I welcome you all to the 12th Informal ASEM Seminar on Human Rights. I find it truly apt that we are holding this seminar on "Human Rights and Information and Communication Technology" in Korea – a country known worldwide for its advanced Information and Communication Technology (ICT) infrastructure and sophisticated innovations. I would like to thank the Government of the Republic of Korea for their warm hospitality and excellent arrangements for the seminar.

I would also like to take the opportunity to give due credit to the two rapporteurs, Dr Wolfgang Benedek and Dr Madanmohan Rao, for coming up with a very informative background paper for this informal seminar. In fact, it is so effective that it has enabled someone like me – who has been working on the concept of human rights for several decades already but is, at the same time, what ICT experts would call an "older digital migrant" – to speak with some semblance of credibility on the topic.

The evolving nature of ICT: the Internet as an entity in itself

In the same manner that the concept of human rights changed the world's view of how human beings should co-exist, the Internet has altered the way human beings obtain information and communicate with each other. In fact, it can be argued that the Internet singularly ushered in Information and Communications Technology, or ICT, as we use the term today. For it was only with the prevalence of the Internet and all of its peripheral technologies that we began looking at ICTs the way we do now.

Without doubt the Internet is unlike anything the world has seen. It is unlike any of the previous communications platforms that dominated the world. It cannot be compared to other mass media like television, radio or print, as its nature and business models are entirely different. The Internet, therefore, is *sui generis*. As such, it requires a new set of paradigms that shall govern the different aspects of its facilitation, access and use.

Relationships, not definitions

The question of whether access to the Internet is a human right requires a complex but worthwhile discussion. The issue will definitely be polarising and the debate will most certainly be contentious. What cannot be argued, though, is the existence of relationships between the two. The linkages between human rights and ICT are not only evident, they can also be developed and explored to further advance both. Indeed, it can be posited that human rights and ICT can be mutually reinforcing, in that what is good for one is ultimately beneficial to the other.

Our task here, then, is not so much to define one within the frame of the other, but rather to ask questions about their overlaps and linkages and, hopefully, arrive at constructive insights. Our discussions on the working group topics – Freedom of Expression, The Right to Privacy, The 'Digital Divide' and The Right to Cultural Enjoyment of the Internet – shall help us accomplish just that.

Allow me please to give my initial thoughts on these working group topics.

Freedom of Expression and the Right to Privacy

A very good example of the relational dynamics between human rights and ICTs can be found in "freedom of expression". It goes without saying that the right to speak and be heard is helped along by the various modes of communication available to us now.

Opinions can now be published in the form of blogs, while traditional print media now have their web-based incarnations as an alternative outlet. Political and creative content can be broadcast, shared and sold in the form of podcasts and

other downloadables. Not only do people with something to say have more ways of saying it at their disposal, their audiences now also have greater means of providing feedback and being heard. All this interaction makes for a more vibrant democratic dialogue. And if you want examples of this, you need not look farther than the comments section of any YouTube video.

In the Philippines, ten years before the world witnessed how social media fuelled the Arab Spring, Filipinos peacefully overthrew a dictatorial president with the aid of text messages or SMS. The crowd during the second EDSA People Power Revolution of 2001 assembled faster and organised better by communicating through their mobile phones.

Major political events, such as the recent impeachment trial of our Supreme Court Chief Justice, are streamed live online so that people working in their offices can watch them and contribute to the discussions at the cafeteria during lunch.

These are examples of the power of ICT to invigorate the existing liberties that we enjoy. However, we must also recognise the challenges and responsibilities that accompany these benefits. Hate speech, discrimination, cyber-bullying, libel and political slander are also enabled by technology. These should be addressed while balancing the right of Freedom of Expression with the duty of the State to provide security and to protect the right of its citizens to privacy. How to strike this difficult balance should form the crux of discussions on ICT governance.

When the State and the private sector take steps to ensure citizens' Right to Privacy, people are emboldened and they transition from being mere users to becoming active participants. When online transactions are secure and reliable, the ICT economy will flourish, encouraging more participation from the public. In return, an active ICT economy provides more motivation for stakeholders to provide favourable conditions that will sustain growth. This mutually reinforcing relationship will only help advance both Freedom of Expression and the Right to Privacy as institutional norms within the Information Society.

The 'Digital Divide'

The benefits brought about by ICTs need to be shared both between and within countries and across social sectors to advance our development goals. The 'digital divide', which takes many forms and exists on various levels, must therefore be addressed. The role of women, for instance, in policy-making within the ICT sphere must be enhanced. Technological literacy among women, the poor, indigenous peoples and other marginalised groups must be promoted so that they may become not only effective consumers of content, but also empowered players in the information society.

The issue of the digital divide inevitably brings to the fore questions about access and use of ICTs. Whether access to ICTs shall be considered a human right is open to debate. What is certain, though, is that governments and businesses must work together to create a favourable environment and conditions that will allow everyone to enjoy the benefits of ICTs.

In the Philippines, the use of mobile phones expanded at an astonishing rate primarily because telecommunications providers were given the opportunity to develop the prepaid retail market. This innovation made owning a mobile phone easier by doing away with documentary requirements for subscription applications. Users can purchase airtime and SMS credit for as little as US$ 0.50 at a time. It is equally convenient for retailers as they need only a mobile phone to purchase and sell credits to mobile users. The result is that 90% of our population are active mobile phone users. This has set the stage for the dissemination of more advanced mobile-based applications such as mobile banking, social media and others.

This is, of course, just one example among many around the world.

Cultural Diversity and the Right to Cultural Enjoyment of the Internet

The Geneva Declaration adopted at the World Summit on the Information Society (WSIS) proclaimed that "cultural diversity is the common heritage of humankind" and that it is imperative to preserve the same. ICTs are invaluable tools in this endeavour.

On a practical level, for instance, the Internet has helped maintain the Filipino cultural value of close family ties despite the Diaspora of our millions of migrant workers. A Filipino nurse living and working in London can regularly connect with

family and friends back home through Skype, Facebook and other applications. He or she can even send remittances wirelessly using various mobile banking features. These seemingly simple acts have somehow mitigated the social costs associated with labour migration.

On a technical level, while ICTs certainly contribute to the disquieting trend of cultural homogenization in the Information Society, they also hold the immense potential to help in the preservation of cultural heritage by providing platforms for the development and diffusion of diverse cultural content. The question for us, therefore, is how to optimise the use of ICTs in the interest of cultural diversity.

This is just one of the many relevant questions we will tackle in the next few days, and I am confident that we can ably address them with the help of our moderators and rapporteurs.

On this note, I wish you all an enriching and fruitful seminar.

Thank you.

Keynote Speech

Ms Agnès CALLAMARD
Executive Director, ARTICLE 19[1]

I am honoured to speak before you today at this critical moment in history, when the path of information and communication technology and the path of human rights – two fields that years ago, seemed so distant from one another – finally meet. Not only are ICT developments and human rights related, they are now intricately intertwined, and our meeting here in Seoul attests to that fact.

The Current State of ICTs Globally

At this present moment, one-third of the world's population is online with China alone representing almost 25% of all internet users worldwide.[2]

In terms of Facebook, India boasts the second largest number of users in the world – behind only United States where the social media giant originated – with approximately 43.5 million people on the social media network. Indonesia is close behind India with just over 43 million users.[3]

The world's top broadband economies are from Europe and the Asia-Pacific. Europe leads in broadband connectivity, with fixed- and mobile-broadband penetration reaching 26% and 54%, respectively.[4]

How remarkable is it that there are 5.9 billion mobile-cellular subscriptions worldwide? Increasingly, people in the least developed areas of the world are accessing and using the Internet through their mobile phones. Nigeria has a booming financial services economy based on mobile technology; farmers in Kenya access data about market prices on their mobile phones.

While the Arab Spring was not an Internet or twitter revolution, it was probably the first historical example of the incredibly crucial role that information technology can play in liberating people's voices, spreading them around the world, and empowering others to take action. The Arab Spring has exhilarated many human rights activists and has made many others very nervous that the bug could spread.

So the Internet has transformed politics, society, religion, culture and tradition, and is increasingly becoming the medium of choice through which people work, socialise, get involved, associate, act, and express themselves globally.

These transformations have come with a range of problems and challenges not only for governments around the world, but also for private and civil society actors. The Internet knows few boundaries but exists of course in an international system, dominated by nation-states and their corollary: national sovereignty. The co-existence is complicated.

There is still a large number of people around the world, indeed the majority, who, in terms of access to Information Technology, are either *access poor, access denied or access repressed* around the world.

Access poor

According to the ITU, 65% of the world population does not access and use Internet. While the figure is down from 82% in 2006, it is still very high. There is only a 4% internet penetration in Africa, and only 1% of this is broadband based.[5]

Access Denied

A large number of governments around the world have been denying access to the Internet at specific moments in time. For instance, Algeria, Burma, Egypt, Libya, Syria and Tunisia shut down access to the Internet for everyone during periods when they needed to prevent information flowing in and out. A number of countries have large number of highly trained experts carrying out covert hacking activities on dissenting sources of information[6]. According to Freedom House's latest Internet Freedom report, "… In 12 of the 37 countries examined, the authorities consistently or temporarily imposed total bans on YouTube, Facebook, Twitter, or equivalent services."[7]

In a joint statement of May 2011, four international experts mandated by the United Nations (UN), the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE) and the African Union (AU) asserted that cutting off the Internet or parts of the Internet for whole populations or sections of the public can never be justified, including on national security or public order grounds.

---

[1] *ARTICLE 19 is an international human rights organisation which focuses on the defence and promotion of freedom of expression and information world-wide, including Asia and Europe.*
[2] *International Telecommunications Union (ITU), The World in 2011: ICT Facts and Figures, http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf*
[3] *http://www.forbes.com/sites/limyunghui/2012/02/02/india-is-now-facebook-nation-no-2-behind-the-u-s/*
[4] *ITU, op. cit*
[5] *Ibid.*
[6] *See Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom, Basic Books, February 2012*
[7] *Freedom House, Freedom on the Net 2011 Report, New Technologies, Innovative Repression: Growing Threats to Internet Freedom, p. 3*

In its most extreme form, access denied also includes North Koreans who are completely isolated from the rest of the world. There, the government has put in place a national intranet in order to remain isolated from the world. The Iranian government has announced the development of a similar technology.

Access repressed

Many people around the world are access repressed. This includes all those who face jail terms, imprisonment or worse, for using internet or communicating through social media. Online journalists, including bloggers and tweeters, account for the largest number of imprisoned journalists around the world.

According to press freedom organisations, the number of imprisoned online journalists has been through several consecutive years of significant increases. For instance, 69 journalists whose work appeared primarily online were in jail as of 1 December 2010. This constituted nearly half of all imprisoned journalists at that time. In Mexico, tweeters and bloggers have increasingly been targeted by drugs cartels for providing information to the Mexican public, which the traditional media were unwilling to communicate out of fear. As of June 2012, according to Reporters Sans Frontiers, 12 online and citizen journalists have been killed.[8]

The existence of billions of individuals and groups of people around the world who are unable to access the Internet, are prevented from doing so, or are threatened and repressed if they do access it, testifies to the fact that censorship has largely moved online. This includes the imposition of cyber-borders, meant to prevent the flow of ideas and information.

As the excellent Background Paper by the rapporteurs of this conference testifies, the development of the Internet over the last decade is posing very difficult issues and challenges to governments around the world, and indeed, to a range of civil society and private actors as well, regarding issues such as governance, regulation, permissible limits.

There are no simple responses to these challenges, and while the temptation may be great to resort to quick fix solutions, I hope this conference will highlight the need to think outside the box; to challenge pre-conceived ideas; to strengthen our understanding of this new technology and mediums of expression rather than investing energy into unduly restricting them out of fear of the unknown or an innate desire to control.

ICT runs the discovery journey into our century, and we are all on board. Like you, I don't know where the journey is bringing us. I am not even sure I know how we will be traveling since the means of communication evolve so quickly – who tweeted two years ago? But in the remaining time that I have to speak before you, I would like to share what I think should be the possible ground rules to make this journey as useful and agreeable for everyone; some markers to guide us back and forth as we travel.

The first such marker for this journey is fairly self-evident and concerns the limits to free expression online.

I think that we ought to address this issue right at the beginning of the journey and get it right, too. As voiced by the four international experts mandated by the UN, OAS, AU and OSCE to deliver expert advice on freedom of expression, international standards on freedom of expression apply to the Internet, as they do to all means of communication. This means that the traditional human rights paradigm applies to internet.

It is clear that the notion of 'seeking, receiving and imparting information or ideas' also encompasses activities which few societies could tolerate, such as incitement to hatred or murder, or the sale of pornography to children. While the right to freedom of expression is universally recognised as one of fundamental importance, it is therefore also accepted that this right is not absolute.

Certain important public and private interests may justify action by the authorities which interferes with or limits the exercise of the right. A key question, then, is exactly when and under which circumstances does international law permit states to impose such restrictions?

Under Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR), the right to freedom of expression can be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:[9]

for respect of the rights or reputations of others;

for the protection of national security or of public order (ordre public), or of public health or morals.

In addition, and under Article 20 of the ICCPR, freedom of expression must be restricted in situation of incitement to hatred.

International courts have also devised a valid and reasonable three-part test to determine whether a restriction is justified: the restriction must have a clear legal basis; it must pursue a legitimate aim; and it must be necessary for the protection or promotion of the legitimate aim. In order to justify a restrictive measure which interferes with an individual's right to free speech,

---

[8] *Updated figures can be found in Reporters Sans Frontiers' Press Freedom Barometer 2012, http://en.rsf.org/press-freedom-barometer-netizens-and-citizen-journalists.html?annee=2012*

[9] *Article 19 (3) of the International Covenant on Civil and Political Rights, available at http://www2.ohchr.org/english/law/ccpr.htm#art19*

a government must be acting in response to a pressing social need, not merely out of convenience.

In addition, if there exists an alternative measure which would accomplish the same goal in a manner less intrusive to the right to free expression, then the restrictive measure is not in fact 'necessary'. Finally, the measure must impair the right as little as possible and, in particular, must not restrict speech in a broad or untargeted way, or go beyond the zone of harmful speech to rule out legitimate speech. In protecting national security, for example, it is not acceptable to ban all discussion about a country's military forces.

The problem is that, very often, the authorities seek unduly to remove online content which is perfectly legitimate, or in seeking to block access to unlawful content, they block access to entire websites rather than the particular content at issue. The UN Special Rapporteur has recommended that the mandatory blocking of a website should only be ordered by a court. Furthermore, the UN Human Rights Committee (UNHRC) recently confirmed in its General Comment No. 34 on Freedom of Expression that such orders should always be limited in scope, that is to say targeted at particular web pages rather than an entire site. More specifically, the UNHRC stated that permissible restrictions should be content-specific, and that generic bans on the operation of certain sites and systems are not compatible with international law.[10]

Similarly, the prohibition of a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government, is not a permissible restriction under international law. Indeed, this would be akin to censorship.

The second marker on this journey should be to determine and agree how we are going to travel and work together.

After all, there are a number of different actors involved, who are not necessarily used to travelling and working together. I hope we will have time to think through how we want this multi-stakeholder approach to work out and what the ground rules should be. I think this is a fundamental aspect of the challenges confronting us at the moment.

From my standpoint, I think some rules for this multi-stakeholder approach might be outlined as follows:

Online anonymity

Firstly, online anonymity is an important component of freedom of expression but it is not an absolutist principle. Online anonymity matters because it protects and allows individuals to freely express themselves without fear of reprisals.

ARTICLE 19 is in agreement with the UN Special Rapporteur when he wrote that "The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."

On the other hand, in situations where anonymous online users are suspected of a crime, or are subjecting others to vicious harassment, anonymity should be lifted – but only through a legal process, allowing a judge to do so, as it is in the case of requests being made in the 'material world'.

The role of industry

Second, the role of the industry, primarily internet service providers, and the various platform providers, should not include law enforcement. As the law currently stands, in a large number of countries, private sector companies – in particular internet service providers, search engine companies, and other intermediaries – are put in the position where they are required to either remove online content upon notice or face liability, known as 'notice and takedown'.

For instance, news website administrator Chiranuch Premchaiporn was charged under the Computer Crimes Act of 2007 for failing to quickly remove 10 anonymous and allegedly defamatory comments posted to her website. Please bear in mind that she did remove the content when prompted by the authorities, but it just was not fast enough. While her 8 month prison sentence has been suspended, the court did uphold the charge. Her conviction is also in breach of international standards for the protection of freedom of expression[11].

In fact, no one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information. This is the same rule that applies to telephone companies, by the way. Liability should only be incurred if the intermediary has specifically intervened in the content that is published online.

There is, however, plenty evidence around the world, of Internet Service Providers (ISPs) and other intermediaries removing material that is potentially legal in order to avoid liability. Does this matter? I think it does. A great deal in fact.

ISPs have no legitimacy in playing the role of the censors

[10] *United Nations Human Rights Committee, General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf*

[11] *http://www.article19.org/resources.php/resource/1740/en/web-developer%27s-13-year-prison-sentence-another-setback-for-freedom-of-expression*

by removing content. The privatisation of the rule of law, and of law enforcement, is an immensely problematic area of law. It cannot and should not be put in place without proper consultation with all actors concerned, including the users and the companies themselves. Of course, there are arguments behind the current 'notice and takedown' mechanism, given the sheer volume of takedown requests. Google's transparency report shows that there were over 1.9 million copyright removal requests to the search engine made in the past month [May 2012] alone.[12]

However, expediency is not a legitimate argument to justify a government's abuse of the rule of law and due process. Furthermore, blocking and filtering measures constitute a serious interference with freedom of expression. So what can we do instead?

On this ICT journey, we cannot put internet companies in the position of making decisions as to the legality of particular types of content; decisions which they are not best suited, and are often reluctant, to make.

ARTICLE 19 recommends a hybrid system with ISPs and other intermediaries following a due process which will offer some legal certainty. At best, this due process would be a court order. The UN Special Rapporteurs have also recommended that ISPs and other intermediaries should be required to take down content only following a court order. Short of that, we should think of judicial or quasi-judicial mechanisms which would allow for a proper and legitimate process regarding both control and protection of online freedom of expression.

My last marker, as we are pursuing our journey, is a key question we ought to ask ourselves: who is travelling with us?

We ought to remember that, in the space of a decade, the Internet has become ubiquitous in our lives. Not only do we use it to access information that we are interested in, but it has also become increasingly necessary in finding a job, working, studying, and selling and purchasing goods. It has become a basic part of everyday life.

ARTICLE 19 believes that access to the Internet is a human right and that States have a positive obligation to promote universal access to the Internet. Approximately 70% of individuals under the age of 25 – totalling 1.9 billion people – are not online yet. Also, ICT services remain more affordable and available in high-income economies than in low-income economies.[13] In 2010, the cost of ICT services in developed countries averaged at 1.5% of gross national income per capita, as compared to 17% of gross national income per capita in developing countries.[14]

Furthermore, there is a significant divide in the level of Internet bandwidth available per Internet user, with an Internet user in Europe having approximately 45 times more bandwidth available than that of an Internet user in Africa.[15] So surely the final marker in this journey ought to be that there is a universal right to internet, that the Internet is both an enabler of rights, and a right in and of itself. The right to freedom of expression may transcend any particular technology but that does not mean that the particular medium of technology is unimportant.

So the final marker on our journey is that we should do our very best to ensure that we take as many people as possible with us – no one should be left behind because they were late or did not run fast enough or had a bad start. Surely, this is the one journey which everyone should take.

---

[12] *Google Transparency Report available at http://www.google.com/transparencyreport/removals/copyright/*
[13] *ITU, op. cit.*
[14] *Ibid.*
[15] *Disparities between regions in terms of available internet bandwidth per internet user remain, with on average almost 90,000 bit/s of bandwidth per user in Europe, compared with 2,000 bit/s per user in Africa. ITU, op. cit.*

Keynote Speech

Mr Pavan DUGGAL
Advocate, Supreme Court of India and President Founder of Cyberlaw Asia

Ladies and Gentlemen,

The world moves very quickly. Recently, a 24-year-old named Richard O'Dwyer from the UK captured the world's attention. In 2007 he created a website called TVshack.net, a website which enabled users to find free movies online. Through this site, he is said to have committed certain copyright violations in the United States. US authorities have pressed for his extradition and the British government have approved the request. Now only formalities remain.

While this was occurring, the founder of Wikipedia, Jimmy Wales, started an online petition to stop the extradition, arguing that "the internet as a whole must not tolerate censorship in response to mere allegations of copyright infringement. As citizens we must stand up for our rights online. Richard O'Dwyer is the human face of the battle between the content industry and the interests of the general public." Ladies and gentlemen, welcome to the new world of online human rights!

Traditionally, human rights have always been considered as rights existing in the physical world. Consequently, the entire treatment of the concept of human rights has been developed keeping in mind the physical world alone.

The advent of the World Wide Web and the Internet has brought a completely new dimension to our existence: cyberspace. It is one domain that is becoming increasingly relevant in our day-to-day lives. The Pentagon has formally recognised cyberspace as the "fifth domain" in warfare, which has become just as critical to military operations as land, sea, air, and space.

The number of people online is increasing with each passing day. Recent figures pertaining to the total number of people online show a 528.1% increase in users between 2000 and 2011.[1] The Internet has ceased to be merely tool for the exchange of information. It is the paradigm shift of our generation. The Internet is one of the most significant developments in human history after the advent of fire. Since that time, no other event has had such a dramatic and remarkable impact upon the growth of civilization as the creation of the Internet. We now also have social media, which is the flavour of the times. More and more people around the world are joining social networking sites. Today, Facebook has more than 900 million users, which would make it the third most populous nation in the world.[2]

With an increasing number of people online comes a growing expectation of rights and the expectation of the protection of these rights. In that sense, it is increasingly clear that there is a need for recognising existing human rights in cyberspace and on the Internet, and that these human rights are open to being violated by different entities in the cyber world, not necessarily just States but also private entities and internet providers.

These human rights include the following basic human rights:

- The right to access the Internet as part of the basic right to life and human dignity.
- The right to a meaningful life using the Internet.
- The right to use the Internet for living a well-balanced human life.
- The right to freedom of speech and expression on the internet.
- The right to education, knowledge and communication using the internet.

It all started with the creation of the Advanced Research Projects Agency Network (ARPANET) as a military experiment in 1969. Consequently, the World Wide Web came in the early 1990s, which changed the way we communicate. Today, in 2012, at just over four decades of the advent of the Internet, it is time for jurisprudence around the world to evolve in the context of human rights and cyberspace. In fact, the entire concept of human rights has to be expanded to be interpreted in the context of cyberspace, the Internet and ICT. When one examines the jurisprudence of different countries across the world, one finds that there is hardly any development in the said jurisdictions pertaining to legal recognition of human rights in cyberspace. Thus, there is a need for the legislations of different countries to enshrine and specifically recognise in law the concept of human rights in the context of cyberspace.

There is also a need to amend national legislations so that they can be provided with appropriate practices, procedure and processes which institutionalise the process of protection and preservation of human rights in cyberspace as also human rights in the context of Information and Communication Technologies. The

---

[1] *Full statistics can be found at http://ansonalex.com/infographics/online-population-growth-statistics-2012-infographic/#infographic*
[2] *Facebook has Grown Up: Time to Take It Seriously, available at http://www.officingtoday.com/2012/09/facebook-has-grown-up-time-to-take-it-seriously/*

abuse or violation of human rights should be especially condemned and there is a need to provide legal provisions which penalise such violations of such human rights.

When one analyses such scenarios, one often finds that there is an intrinsic conflict between the existence and preservation of human rights on the one hand, and the requirements of national sovereignty, interest, integrity, and defence on the other. The last four decades have demonstrated that the sovereign state would not hesitate to punish any activity in cyberspace which might prejudicially impact or affect any aspects pertaining to national security, integrity, and defence of the relevant sovereign nation.

Violations of human rights in the physical world have had a direct impact in cyberspace. The Arab Spring Revolution is a case in point, which has demonstrated in no uncertain terms that contraventions of basic human rights in the physical world are likely to create rumbles of thunder in cyberspace. These, in turn, can be sufficient to impact and overthrow existing political regimes. There is a need to update and expand the scope and interpretation of the existing international legal instruments relating to human rights. These would include the Universal Declaration of Human Rights (1948), the International Covenant on Economic, Social and Cultural Rights (1966), and the International Covenant on Civil and Political Rights (1966), so as to make the said interpretations relevant to the context of the evolution of ICTs and cyberspace. It is my belief that a Charter on the protection and preservation of human rights in cyberspace should be drawn up and signed.

The existence of a digital divide can be found everywhere, not only between Asia and Europe as continents, but also as regions. In the context of Asia and Europe, there is a need to learn from of each other's experiences.

Cybercrimes today are increasingly gaining the attention of sovereign nations. Broadly speaking there exist today three categories of cybercrime:

- Cybercrimes Against Persons
- Cybercrimes Against Property
- Cybercrimes Against Nations

Cybercrime is also becoming an impediment to the enjoyment of human rights online. The inability of States to bring cybercrime under effective control contributes to the violation of human rights on the Internet.

The popularisation of mobile devices and mobile Internet has given a unique twist to the entire issue. Mobile phones can not only ensure the identification of human rights abuse, but can also be the target of large-scale State surveillance. This has given rise to the emergence of a new branch of law known as Mobile Law, which looks at all legal issues pertinent to the use of electronic devices and portable communication. This legal branch seeks to preserve human rights within the mobile ecosystem.

Clearly, the Internet is no longer a phenomenon, but rather it is a way of life and culture. The right to access and be a part of this way of life and culture is understood as a given, in today's context. I would like to take this opportunity to mention a case study from my home country of India.

The Indian approach is unique and is customised to the needs of India itself. In recent days, a number of media outlets have reported social media censorship in India, but nothing could be further from the truth. Indian ICT legislation has been regularly updated over the years. The Information Technology Act of 2000 was amended in 2008. The Information Technology Rules of 2011 stipulates certain due diligences to be undertaken by intermediaries while discharging their obligations under the law. Clearly, there are challenges in terms of privacy, data protection and cyber-security, but these are currently being worked out through draft legislation pending review. I would argue, therefore, that there are more advantages than challenges in the context of the Indian eco-system.

Indeed, India has long played an important role on the Internet, and the Indian approach to Internet Governance has been shown in the following ways:

- India has been participating in the ICANN process.
- India is a part of the WSIS process and is committed to the Internet Governance Forum (IGF), which it hosted the IGF in Hyderabad in 2008.
- In 2011, India mooted the establishment of a new institutional mechanism in the United Nations for global internet related policies, to be called the United Nations Committee for Internet Related Policies (UN-CIRP).

The intent behind proposing a multilateral and multi-stakeholder mechanism is not to "control the Internet" or to allow Governments to have the last word in regulating the internet. Rather it aims to make sure that the Internet is governed, not unilaterally, but in an open, democratic, inclusive and participatory manner, with the participation of all stakeholders. The idea is that we can develop universally acceptable and globally harmonised policies in important areas, and further pave the way for a credible, constantly evolving, stable and well-functioning Internet that plays its due role in improving the quality of people's lives everywhere.

There is going to be increasing tension between the existence and protection of human rights in cyberspace on the one hand and the inherent rights of nations to protect

and preserve their national sovereignty and security on the other. However, only in obtaining a meaningful balance between the two equally relevant but conflicting directions can there be growth and development of jurisprudence around human rights in ICTs in the future.

It is my belief that nation states must realise that if they continue to trample upon and contravene basic human rights in cyberspace and ICT, there is a likelihood of more 'Arab Spring' type revolutions evolving with much greater intensity. This could have an immense impact upon existing political regimes in different parts of the world. The governments of the world have to realise that cyberspace is a paradigm that cannot be completely and absolutely controlled by the State. Sovereign nations will have to learn to respect, protect and preserve basic human rights in cyberspace. The violation of the same can only be an exception by the State and not by the rule.

There is an underlying necessity to recognise that trammelling or violating basic human rights in cyberspace and ICTs could constitute crimes against humanity. It is indeed time to broaden the scope of definition of the term 'crime against humanity'[3] so as to consider the possibilities of human rights abuse online. As new technologies cannot be predicted, it is important recognise the importance and potential threat cyber-terrorism, cyber-crime, breaches of cyber security, and cloud-computing with all of its ambiguities. There is virtually no work happening in this direction. The beginnings have to be made.

It is in this context that opportunities such as the Informal ASEM Seminar on Human Rights series could be the starting points for the development of steps in that direction. I would urge all delegates at this 12th Seminar to come up with conclusions which will encourage relevant stakeholders to recognise the existence of the concept of basic human rights in cyberspace, and further work towards the evolution and development of jurisprudence around the protection and preservation of human rights in cyberspace and ICT. The future is a dynamic future! All relevant stakeholders, whether States, civil society, lawyers, judiciary, law-enforcement or the netizen community at large, should contribute to the process of development of jurisprudence in this area.

Only the sustained development and progressive evolution of human rights in the context of ICTs and cyberspace, can pave the way forward for healthy meaningful growth and the evolution of cyberspace and concerned relevant jurisprudence in the coming times.

Thank you, ladies and gentlemen.

---

[3] *The term 'crime against humanity' includes inhumane acts intentionally causing great suffering, or serious injury to body, or mental or physical health, when committed as part of an intentional widespread or systematic attack directed against any civilian population.*

Seminar Report

Dr. Wolfgang BENEDEK
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, Austria

Dr. Madanmohan RAO
Research Advisor at the Asian Media Information and Communication Centre (AMIC) and Editor of The Asia-Pacific Internet Handbook; Banglore, India

I. EXECUTIVE SUMMARY [1]

The 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights was held on 27-29 June 2012 in Seoul, Korea. Hosted by the National Human Rights Commission of Korea and the Korean Ministry of Foreign Affairs and Trade, and organised by the Asia-Europe Foundation and organised by the Asia-Europe Foundation, the Raoul Wallenberg Institute of Human Rights and Humanitarian Law, the French Ministry of Foreign and European and Affairs, the Philippine Department of Foreign Affairs, the Seminar was dedicated to one of the greatest challenges that international law, international politics and diplomacy face in the 21st century: how to respond effectively to the challenge posed to human rights by Information and Communication Technologies (ICTs).

The Seminar brought together over 120 participants representing 42 of the 48 ASEM participating countries, making it the largest multi-stakeholder human rights meeting spanning the two regions. Participants notably included representatives of States, national human rights commissions, human rights ambassadors, representatives of justice and foreign affairs ministries, academics, NGO representatives, social media entrepreneurs, activists and human rights defenders. The different backgrounds and the common quest to find answers to the most pressing questions of human rights protection online formed the foil against which the seminar asked important questions and delivered essential answers, with the goal to implement effective human rights protection mechanisms in a networked and multi-layered world.

Seminar participants convened in four Working Groups focusing on key aspects of human rights protection and information and communication technology that had been identified by ASEF and the two main rapporteurs:

- Working Group 1: Freedom of Expression
- Working Group 2: The Right to Privacy
- Working Group 3: The Digital Divide
- Working Group 4: The Right to the Cultural Enjoyment of the Internet

II. SEMINAR REPORT

A. Introduction

New technologies have always ushered in new challenges to human rights. No technological innovations have ever brought comparable cataclysmic changes to the ways humans express themselves, interact, associate, play, demonstrate, shop, debate, organise and start revolutions as have ICTs such as the Internet. In light of the deep impact of the Internet on human activity, challenges have emerged in relation to all existing human rights. The organisers therefore had to pick and choose, and selected four key aspects that are characteristic of the impact of information and communication technologies on human rights.

The first topic was the role of freedom of expression online. Freedom of expression is a key human right, not only in itself, but also as a means to ensure other human rights. In that, the Internet is similar; derived from the conclusion that all the Internet-related rights depend on having access to the Internet in the first place, there is a movement to increasingly recognise Access to the Internet as a human right. At the same time, the Internet is a catalyst for achieving a higher level of human rights protection.

Second, no single human right may have been so deeply impacted by the changes in social mores occasioned by the Internet as the right to privacy. Indeed, some observers have even declared the end to privacy, and the concept of privacy has been substantially altered in light of new generations of citizen journalists and changing sensibilities of where to draw the line between what is public and what is not.

---

[1] *The Main Rapporteurs of this Seminar Report are Wolfgang Benedek and Madanmohan Rao, who also acted as rapporteurs for Working Groups (WG) 2 and 1, respectively. Working Group Rapporteurs Dieter Zinnbauer (WG 3) and Delia Browne (WG 4) also contributed to this report, as did the rapporteurs' assistant, Matthias C. Kettemann. The report reflects the views and opinions expressed by the participants of the seminar. The authors gratefully acknowledge their contributions. This document has been produced with the financial assistance of the European Union. The content of this document is 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.*

The third topic addressed the most fundamental challenge to equitable and sustainable development in the age of the Internet: bridging the digital divide. This means not only the classical divide between rich and poor nations, but also the other divides – those within nations, between rural areas and cities, between the formally educated and the illiterate, between men and women, between the differently abled and the rest of the population.

Finally, the fourth topic looked at the potential of the Internet to ensure cultural enjoyment, to secure our cultural heritage, and to navigate between the Scylla of tightening intellectual property regimes and the Charybdis of free access with potentially negative consequences on human creativity.

Based on these four topics, the discussion in Seoul took place in the format of working group discussions. The outcomes from each of these working groups are presented in the following sections.

B. Working Group 1: Freedom of Expression

I. Introduction: Key Challenges to Freedom of Expression on the Internet

Freedom of assembly and the right of expression have been some of the first broadly accepted principles of democratic societies, which connect to human rights. Freedom of Expression (FoE), for instance, included the right to speak out in public gatherings, and later, with the rise of the mass media age, also included a free press and broadcast media. More recently, digital networks and media such as the Internet and mobile phones have opened up unprecedented opportunities for citizens to record events and express their own views in real-time to global audiences. Thus, freedom of expression in the 21st century is one of the crucial human rights that must be recognised and protected.

II. Jurisdiction in Global Digital Media

Governments continue to play an important controlling role in digital media, especially in Asia. While it has been maintained that offline rules about freedom of expression should also apply to online, there are differences in interpretation and application of this principle around the world. Many laws about expression are still linked to geography, e.g. hate speech, 'taboo' topics, defamation and child protection. An emerging challenge is privatisation of censorship, where governments and private sector players, such as social media sites, strike their own deals about what is permissible expression, without any public debate on the issue.

III. Freedom of Association and Assembly Online

Online association and assembly is a relatively new subject of work, and still needs some clarity in basic definitions. For example, are avatars or online 'gatherings' are a form of assembly? But it has been clearly proven that mobile social networking effectively enables 'smart swarms' and 'smart mobs' – online coordination of offline movements. There are some countries in Asia, however, where public assembly and protests are banned, thus making the online equivalents even more important.

IV. Anonymity

There are clear benefits (e.g. whistleblowing, lobbying) as well as challenges (e.g. online stalking, defamation) of anonymity in digital media. Some governments require registration of citizens for digital participation, and a range of such registrations duties is emerging, for instance, for (i) Net/mobile connections, (ii) pre-paid SIM cards, (iii) online chats, (iv) cybercafés/hotspots. Some governments do not require registration at all; some require registration for all or only some of the above categories. Some private sector players also require registration for participation in digital surroundings such as chatrooms or social networking services.

There are concerns over retention of and access to user data (both telecom and Internet) by private and government players. Differences of opinion also arise in some Asian countries about registration and classification of political sites, and foreign funding for such sites (e.g. whether it is genuine concern over 'foreign interference' or merely a ploy to restrict freedom of expression.

In addition to government and private sector surveillance, there is also concern over surveillance in the home, such as surveillance of women's use of mobile phones and the Internet by their spouses and relatives.

V. Access to ICTs

Access to ICTs arises in a number of dimensions: individual access to 'basic' Internet services such as email and Web; access to the full Web (all Web sites); and access to all social networking services and social media. Governments have played a controlling role in each of these areas, as well as in shared access in cybercafés and libraries, though, for example, the requirement to install filtering software.

Some Asian governments block access to certain websites but do not publish a list of such sites; others block access to social media sites. Some countries have Internet connection costs which are so high that they effectively restrict access and expression. An interesting good practice is Finland's guarantee of Internet access for all its citizens, but this may not be feasible for emerging economies where such public subsidy is not affordable. Governments, device manufacturers and content

providers are also becoming increasingly aware of usability issues, for differently-abled citizens, for example, and of assistive technologies for seniors.

Some governments block the use of certain terms and keywords in search engines, thus filtering the content that citizens can access. There have also been instances of online commercial services such as Voice over Internet Protocol (VoIP) that have been blocked by private and government-owned telecom operators. Such filtering also interferes with freedom of expression.

VI. Whistleblowing

The phenomenon of WikiLeaks has opened up new dimensions to online whistleblowing. This can be challenging to some diplomats, but in several cases it has exposed corrupt practices. Though some such leaks can be embarrassing, others can also cause damage to some governments, defamation to companies and risks to dissidents. Whistleblowers need protection by the government, and also some remedial assistance and cultural support in re-integration with the workplace.

VII. Citizen Journalism

In numerous cases, citizen journalists have exposed the shortcomings of traditional media, by exposing, for instance, new facts or correcting reported incidents. However, governments can also analyse such citizen media to identify and track dissidents. Citizen media have faced technical challenges, such as Distributed Denial of Service (DDoS) attacks, which many citizen journalists and publishers are technically unable to overcome. Ethical practices, codes of conduct and education about appropriate use of citizen media are called for, especially regarding issues of trust and reputation.

VIII. Role of Private Sector Actors

Freedom of expression is not just an issue between governments and citizens, but also involves a range of private sector players with differing agendas, concerns and pressure points. For instance, IT players and portals do not require government permission to give access to citizens, whereas operators and service providers come under licensing and regulatory requirements. Sometimes, private sector players strike their own deals with governments without involving citizen concerns. Some private sector players are becoming aware of the bigger concerns of civil society and humanity, but more pro-active initiatives are called for in corporate social responsibility and beyond. Dialogue is needed between private sector players and their governments as some of these players expand into international markets.

IX. Protection and Advocacy Agencies for Freedom of Expression

A number of local, regional and global organisations protecting FoE are emerging around the world. But many netizens and bloggers are not aware of what kinds of assistance are available and how this can lead to self-censorship. More networking and support circles are needed between 'friends of FoE.' This is more effective than just engaging in condemnation of authorities.

X. How Governments are Promoting Freedom of Expression

Governments can support freedom of expression in a number of ways. One such way is to connect to social media and actively engage with citizens. More important ways are to provide constitutional protection for free expression and invite citizen debate during policy formulation. Freedom of information, or right to information, acts are also necessary. Some governments also organise international conferences to showcase freedom of expression and show commitments to upholding it. But governments themselves face challenges in keeping up with technology, and a maturity framework is needed to help gauge progress in this regard. A range of global organisations, such as ARTICLE 19, have pioneered the cause of freedom of expression, and watchdogs, such as Reporters Sans Frontiers, publish annual reports on incidents and legislation with respect to freedoms of expression. Such reports should be taken seriously by governments, media, educators and local NGOs, who should also actively engage in discussion with the Universal Periodic Review Mechanism of the Human Rights Council.

XI. Conclusions and Recommendations

The Working Group agreed on three types of recommendations: those asking for vigilance (requiring watchfulness and research), protection ('pushing back' infringements on freedom of expression), and on best practices (recognising progressive moves by government and private sector in upholding freedom of expression).

Vigilance

- All stakeholders need to be vigilant about infringements of rights and freedoms, and keep up with the rapid pace of technological change and resultant benefits and abuses(for example, new technologies like Near Field Communication, the Internet of Things, augmented reality, embedded devices, and mobile cloud).

- Governments should publish lists of blocked sites, and the restrictions they place on Internet Service Providers (ISPs).

- Governments should also open up more of their data for analysis and interpretation by citizen groups.
- For their part, citizens should learn how to protect themselves and their sites with respect to technology and media practices, in relation to citizen journalism, for example.
- Self-regulation should be encouraged to 'shame' inappropriate behaviour online.
- More organisations, alliances and research programmes are needed to monitor continuously what governments and the private sector are doing in the areas of emerging technologies.

Protection

- Governments should use international human rights mechanisms, peer reviews, and bilateral dialogue to keep up with their FoE responsibilities.
- Governments should refrain from arbitrarily restricting funding to citizen journalism sites.
- Where possible, restrictions on freedom of assembly should be lessened. Clear, transparent and effective mechanisms should be spelled out for judicial redress, dispute resolution and mediation if there are accusations of FoE violations.
- On the technical front, it should be ensured that freedom of expression is not compromised via pressure on intermediaries such as domain registrars, anonymisers, and URL shortening services.
- Harmonisation of data protection laws should occur on a regional and global level. For instance, countries in Asian organisations, such as ASEAN, could begin such harmonisation at a regional level and then expand across Asia and the world.
- Journalists' associations should be strengthened to protect freedom of expression, so that a journalist whose rights have been threatened can turn to the media community for support. Such associations should also have the legal power and skills to provide assistance to affected journalists in case their human rights have been violated.

Best Practices

- Promoting the cause of freedom of expression should not just be a confrontational matter, but should also rely on incentives and inspiration. Instead of just 'carrot and stick' approaches such as force and trade, there should be change management via genuine appreciation and recognition of progress made with regard to freedom of expression by governments and private sector players.
- For instance, 'Friends of FoE' awards could be given to countries and companies. Prizes should be given for progressive practices and policies in the areas of access to ICTs, such as making them affordable, increasing their reach, and increasing bandwidth.
- Recognition should be given to countries and companies that affirm Rights not just in the abstract, but Rights on the ground. More countries and companies should be encouraged to expand the Freedom Online Coalition and Global Network Initiative.

C. Working Group 2: The Right to Privacy

I. Introduction

The Working Group benefited from an introductory presentation on the challenges of protecting privacy by the Chair, and then engaged in a mapping exercise and discussion of the main issues, on-going discourses and regulatory challenges. Finally, the Working Group endorsed a set of conclusions and key messages, which can be found at the end of this section.

II. Challenges to the Right to Privacy

Information and Communication Technologies (ICTs) have substantially enlarged the opportunities to realise one's human rights, but have also resulted in the emergence of new challenges. This is particularly true of the right to privacy, which faces challenges such as profiling for public and private purposes, geo-location, cloud computing, data loss, mobile Internet, privacy policies of social networks, and trans-border data flows.

Ensuring the right to privacy is key to enabling human security online and to allow for the full realisation of human potential online, especially with regard to the freedom of expression, and notably for young people. The right to privacy has been situated in different times of human evolution, at different points on the complex continuum between liberty and security. Against this background, the workshop aimed to situate privacy rights as human rights within global information societies; to identify special challenges to privacy rights in online contexts and; to stimulate comparative analysis of privacy approaches in Asia and Europe.

III. Actors in the Privacy Debate

The Working Group agreed that the importance of privacy has risen significantly in the online environment due to changing security conceptions, economic developments and changes in user behaviour. Governments collect more data to respond more effectively to what they perceive as threats to national security – for example, by increasing data retention requirements. Companies collect more data for business purposes in light of decreasing storage

costs and increasing data mining technologies. Finally, individual Internet users wish to enjoy protection of their privacy, but also voluntarily give up some private information to increase what they perceive as the quality of their social interactions and their online profiles. Being always 'online' implies being in a non-private space. At the same time the extent to which we insist on, or give up, privacy significantly affects the roles we play in society – as citizens, consumers, friends, family members, travellers, patients and partners.

The Group looked at the avenues to be pursued to empower individuals vis-à-vis Internet service providers. While the Council of Europe is currently working on a compendium of the rights of Internet users, some Working Group members felt that because semantics mattered, rights of individuals should be at the centre of the debate. Recognising the centrality of the individual, the Working Group agreed to focus on the privacy of individuals and the protection of their personal data. It was seen as problematic that personal data protection laws have been used by corporate and State officials to stop freedom of information-based requests.

With the responsibility of Internet intermediaries being limited, the Working Group underlined that States shared a responsibility for protecting their citizens. This is also in line with recent jurisprudence of the European Court of Human Rights.

IV. Scope and Substance of Privacy Protection

Different legal instruments on privacy have been adopted on the international, regional and national levels. They all regulate the collection, use and disclosure of information. Nevertheless, the Group pointed out that in some Asian countries, such as Japan and Malaysia, no legal definition of 'privacy' exists in the constitution or in national legislation.

In light of the spatial scope of national data protection versus the trans-border nature of data flows, international law was considered important. An underlying feature of privacy protection is the interaction between international, regional and national law on privacy. Internationally, Article 17 of the International Covenant on Civil and Political Rights protecting the right to privacy, unlike the right to freedom of expression, does not contain a limitation clause outside of cases of emergency. National legislation however, often provides for limitations and so do regional human rights documents, such as the European Convention of Human Rights.

Acceptable exceptions of the right to data protection have to be provided in accordance with the law – necessary in democratic society in light of legitimate purposes, such as national security or public order - and proportionality, which requires a balancing act.

Regional examples of best practices in the regulation of aspects of privacy, notably data protection, are the Council of Europe's Convention No. 108 of 1981 on data protection, which is presently being modernised, and the European Convention on Human Rights. On the Asian side, the Group discussed the APEC Privacy Framework of 2004.

As concerns specific human rights approaches, the Working Group debated the role of the right of self-determination or autonomy of individuals with regard to privacy. The German example of the right to informational self-determination related to human dignity was highlighted as were other approaches like the right to liberty in India and Japan or the protection of personality in Norway.

V. Towards a Harmonisation of Approaches to Privacy?

Recognising the divergent approaches to, and levels of protection of, privacy, the Working Group agreed that striving towards conceptual convergence was less important than identifying common threats to privacy. But as the problems were converging, a future regulatory convergence could also be expected.

The Working Group also identified substantial differences in the intensity of privacy discourse between Asia and Europe. The different levels of public awareness were conceived as challenging in light of the outsourcing of ICT services and other business processes by European and US companies to Asian firms.

VI. The Role of Internet Intermediaries and Data Collectors

Internet gatekeepers, such as search engines and social network providers, are increasingly harvesting user data in order to monetise their services. The Working Group found that governments have a responsibility to provide – both for Internet intermediaries and companies more generally – a regulatory framework under which the rights of individuals are protected from the profit-driven data demands of the private sector. Remedies of individuals against violations of human rights must not only exist de jure but also need to be effective.

The Group looked with concern at trends to overestimate self-regulation. The users of big Internet intermediaries have, in some cases, successfully impacted changes in privacy policy and can thus limit the self-regulatory powers of Internet Service Providers. This was, however, considered imperfect, especially with regard to smaller companies lacking a well-organised and data-sensitive user base.

As an alternative to standard regulation and self-

regulation, untried in parts of the world, the Working Group underlined the promises of the co-regulatory approach. Whatever the regulatory model chosen, however, ISPs need to be protected from regulatory overreach of States, just as individuals need to be protected from violations of their privacy rights.

States are obliged to ensure that the human rights framework is applied also to private, commercial spaces and that companies do not violate human rights. Companies have a corporate social responsibility (CSR), which includes human rights obligations as developed recently by the globally accepted Ruggie Report.

VII. Raising Privacy Awareness

Reiterating that privacy awareness is essential for ensuring adequate protection, the Working Group found that ensuring technological literacy is key for effective privacy protection at all levels of society. For example, in Asia the awareness of technology to enhance privacy is still low.

In the 2009 Madrid Declaration, civil society expressed their support for independent data protection authorities. The Working Group echoed this call, underlining that these can help ensure adequate protection. Further, some members argued for installing specialist tribunals within the national court systems for privacy cases in order to ensure quick and easy adjudication. Within companies, data protection officers can help increase data sensitivity and to gain access to remedies.

The Group viewed critically the argument that some people, especially younger people, tend to share their data freely and were therefore not in need of protection. Rather, as in the case of the right to health, it is essential to ensure awareness and protection, even if individuals are less aware than they should be of the dangers of data oversharing. Further, awareness-raising among Internet professionals was also considered important.

In view of a lack of information and transparency, the Working Group recommended that Asian States develop a collection of privacy legislation in their countries as a basis for future policy-development and law-making. In Europe and in Asia, States should provide citizens with information on effective redress of violations of the right to privacy.

VIII. From Private to Public Spaces

The Working Group intensively discussed how private spaces developed into semi-public or public spaces. The more successful a company is in drawing users to their services, the more likely it is that the social space provided by the company becomes a public space in which companies have fewer private law-based rights and can no longer freely determine user behaviour. For example, private archives, if open to the public, have to follow rules for public archives.

IX. Privacy by Design and Privacy-Enhancing Technology

In light of underdeveloped data sensibilities of Internet users, one sensible approach is to commit companies to ensuring that the default settings are more data-sensitive. This 'privacy by design' should be materially reflective of privacy protection law, including the principles of transparency, consent, integrity, necessity and proportionality in the collection of data. Data-sharing, for instance, should be discouraged as a default option, by changing sharing settings from 'opt-out' to 'opt-in'. The development and use of privacy-enhancing technology should be encouraged. In some countries of Asia, however, the use of these technologies, such as anonymisers or proxy servers, can even be illegal.

X. Intersecting Levels of Protection

The Working Group underlined that the most effective protection of privacy would seem to be multi-stakeholder-based, and ensured in a multi-level architecture with a variable normative geometry. This enforcement hierarchy has five levels. These levels would include, first, awareness-raising on the user level and, second, effective and human rights-sensitive self-regulation by companies. Third, independent data protection authorities and ombudspersons (or specialised tribunals) can provide quick redress. Fourth, nationally, general data protection laws and sectoral laws, for example, for the banking sector, are necessary. Where applicable, States are asked to update their data protection laws speedily. Finally, fifth, the international level – through (inter-) regional co-operation and international agreements – provides the frame for national legislation and possible correction of national decisions violating internationally and regionally accepted human rights codifications.

XI. Increasing the Effectiveness of Remedies

The Working Group agreed that violations of the right to privacy of users by the private sector need to be addressed through effective remedies – for instance, fines imposed by oversight bodies similar to those in competition cases. Naming-and-shaming procedures involving NGOs were also mentioned. The Working Group also felt that in addition to public human rights-based enforcement of privacy rights, contractual remedies could be an effective approach for individuals to ensure that their rights are being respected by companies. Additionally, alternative dispute resolution measures could be envisaged. Altogether, a comprehensive and coherent system of protection is needed.

XII. Commodification of Personal Data

The Group expressed concern about the increasing commercialisation of personal data of Internet users. It welcomed initiatives to make young people see that the 'bargain' struck at the beginning of a contract on sharing their data in order to receive services is detrimentally slanted. Minors should be empowered to use the Internet as much as possible, while being protected as a vulnerable group.

In the future, personal data will increase in importance and the economics of personal data will need to be addressed in more depth.

XIII. Research Co-operation

The Working Group further highlighted the role of alliances and co-operation between Asian and European research centres for increasing excellence in privacy research. NGOs such as Privacy International should also be harnessed to learn about threats and share best practices.

Whistleblowing websites have been set up around the world. The Working Group highlighted that a common-sense mechanism should exist between the leaking of documents and their publication.

XIV. Conclusions and Recommendations

Opportunities and Threats

- The Working Group agreed that ICTs hold important opportunities, but have also led to substantial challenges to privacy. The misuse of personal data for profiling, or commercialisation without the consent of the user, needs to be effectively countered. Emerging threats include those from geo-location software, cloud computing and other emerging technologies, which need to be addressed by actors – States, private sector, international organisations, civil society and users – within their respective fields of responsibility.

- There is a need for a common, coherent and global understanding of the concept of privacy and data protections fully respecting human rights guarantees.

- There is a need to simplify the terms of service of Internet Service Providers, Social Network Providers and Search Engine Providers.

- In terms of rights, the right of informational autonomy of the individual, also called the right to informational self-determination, is essential. It provides the individual with a right to control over his or her own data and over the use made of it.

Need for Regulation Based on Human Rights

- Existing legislation and rules need to be transparent and open to all. Limitations need to be interpreted restrictively and to follow the principles of necessity and proportionality.

- Governments have a responsibility to protect individuals against violations of human rights and data protection by public authorities, but also by private entities.

- States need to ensure that the human rights framework is applied also to private, commercial spaces, and that companies do not violate the human rights of their users.

- The Working Group recommends that States not yet having privacy and data protection laws should adopt them – for reasons of human rights protection as well as for reasons of legal security and in order to facilitate trade in ICTs, e-commerce, international investment in local ICTs, and the general vitality of the ICT sector.

- Governments have a responsibility to protect individuals against human rights violations and to provide data protection by public authorities, as well as a responsibility, through data protection legislation, for data held by private entities. Therefore, States need to ensure that the human rights framework is also applied in private, commercial spaces, and to ensure effective remedies, if it is not the case.

- Notably, States should consider the opportunity to join the Council of Europe Convention (No. 108) on Data Protection, which is open globally.

- Existing examples of good practice in the respective regions should be taken into account in an effort of mutual learning. Where possible, a multi-stakeholder-based approach to data protection and privacy regulation should be followed.

Need for Effective Remedies

- Effective remedies need to be provided on the various levels of regulation, and people should be made aware of them. In particular, States should create independent data protection authorities and/or ombuds-institutions. Data protection officers should be installed in companies handling large amounts of data. The corporate sector should follow CSR principles, as contained in the Ruggie framework.

- Common principles on privacy and data protection should be applied. These include the right to know, to consent, to access data for individuals and the integrity and security of data.

- Privacy by design and privacy-enhancing technology should be encouraged.

- For all these purposes, co-regulation approaches should be implemented where possible, as self-regulation often conflicts with business interests. In this context, the responsibilities of all actors need to be clarified.

- Though ISPs cannot be committed to control content in general, gatekeepers can be expected to delete illegal content violating individual privacy after following due process.

Awareness-raising and Protection

- Digital literacy, awareness and capacity-building are needed to enjoy human rights such as privacy in the information society. In particular, there is a need to increase awareness of the importance of data protection among young people.

- Appropriate protection of minors and other vulnerable groups needs to be ensured. They have to be empowered and not unnecessarily limited in their access to the Internet. They also have a right to privacy.

International Co-operation

- Asian States are encouraged to develop a collection of privacy legislation in their region to improve transparency and as a basis for future policy-development and law-making.

- International co-operation needs to be strengthened between State and private actors from Asia and Europe at all levels.

D. Working Group 3: The Digital Divide

I. Introduction: Effectively Tackling the Digital Divide

Working Group 3 addressed a broad range of issues related to understanding and effectively tackling the so-called 'digital divide', with a particular emphasis on a human rights perspective. The Group explored different attributes and drivers of the digital divide, which can be clustered around three principal dimensions.

1. Which technologies are affected?

The discussion indicated that a focus on the Internet alone is too narrow. Instead, the Divide needs to be examined in the context of an entire ICT 'ecosystem', in which a broad range of information and communication technologies – including mobile and fixed phones, TV, radio, print media, GPS – increasingly interlink and build on each other, thus shaping and conditioning the overall bundle of functionalities and benefits that citizens can derive from ICTs. As a result, digital divide issues need to be explored in the context of this entire system of technologies, rather than just the Internet alone.

2. Where and in what form can digital divides occur?

The discussion clearly demonstrated that digital divide issues are not confined to technology access, but that consequential disparities can occur at several points along the transmission mechanism that turns technology potential into realised technology benefits for citizens. At the technology level, these disruptive disparities range from unequal access to ICT infrastructures and devices, to challenges with regard to affordability. Built-in biases at the software architecture level include possible lock-ins into a particular software or content ecosystem, insufficient multi-language support or limited adherence with accessibility standards.

In addition, the digital divide can also be driven by inequalities in related ICT skills and knowledge, or by asymmetric access to respective education and training opportunities. Moreover, disparities can also take hold at the usage level and pertain to unequal access to digital content, crucial applications or essential digital services. The latter was identified as particularly deplorable, when essential services such as banking or bill payments move online and lead to a phasing out of offline alternatives, thus leaving those who are not able to use the electronic service modality worse off than before.

3. What groups of people are at risk of being excluded?

The examples of digital exclusion provided by participants highlighted that digital divides often map onto pre-existing drivers of marginalisation. At the level of geography, digital disparities can be observed between countries and between rural/remote and urban regions. Digital exclusion can also arise along gender lines (with women typically disproportionately excluded), age differences (elderly most affected), income and education levels (poor/less educated at risk), ethnic or language differences (minority groups disadvantaged), ability levels (disabled most affected) or pre-existing degree of civic and political engagement (disengaged affected). Gender and state of ability were identified by participants as particularly salient factors that can frustrate the efforts of women and the disabled to harness the benefits from ICT in multiple and particularly significant ways.

These three dimensions of the digital divide span a risk matrix in which specific digital divide issues of a country or community and most examples invoked during the Working Group discussion can be located.

II. The Dynamic Characteristics of the Digital Divide

Various examples provided by participants also suggest

that the digital divide should not be understood as a static gap to be filled once and forever through a specific set of policy interventions, but that it is essentially a dynamic phenomenon. Rapid progress in ICT development continuously shifts the technology frontier outward and makes existing technologies obsolete in a very short time span, thereby aggravating existing divides and opening new ones.

What is more, digital divides can be driven by dynamic processes in which disparities reinforce each other and thus progressively worsen the chances of the affected to catch up; for example, when lack of access breeds lack of interest in acquiring ICT skills on the potential user side, as well as lack of interest in developing useful applications for these excluded groups on the ICT production side, thus further diminishing incentives to seek access for the affected groups. It was also noted, however, that policy interventions can take advantage of the dynamic qualities of the digital divide and help trigger a virtuous circle; for example, when policy interventions lead to easier public availability of the internet for young people and thereby stimulate demand for skill-building and learning by this group, which in turn will stimulate further demand for ICT access and use, as well as development of related applications by ICT entrepreneurs.

Another important time-related characteristic of the digital divide was also mentioned: the mismatch between short-term return on investment horizons that drive ICT business decisions and the longer-term public outlook to generate sustainable social benefits from ICT. Aligning these different time horizons was considered essential to ensuring that the business sector can be most productively engaged in closing the digital divide.

III. Towards Tailored Approaches

The tremendous diversity of digital divide issues and priorities that the discussion generated led to the conclusion that every country or community will be required to define its own priorities, mix of policy interventions, as well as their related sequencing for effectively bridging of the divide. According to one view expressed in the debate, this may require movement at a more measured pace and helping the digitally excluded appropriate more familiar ICTs, such as the education potential of TV, first before moving into intensified promotion of more advanced technologies. At the same time, it was pointed out that the potential to leapfrog some costly, outdated technologies and move straight into superior technological solutions such as advanced wireless ICTs should not be underestimated.

IV. ICT Access as a Right for All Humans

No clear consensus could be established within the group on whether ICT access can be fully and technically, from a legal viewpoint, classified as a human right. While a number of participants expressed their support for this position, others were hesitant to place what they considered rather a means for a human rights end in this category. This inconclusive outcome, however, hinged only on minor, rather than technical differences in perspective.

More importantly, it does not detract from the fact that a clear consensus was established in the Group that ICTs are by now so deeply embedded and central to almost all aspects of human activity, well-being and societal development that they constitute an essential, albeit not sufficient, condition for realising a wide range of fundamental rights, from freedom of expression, participation and information to the right to dignity, health, education, cultural expression, economic livelihood, personal development, social and political participation.

V. Different stakeholders with a shared, but differentiated responsibility for bridging the digital divide

Irrespective of whether a right to digital inclusion should be considered a full human right or 'just' a prerequisite to realising an entire array of fundamental rights, the discussion made very clear that what flows from either interpretation are clear, strong, unambiguous responsibilities for governments and other stakeholders on one side, as well as rights and entitlements for citizens on the other, in order to make digital inclusion a reality.

Citizens – Self-Determination, Choice and a Say in Internet Governance

The rights and entitlements of citizens that were enumerated by participants revolved around the guiding principles of self-determination, choice and control over technology use. In addition, the importance of spaces for experimentation and do-it-yourself tinkering with technologies was emphasised, in order to allow citizens and communities to appropriate and adapt ICT for their own purposes. Finally, the right of citizens to get involved in issues of Internet governance was stressed on several occasions, strongly affirming the multi-stakeholder principle that has been explicitly embraced by many institutions involved in Internet governance.

Governments – the Responsibility to Act as a Multi-Level Enabler

The roles and responsibilities for government that transpired from the discussion and were invoked by different participants include:

- Coordinate and, where necessary, actively seed and drive infrastructure build-out when markets and the private sector fail to deliver on the full range of digital opportunities for all;

- Safeguard competition and provide regulatory oversight to prevent market concentration, and establish, as well as protect against the infringement of, a full catalogue of ICT user rights;

- Promote awareness about digital opportunities and provide the necessary education, training and skill-building, if necessary, in a targeted and affirmative manner to tackle digital exclusion;

- Catalyse the development of, use, and – where required for essential functions and applications – mandate the adoption of interoperable, open and non-proprietary software standards;

- Actively help create and fully exploit digital opportunities for all from e-health and e-education, to e-participation;

- Limit government interference with ICT use by citizens to essential, clear, as well as narrowly defined public interest concerns; follow due process and be transparent about and accountable for these interventions; and

- Fully embrace the principle of open government and pro-actively disclose information about its own workings and performance to the public.

The wide spectrum of identified roles and responsibilities also exemplifies how closely digital divide issues are interlinked with each other and cannot be discussed separately from other ICT and human rights issues that were broached by the other working groups.

Business and Civil Society – Indispensable Partners to Realise the Digital Dividend for All

The discussion also explored what business and civil society should and can do to help tackle the digital divide. Businesses, with their much-needed capabilities to mobilise resources, expertise and entrepreneurial spirit, were recognised as indispensable partners in driving technological progress and achieving digital inclusion. At the same time, some participants noted that maximising this role will depend on appropriate regulatory frameworks and incentives to ensure that markets do not aggravate existing disparities, but actively address the needs of marginalised groups.

Moreover, ICT-related business will have to act as responsible corporate citizens on the basis of binding codes of conduct, particularly when their products and services reach a market share and centrality in public life that turns them into de-facto essential facilities. More specifically, this may include the responsibility to adopt state-of-the art accessibility standards or to safeguard appropriate levels of interoperability with other products and services.

Civil society was acknowledged to play an important role in bridging the digital divide in several respects. Some participants stressed the contributions that civil society actors can make at the technology development level, for example, by catalysing or even driving the development of open standards, or conducting usability testing for minority groups. Undertaking research, awareness raising and advocacy on ICT policy issues from a public interest angle was highlighted as another important function. With regard to Internet users and citizens, helping to defend the human rights of Internet activists, such as citizen journalists or whistleblowers, and representing the interests of marginalised stakeholders in Internet governance were added as important roles for civil society.

VI. Skills and Access to Knowledge – Essential ingredients to bridging the divide, but often overshadowed by a focus on infrastructure and hardware

Framing the digital divide as primarily an issue of unequal access to infrastructure and technology is incomplete and unlikely to yield effective remedy. This central insight has been prominently reflected in a number of contributions that provided examples for existing ICT disparities. It featured prominently again when exploring possible remedies and policy interventions. From school computers in Sweden to rural communities in Vietnam, young people in Estonia or senior citizens in Thailand: skills and training, pertaining not only to technology use, but also to media literacy and information competence, all tailored to specific user groups and ICT uses were referenced as integral parts of strategies to bridge the digital divide. Facilitating and protecting inclusive access to online content was identified as another important step. In this context, at least three key policy challenges were flagged by participants:

- A balanced approach to intellectual property protection that respects and protects citizen rights, as well as the public interest, was viewed as a pivotal policy issue. This analysis was underpinned by examples of researchers in developing countries unable to afford essential scientific publications online;

- A strong endorsement of the Net neutrality principle, that ensures that infrastructure and appliance providers do not discriminate against or unduly privilege specific contents, but guarantee a fair level of visibility and accessibility or all lawful content from individual bloggers to large business players; and

- The production of content in local languages and the language-related localisation of software and services to ensure cultural diversity and inclusiveness online.

VII. From Digital Divide to Sustainable, People-Centred Digital Opportunities for All

A final common thread from the debate with particularly important policy implications relates to the somewhat overly negative and static notion of a digital divide. Such a picture conveys a negative outlook for the perceived impact of new digital technologies and it would also lead to policy interventions with a narrow focus on closing existing, more or less given and static gaps.

The discussion showed clearly that such an understanding is incomplete and misleading for several reasons, including the following:

- Notions of a divide that excludes and disadvantages need to be balanced with an emphasis on the potential of digital technologies to foster inclusion, connection and opportunity, by, for example, providing tools for weaving lateral connections that cross organisational or social hierarchies, or by helping individuals to explore more fully and articulate their identities, and to connect with like-minded people.

- The digital divide is clearly a dynamic and ever-changing challenge. As mentioned earlier, ICTs are developing in leaps and bounds, and focussing longer-term strategies for catch-up as response to the disparity of today is incomplete at best, and ineffective at worst. Instead, many important policy remedies that were shared by participants pointed towards a more strategic, forward-looking approach that helps in closing digital divides in a more systematic and sustainable fashion.

Based on this debate, the challenge to close the digital divide could be reframed as the challenge to design for sustainable and maximum digital opportunities for all on three levels:

- Infrastructure build-out, including encouragement for community-led and community-rooted initiatives, recognition of peer-to-peer mesh network technologies to ameliorate last-mile connectivity problems and open-spectrum policies for vibrant competition in access provision;

- Inclusive software architectures and applications, including sound interoperability provisions, open standards and the adherence to and further expansion of universal design principles that ensure maximum accessibility for disabled persons;

- Design for governance institutions that incorporate the multi-stakeholder principle through appropriate mechanisms for consultation, representation and participatory decision-making, as well as provisions for affirmative inclusion of marginalised groups.

VIII. Conclusions and Recommendations

Heeding all these design principles and anchoring them in a strong framework of ICT-related citizen entitlements has the potential to prevent, rather than simply react to, incidences of digital exclusion today and in the future, which will without any doubt continue to emerge in the context of runaway technological progress. Furthermore, as the Working Group discussion showed, such a rights-based, human-centred and design-oriented approach can represent an important step in doing justice to the essential role that ICTs play in protecting and progressively realising an expanding set of human and other fundamental rights around the world.In particular, the Working Group reached the following conclusions:

- ICTs are by now so important in our societies that they constitute an essential, albeit not sufficient, condition for realizing a wide range of fundamental rights.

- Increasingly interlinked and complementary ICTs require looking beyond the Internet alone and considering an entire suite of ICTs that can be affected by the digital divide, including Internet, phone, TV, radio, newspaper, and GPS satellites.

- Digital divide issues are multi-faceted and require a holistic approach that safeguards and promotes inclusion on all levels, from the basic infrastructure and device and software level, all the way to digital content, applications and e-services, and to the decision-making architectures that underpin all these areas.

- One-size-fits-all thinking is not possible. A tailored approach is required to maximize digital opportunities for all countries and communities, both in terms of policy priorities, mix of interventions and their most effective sequencing.

- Making digital inclusion a reality needs to be underpinned by strong, unambiguous responsibilities for governments and other stakeholders to help bridge the digital divide, as well as by clear rights and entitlements for citizens as ICT users and co-producers.

- Related citizen rights include self-determination, choice and control over technology use, and spaces for experimentation.

- Governments need to ensure inclusive infrastructure build-out, competitive ICT markets, sound regulatory oversight, ICT skill development for all, and inclusive access to essential ICT facilities and services, as well as to government accountability information.

- Businesses, as indispensable partners for bridging the digital divide, will have to act as responsible corporate citizens on the basis of binding codes of conduct, adopt state-of-the-art accessibility standards and

interoperability principles, particularly where essential services are concerned.

- Civil society has an important role to play as promoter of accessibility designs and open standards, as public interest advocate in ICT policy-making and the protection of user rights, and as catalyst for engagement by marginalised groups in Internet Governance.

E. Working Group 4: The Right to Cultural Enjoyment of the Internet

I. Introduction

Set out below are the key themes discussed and the main recommendations developed in the Working Group on the right to cultural enjoyment of the Internet, including additional issues raised at the Seminar's closing plenary sessions - Working Group Rapporteurs' Summary Reports and the Special Plenary: Governance of the Internet.

II. Right to Cultural Enjoyment

At the outset, the participants defined "culture" very broadly to include knowledge of all kinds including education, information, scientific knowledge, traditional knowledge, from ancient to contemporary culture. It was generally agreed that culture, like the Internet, has no borders and the right to access knowledge is a fundamental human right.

The participants also noted the treatment of knowledge and culture as a property right is a relatively new formal concept for many Asian countries, where knowledge and culture is traditionally viewed as a social good that is shared and respected.

After much discussion, there was a strong consensus that the right to cultural enjoyment f the Internet is a component of the right to access knowledge which is enshrined in existing human rights conventions and instruments, such as:

- Article 19 of the International Covenant on Civil and Political Rights;
- Article 27(1) of the Universal Declaration of Human Rights;
- Articles 2 and 15 of the International Covenant of Economic, Social and Cultural Rights.

The Working Group did not feel that additional international instruments were needed. That said, the international community still needs to ensure that access to the Internet and the right to access knowledge, are protected equally in the online world.

There was general consensus that the Internet plays an enormously positive role in enabling access to knowledge and in particular access to culture, and that access to knowledge is vital to the cultural development of the Internet. However, it was also recognised that the right to access knowledge and culture is not an absolute right and there are some tensions in providing such access.

III. Promotion and Preservation of Cultural and Linguistic Diversity

The Internet was viewed by the participants as a vital tool in the promotion and preservation of cultural and linguistic diversity for minority and ethnic groups and indigenous peoples. Minority and ethnic groups are increasingly using ICTs and the Internet to preserve and promote dying languages and dialects, particularly in Asia in countries such as Indonesia, Cambodia, and the Philippines, and to promote and protect their culture, thus helping to prevent the potential extinction of minority, ethnic and indigenous languages and culture.

It was felt that the predominance of the English language on the Internet is a threat not only to online cultural and linguistic diversity but may also limit the ability of minority, ethnic and indigenous peoples' right to:

- Access to their (traditional) knowledge and culture;
- Access education (e.g. learning ICT skills in one's own language); and
- Participate in society, for example, the right of freedom of expression, right to information, the freedom to hold opinions and to receive and impart information, the right to access to knowledge in one's own language.

The participants noted the Internet Corporation for Assigned Names and Numbers (ICANN)'s approval, in 2010, of Internet addresses containing non-Latin characters, including Greek, Hindi, Arabic, Korean, Japanese and Cyrillic, thus opening the Internet to more people around the globe. It was noted that Korea has successfully begun to use Korean character domain names.

The Working Group agreed that the promotion and preservation of cultural and linguistic diversity helps to ensure that minority, ethnic and indigenous peoples are able to participate to the fullest possible extent in the global digital world, and to fully enjoy their fundamental human rights. This is difficult to achieve in countries such as the Philippines and Indonesia, where there are hundreds of minority ethnic dialects and languages. In comparison, Maori is one of New Zealand's official languages under the Maori Language Act 1987, and most government departments and agencies have bilingual names, in English and Maori. This is a great example

of how government can help promote and preserve indigenous languages.

The Working Group strongly felt that the right to use one's own language should extend to the right to be able to access knowledge and culture in one's own language on the Internet.

IV. The Role of Governments

There was a strong consensus from the Group that government can play a positive role in creating, enabling and facilitating an online environment that:

- Provides access to knowledge;
- Promotes and preserves culture in general; and
- Promotes economic development opportunities.

It was strongly felt that, where appropriate, governments should remove technical, legal and economic barriers that impede the above objectives, and the Working Group identified a number of potential areas where government action could be employed.

The Working Group mainly focused on the promotion and preservation of cultural and linguistic diversity and, in particular, the preservation and promotion of minority ethnic and indigenous culture and languages. However, the issues raised and recommendations could equally be applied to all culture and national languages.

Localisation of Tools, Technology and Content

One key area is the development of localisation tools and technology for national languages and by minority ethnic and indigenous peoples. Localisation includes not only the localisation of content but also of technology such, as the ability to adapt software in national and threatened languages. In particular, localisation helps minority, ethnic and indigenous peoples to obtain access and disseminate knowledge, culture and education within their own communities.

Governments should encourage the development of content and technology tools, and of ICT skills education in their own national language, and as many minority, ethnic and indigenous languages where practicable, as this may promote economic development opportunities for minority, ethnic and indigenous peoples.

There was strong consensus that, where appropriate, governments should fund the localisation of content, tools and technology in national and minority languages, including projects where minority, ethnic and indigenous peoples are funded to localise content and adapt software in their language. For example, the Cambodian government funds a computer education program in the Cambodian national language using locally trained programmers and engineers. However, it was acknowledged that not all countries have the financial resources to fund such initiatives.

The Working Group noted that much cultural content is financed by public or taxpayer funds, but is not accessible by the public. There is increasing demand for public cultural institutions to digitise and make their collections available online, and for governments to release public and government information. Some participants went so far as to suggest that not allowing access to material free of copyright should be treated as a human rights violation. There was a strong consensus that governments should actively explore ways to encourage public access to public/cultural goods and the release of public information, and there was much discussion in relation to the role of open standards.

Open standards were recognised as important localisation and dissemination tools enabling access to knowledge and culture.

It is recommended that, where appropriate, governments should provide policy frameworks in relation to publicly funded information and culture that actively encourage the use of open standards – open source, open data, open formats, open licences, open access and open education resources – so as to ensure public access and re-use of publicly-funded information and culture.

V. Balancing the Interests at Stake

Right to Access to Knowledge (A2K) versus Preservation of Culture and Cultural Heritage

The Working Group acknowledged the potential conflicting interests between the right to access knowledge, culture and education, and the rights to preserve and promote cultural and linguistic diversity, especially of the minority, ethnic and indigenous languages and culture.

In particular, there needs to be appropriate balancing between enabling access to knowledge, promotion of culture and cultural heritage, and preservation and protection of culture and cultural heritage. These interests are not necessarily conflicting and are in many ways complimentary. Access to knowledge helps minority ethnic and indigenous peoples promote, preserve and protect culture and cultural heritage.

In addition, the Working Group recognised that communal/collective ownership of traditional knowledge should be acknowledged where appropriate and in accordance with the following international conventions and declarations: the UN Declaration on the Rights of Indigenous Peoples; Article 8(j) of the Convention of Bio-Cultural Diversity; the Convention on the Protection and Promotion of the

Diversity of Cultural Expressions; and Principle 15 of the Geneva Declaration of Principles adopted in the WSIS process.

One participant explained that access to and use of traditional knowledge is often negotiated with the traditional knowledge owners, and access may be denied to outsiders where it is deemed to contravene traditional laws and practices. One such example is the publishing of a Maori person's genealogy ('whakapapa') online.

Intellectual Property Rights versus the Public Interest

Intellectual property rights were viewed as the main legal barrier to the right to access knowledge. Although a key rationale for Intellectual Property Rights (IPR) is to encourage innovation and the creation of cultural content and knowledge, IPR more often acts as a barrier to access to knowledge and stifles innovation. IPR must be appropriately balanced against the public interest and human rights.

The Working Group discussed the continuing importance of "public interest" exceptions in Intellectual Property (IP) legislation. The main aims of public interest balance in IP are to encourage the further creation of creative works, to ensure optimum access to creative works, and to stimulate wide dissemination of knowledge and culture.

Historically, the balance in IP has been achieved through specific public interest limitations and exceptions set out in IP legislation; for example, research and study, library archives and preservation of culture, education, reporting the news, government and public administration, criticism and review, parody and satire.

It is important to note that public interest limitations and exceptions in some countries are limited to analogue or offline forms of access to knowledge. Therefore we need to ensure that the scope of public interest exceptions and limitations are extended, and are applicable, in the online environment so to ensure appropriate online access to knowledge and culture.

More recently, the right to access knowledge and culture is viewed as a key public interest that needs to be balanced against the private and corporate rights of IP owners.

Many members of the working group felt that providing access to knowledge, culture and education did not promote piracy but positively promoted cultural and linguistic diversity, as well as encouraging the creation of new works and innovative products and services.

International Trade Treaties versus the Public Interest and Human Rights

The Group noted IP rights holders' concerns in relation to rampant online intellectual property infringement, and the recent moves to require stronger protection and enforcement provisions that international trade treaties and related IP legislation to combat online large-scale piracy and peer-to-peer file sharing.

The Group acknowledged that the Internet and ICTs have made it much easier for people to violate IPRs both unwittingly and knowingly on a global scale. However, there is concern that the proposed new international trade treaties, such as the Anti-Counterfeiting Trade Agreement (ACTA) and the Trans-Pacific Partnership Agreement (TPP) may have chilling effects on the public interest exceptions, as well as the right to access knowledge, culture and education, and infringe on other essential human rights such as the right of freedom of expression, the right to information, the freedom to hold opinions and to receive and impart information and ideas, and the emerging right to access the Internet. Copyright, in particular, can threaten the enjoyment of the aforementioned human rights.

There are concerns that both ACTA and TPP, and other similar treaties, promote corporate and trade interests at the expense of citizens' rights, and the interests of developed countries over those of developing countries. and that IPRs favour the private commercial interests of rights holders over the public interest and related human rights.

In order to redress the imbalance, governments should consider including the following provisions in multilateral and bilateral trade treaties and agreements:

- An endorsement of international human rights of freedom of expression, freedom of information and the right to privacy, among others.
- A requirement for safeguards on Internet enforcement policies to avoid undue threats to freedom of expression and freedom of information;
- A provision that allows cross-border sharing of copyright works created under an exception for the visually impaired;
- A requirement for open-ended exceptions in copyright, including anti-circumvention law;

It is extremely important that governments ensure that any restrictions to access to knowledge and culture and the public interest are carefully balanced against increased IP protection and enforcement provisions sought in international trade treaties. In particular, there should be credible economic evidence to justify further enforcement and protection provisions in international trade treaties and relevant IP law.

Piracy versus the Right to Earn an Income

The participants discussed the issue of online piracy and the resulting loss of revenue and sales of copyrighted works. Generally, it was agreed that the creator has a right to be appropriately compensated for use of their creative works, but there was no general consensus on best practice solutions. Some thought that royalties were a more important source of revenue to smaller artists rather than sales of content. Others said that 'piracy' and/or unauthorised postings of copyrighted works online may be beneficial to smaller artists as it exposes them to a much wider audience and leads to new works being created by new artists as creators are 'users' too. Participants also noted that not all business models are dependent on copyright royalties (for example, live performances, and online advertisement revenue).

That said, it was generally acknowledged that people may not be so willing to pay for content that is freely available online, and other means of compensation to creators may be needed – such as levies on the purchase of media formats or collective rights management should be considered,(subject to appropriate governance and transparency controls). One participant warned that collective licences often mean that certain users are paying for activities that in other countries are subject to free use exceptions. For example, Australian schools currently pay for educational use of free and publicly available Internet material under a copyright compulsory licence. In addition, the Australian education sector collective licensing experience has shown that even if prices and terms are reasonable at the outset, they may incrementally rise to unreasonable levels as time goes on. Checks and balances would need to be carefully built into collective-licensing regimes to ensure that they complement public interest 'free use' exceptions, as prohibitive licence fees may also be a barrier to access.

One participant suggested that governments could introduce a compulsory licence scheme that allows translations into minority/ethnic languages where there is an insufficient commercial market. Others thought that there are more efficient means to support and encourage the making of new cultural works, such as direct funding to creators from government.

Three Strike Rule versus the Right to Access the Internet

The right to access to the Internet is also threatened by IP protection provisions in International Trade and/or IP treaties, which require online service providers (such as network access providers, web hosts and search engines) to take action against repeat copyright infringers if they wish to be covered by safe harbour provisions that limit their liability for secondary copyright infringements. Such action may include legally requiring online service providers to implement a notice and take down regime, and the adoption of the "three strike rule" under which the online service provider is required to cut off Internet service to the alleged copyright infringer.

The Working Group strongly felt that the adoption of the three strike rule and denying Internet services to any citizen is a breach of the fundamental human rights of freedom of expression, the right to information, the right to access knowledge, the right to privacy, the right to access health and education, and the emerging right to access the Internet.

VI. Conclusions and Recommendations

- Governments should encourage the development of content and technology tools and ICT skills education in as many minority, ethnic and indigenous languages where practicable, as this promotes economic development opportunities for minority, ethnic and indigenous peoples.

- Governments should actively encourage the development of localisation tools and technology for and by minority, ethnic and indigenous peoples. Localisation helps minority groups promote and preserve cultural and linguistic diversity; it removes barriers to participation and allows access to knowledge, culture and education, as well as its dissemination within their own communities. Localisation includes not only the localisation of content but also the localisation of technology, such as the ability to adapt software in local and threatened languages.

- Where appropriate, governments should provide policy frameworks in relation to publicly-funded information and culture that actively encourage the use of open standards where appropriate (open source, open data, open formats, open licences, open access and open education resources),so to ensure public access and re-use of publicly-funded information and culture.

- Governments should always consider the public interest when considering amending their Intellectual Property Laws or introducing new Intellectual Property laws, as they may have chilling effects on the right to access knowledge, culture and education, and infringe on other essential human rights. Intellectual Property Rights (IPR) and overly stringent copyright protection, in particular, can threaten the enjoyment of human rights and hamper human creativity online.

- There are concerns that international trade treaties such as the Anti-Counterfeiting Trade Agreement (ACTA) and the Trans-Pacific Partnership Agreement (TPP) promotes corporate interests at the expense of citizens' rights and the interests of developed countries over those of developing countries. Governments should consider including the following provisions in

multilateral and bilateral trade treaties and agreements:

- A provision ensuring that any interference with human rights needs to be provided by law, pursue a legitimate purpose and be proportionate;
- A provision that allows cross-border sharing of copyrighted works created under an exception for the visually impaired;
- A requirement for open-ended exceptions in copyright, including anti-circumvention law;
- A requirement for safeguards on Internet enforcement policies to avoid undue threats to freedom of expression and freedom of Information;
- An endorsement of international human rights of freedom of expression, freedom of information and other relevant rights.

- Governments need to ensure that the public interest balance is maintained and recognised in domestic IP legislation and international treaties and agreements. Governments should ensure that the rights of users and public institutions – and the fundamental rights and freedoms such as freedom of expression, the right to information, the right to privacy – are positively affirmed.

III. CONCLUDING OBSERVATIONS

Recognising the substantial impact of ICTs on human rights, the Seminar and its four Working Groups looked in depth at the fundamental question of how (and who) to respond effectively to the human rights challenges of the legal and political, social, economic and cultural changes in society due to the use of ICTs.

The Seminar focused specifically on:

- Freedom of expression, a catalyst for the enjoyment of all other human rights on the Internet;
- The right to privacy, a key element of ensuring human dignity and human self-actualisation in the age of the Internet;
- Bridging the digital divide(s), a precondition to effectively using ICTs to fight against human rights violations and a human right in itself; and
- The right to the cultural enjoyment of the Internet, with localisation of content being an important precondition of the full use of ICTs for human progress.

The conclusions and recommendations of the Working Groups can be condensed into fifteen key messages:

1. States should use international human rights mechanisms, peer reviews, and bilateral dialogue to keep up with their Freedom of Expression (FoE) responsibilities. Clear, transparent and effective mechanisms should be spelled out for judicial redress, dispute resolution and mediation if there are accusations of FoE violations. Harmonisation of data protection laws should occur on a regional and global level. Journalists' associations should be strengthened to protect FoE.
2. Governments should publish lists of blocked sites, and the restrictions they place on Internet Service Providers. Governments should also open up more of their data for analysis and interpretation by citizen groups. For their part, citizens should learn how to protect themselves and their sites with respect to technology and media practices (e.g. citizen journalism).
3. Recognition should be given to countries and companies that affirm rights not just in the abstract, but rights on the ground. More countries should be encouraged to expand the Freedom Online Coalition and more companies should join the Global Network Initiative.
4. There is a need for a common, coherent and international understanding of the concepts of privacy and data protection that is fully respectful of human rights guarantees. Common principles on privacy and data protection should apply, such as the right to know, to consent, to access one's own data and to the integrity and security of data. The collection and coordination of privacy legislation, especially in the Asian region, would benefit transparency and co-operation.
5. States not yet having privacy and data protection laws should adopt them – for reasons of human rights protection as well as for reasons of legal security and in order to facilitate trade in ICTs, e-commerce, and the general vitality of the ICT sector. Notably, States should consider the opportunity to join the Council of Europe Convention (No. 108) on Data Protection, which is open globally.
6. Internet gatekeepers, such as search engines and social network providers, are increasingly harvesting user data in order to monetise their services. Governments have a responsibility to provide – both for internet intermediaries and companies more generally – a regulatory framework under which the rights of individuals are protected from the profit-driven data demands from the private sector. Self-regulation is not sufficient. Privacy by design and privacy-enhancing technologies should be promoted. Remedies of individuals against violations of human rights must not only exist de jure but also need to be effective.

7. Effective remedies need to be provided on the various levels of regulation and people should be made aware of them. In particular, States should create independent data protection authorities and/or ombudsman institutions. Data protection officers should be installed in private companies handling large amounts of data. The corporate sector should agree to binding CSR principles, as contained in the Ruggie framework (protect, respect and remedy).

8. Digital inclusion is a right for all humans. ICTs are assuming an increasingly central role in all aspects of human and societal development across the world. As a result the ability to access and make effective use of ICTs has evolved into a necessary, albeit not sufficient, condition for the progressive realisation of a wide range of human and other fundamental rights.

9. This central importance of ICTs translates into strong and clear obligations for governments to work towards digital inclusion by, inter alia, co-ordinating and intensifying investment in infrastructure; exerting regulatory oversight to counter oligopolistic market structures; promoting open, non-discriminatory standards and universal design; providing targeted ICT education; protecting user rights and fair access to content; ensuring that alternatives to online services remain in existence; and leading by example and embracing open government principles – all with a particular focus on supporting the groups at risk of digital exclusion.

10. A pro-active, structural approach is required to close digital divides sustainably and prevent new ones from emerging in the context of rapid technological progress. This includes a focus on promoting the design of:

    a. infrastructure and software architectures for maximum interoperability, language flexibility and accessibility by differently-abled persons;

    b. Internet governance institutions to incorporate fully the multi-stakeholder principle and affirmatively engage marginalised stakeholder groups.

11. Governments should actively encourage the development of localisation tools and technology for and by minority, ethnic and indigenous peoples. Localisation helps minority groups promote and preserve cultural and linguistic diversity; it removes barriers to participation and allows access to knowledge, culture and education as well as its dissemination within their own communities. Localisation includes not only content but also technology such as the ability to adapt software in local and threatened languages.

12. Where appropriate, governments should provide policy frameworks in relation to publicly-funded information and culture that actively encourage the use of open standards where appropriate (open source, open data, open formats, open licences, open access and open education resources)so to ensure public access and re-use of publicly-funded information and culture.

13. Governments should always consider public interest when considering amending or introducing new Intellectual Property laws since they may have chilling effects on the right to access knowledge, culture and education, and infringe on other essential human rights. Intellectual Property Rights (IPR) and overly stringent copyright protection, in particular, can threaten the enjoyment of human rights and hamper human creativity online.

14. There are concerns that international trade treaties such as the Anti-Counterfeiting Trade Agreement (ACTA) and the Trans-Pacific Partnership (TPP) promote corporate interests at the expense of citizens' rights, and the interests of developed countries over those of developing countries. Governments should consider including the following provisions in multilateral and bilateral trade treaties and agreements:

    - A provision ensuring that any interference with human rights needs to be provided by law, pursues a legitimate purpose and be proportionate;

    - A provision that allows cross-border sharing of copyright works created under an exception for the visually impaired;

    - A requirement for open-ended exceptions in copyright including anti-circumvention law;

    - A requirement for safeguards on internet enforcement policies to avoid undue threats to freedom of expression and freedom of information;

    - An endorsement of international human rights of freedom of expression, freedom of information and other relevant rights.

15. Governments should ensure that the rights of users and public institutions – and the fundamental rights and freedoms such as freedom of expression, the right to information, the right to privacy – are positively affirmed in both domestic legislation and international agreements on intellectual property.

Background Paper*

Dr Wolfgang BENEDEK

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, Austria

Dr Madanmohan RAO

Research advisor at the Asian Media Information and Communication Centre (AMIC) and Editor of The Asia-Pacific Internet Handbook; Bangalore, India

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

The rise of transnational 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, which was updated with the invention of the telephone in 1876, articulated support for the availability of telecommunication services for all citizens.

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 US 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, as compared to print media, share several characteristics that have made them especially important in a communication rights context: 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 examples mentioned in this background report, be they countries or private companies, are not here to criticise one or another, but to illustrate the different topics and difficulties any society is facing with ICT. Research support for Professor Wolfgang Bendek has been provided by Dr Matthias C. Kettemann*

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

[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] *Ibid*

[4] *Ibid*

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 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 (e.g. Prodigy, CompuServe, AOL NiftyServe), text-only email and BBSs (e.g. PeaceNet, FidoNet, BitNet), full-fledged multimedia open standards platforms (World Wide Web), and wireless data (mobile networks, WiFi hotspots).

According to Manuel Castells, "[t]he Internet was born at the unlikely intersection of big science, military research, and libertarian culture 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".[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[7]. 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, the 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 topped authoritarian governments.

Digital Media: A Diversity of Challenges, Opportunities and Threats

Frederick[8] 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 corporations[9] – 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 apparatuses,[10] or institutions which perpetuate and reinforce ideology in social formations.

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.[11]

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.

[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] *Ibid.*
[8] *Frederick, Howard (1993). Global Communications and International Relations. Belmont, California: Wadsworth Publishing Company*
[9] *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*
[10] *For more details, please see Althusser (1970), Ideology and Ideological State Apparatuses, In:Lenin and Philosophy and Other Essays, Monthly Review Press*
[11] *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*

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

Source: Adapted from Rao (2003)[12]

[12] *Rao (2003) Op cit.*

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".[13] 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, and Estonia, have included a right to access to the Internet in their national law.[14] Indeed, being excluded from the opportunities that information society offers through the Internet is progressively seen as a denial of the fulfilment 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 global 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 communities with ICT infrastructure to gain access to information available worldwide.[15]

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 Society[16] 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".[17]

In the 2005 Tunis Commitment, States have reaffirmed this commitment to the people-centred, 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 Goals".[18] In this light protecting the Internet as a global public good is a key factor in promoting human self-fulfilment 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.[19] This, too, is a prerequisite for ensuring the people-centred, 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.[20] 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.

---

[13] *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*

[14] *See Organisation for Security and Co-operation 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*

[15] *See UNESCO, Towards Knowledge Societies, Paris 2005*

[16] *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*

[17] *WSIS, Geneva Declaration of Principles (2003), para. 1*

[18] *WSIS, Tunis Commitment (2005), para. 2*

[19] *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*

[20] *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*

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"[21] 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 goods 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.

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 economy[22] 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 engines[23] and social network providers[24] 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.[25]

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,

---

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

[22] Wolff, Jonathan and Nozick, Robert (1991). Property, Justice and the Minimal State, Oxford: Polity Press

[23] 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

[24] 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

[25] 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

however, has only been limited. Sometimes they are also used as fig leaves to cover less noble legislative attempts to exercise more control over political speech or pro-democratic activities for example.

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 (the "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 exception to 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,[26] 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'[27] and the spread of groups promoting hatred. According to the Council of Europe, "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".[28] 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, Facebook's "Abuse Standards" being one such example,[29] 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 exists 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 (ISPs) on private hotlines is not unproblematic, as a recent case in Denmark showed: a human error in a police centre responsible for listing suspected sites resulted in the inaccessibility, for some time, of sites such as Google and Facebook.[30] 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. As 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.[31]

Following up on the various references to the Universal Declaration on Human Rights (UDHR) 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 UDHR, starting from the right to non-discrimination in Internet access, to education, access to knowledge, through to online participation in public affairs and effective participation in Internet governance. Additional rights concerned are the right to development and the rights of the child. The core rights of concern to the Internet, however, are 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

.

The 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 Europe[32] and the Joint Declaration

---

[26] *Council of Europe, Convention on Cybercrime, CETS No. 185 (2003)*
[27] *See Weber, Anne (2009). Manual on Hate Speech, Council of Europe*
[28] *Council of Europe, Committee of Ministers Recommendation 97 (20)*
[29] *Facebook, Abuse Standards 6.2. Operation Manual for Live Operators, http://www.scribd.com/gawker/d/81877124-Abuse-Standards-6-2-Operation-Manual*
[30] *Cf. Torrent Freak. Police Censor Google, Facebook and 8,000 Other Sites by Accident, http://torrentfreak.com/google-facebook-and-8000-other-sites-accidentally-dns-blocked-120302*
[31] *See Internet Rights & Principles Coalition, www.internetrightsandprinciples.org*
[32] *"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*

on Freedom of Expression and the Internet by the four international Special Rapporteurs on freedom of expression.[33] 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.[34] However, recent reports confirm access as a human right.[35]

There is less controversy about the fact that the denial of access to the Internet as such or to part of its content through 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 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.[36]

Mobile Communications and Internet Access

Smartphones offer users a much richer experience of Internet access, beyond voice and SMS of feature phones. 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.

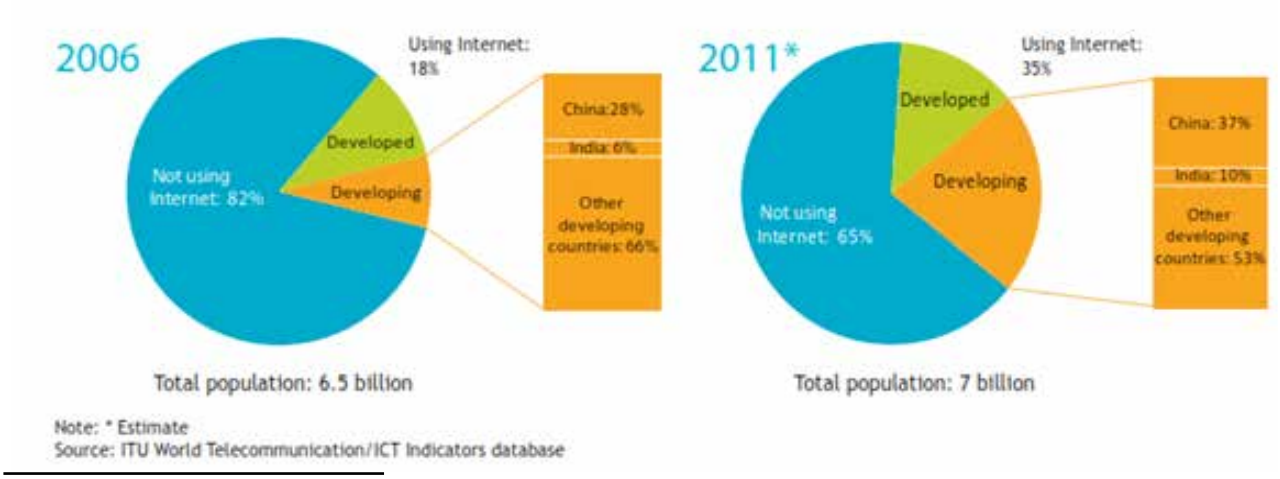
Mobile networks and the Internet differ in significant ways:[37] Mobiles are based on centralised networks, the Internet is based on decentralised networks; mobile services provided by the mobile operator are almost always paid services, but many websites and social media networks provide free or ad-supported 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 spawned 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.[38] Mobiles add a new twist by being both a medium and a content delivery platform . Mobile access to the Internet 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 citizen activists.

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



[33] *"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*
[34] *Cerf, Vint (2012). Internet Access is not a Human Right. In: New York Times (04.01.2012)*
[35] *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*
[36] *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*
[37] *Southwood, Russell (2011), http://www.apc.org/en/node/12433/*
[38] *Ibid.*

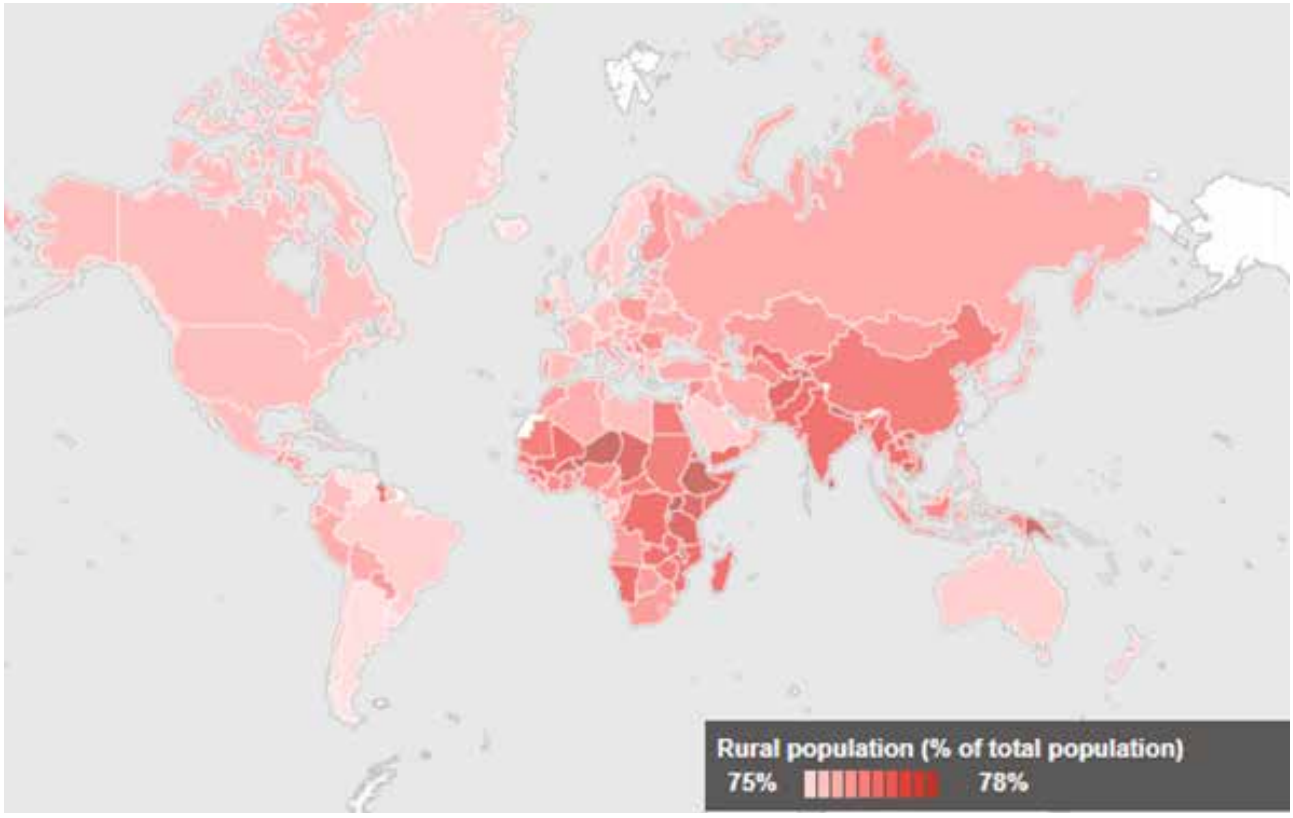
As the Internet is increasingly adopted on mobile phones, particularly smartphones, a new set of opportunities and challenges opens up in ensuring that mobiles are accessible and affordable around the world, and that mobile restrictions do not overlay Internet restrictions to content creation and consumption. 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 Figure 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 make do with 2G applications for a while longer until 3G coverage becomes widespread and affordable.[39]

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 macro-economic 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.

Many 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 Figure 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).

Figure 2. Distribution of rural population



Source: World Bank (2012), Rural Population (% of total population), available at http://data.worldbank.org/indicator/SP.RUR.TOTL.ZS/countries?display=map

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

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 peopl	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: National Telecommunication Union (November 2011)								via: mobiThinking	

Source: International Telecommunication Union[40]

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.

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: Websites that provide e-mail, Internet hosting, search, translation, Voice over Internet Protocol (VoIP) telephone services, 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.

[40] *ITU, http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html*

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 websites are the result of deliberate tampering.

5. No evidence of filtering: Testing did not uncover any evidence of websites 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. The 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 3.

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 Morozov[42] 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 2009,[43] 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.

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 Initiative[41]

[41] *The Open Net Initiative, http://opennet.net/research/profiles*
[42] *Morozov, Evgeny Morozov (2011). The Net Delusion: The Dark Side of Internet Freedom. PublicAffairs Books*
[43] *Ibid.*

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 cyberspace. Therefore, international co-operation 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.

The Internet as Enabler of 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".[44]

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, bloggers were able to share their views and experiences with the outside world, thus shaping international public opinion and garnering international solidarity.[45] They could inform about the situation in places where journalists were not allowed, using short films uploaded on YouTube and thus acting as community reporters or 'citizen journalists'. The experiences of Tunisia and Egypt repeated themselves 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,[46] 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 stopped.[47] 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."[48] Thus, except for very limited cases, a blanket regional or national shutdown is therefore unjustifiable under international human rights law.

---

[44] *Ibid. para. 22, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*
[45] *See Liechtenstein Institute at Princeton, Social Media Revolutions, All Hype or New Reality?, Spring 2011.*
[46] *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*
[47] *Nowak, Manfred (2005). CCPR Commentary, 2nd ed., Kehl/Strassburg/Arlington: Engel, Art. 19, No. 54*
[48] *Mukong v. Cameroon, U.N. Doc CCPR/C/51/D/458/1991 (1994), para. 9.7*

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 the rule of law should be preserved, but the user had also to accept major obligations. For example, the Data Retention Directive[49] of the EU requires all member states to commit 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 evaluation[50] 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: connectivity, content, community, commerce, culture, capacity, co-operation and capital.[51] 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.

Table 4: The "8 Cs" of the Information Society

	ICTs as an instrument	**ICTs as an industry**
Connectivity	How affordable and widespread are ICTs (e.g. 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?

[49] *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*

[50] *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*

[51] *Rao, Madanmohan (2003). "Visions of the Information Society: A developing world perspective." http://www.itu.int/osg/spu/visions/developing/index.html*

	ICTs as an instrument	ICTs as an industry
Co-operation	Is there adequate co-operation 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), Visions of the Information Society: A Developing World Perspective[52]

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, including China, 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	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	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

[52] *Ibid*

Type	Characteristics	Examples
Negotiating	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	1. Sizeable markets for Internet, e-commerce, wireless exist 2. Digital divide is still an issue, donor agencies are active 3. Political climate is generally free of censorship	India, Philippines, Brazil
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), News Media and New Media: The Asia-Pacific Internet Handbook[53]

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,[54] 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'.[55] 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".[56] It is against this background that John Peter Barlow, in 1996, promulgated his famous "Declaration of Cyber Independence".[57] According to this, 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 Lessing explained that "code", together with standards and protocols, the software and the hardware of cyberspace, really was the new law of cyberspace.[58] 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.[59]

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

There exist different modes 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 multi-stakeholder 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.

---

[53] *Rao, Madanmohan (2003). News Media and New Media: The Asia-Pacific Internet Handbook. Singapore: Eastern Universities Press*
[54] *Request for Comments 1855 (Sally Hambridge), http://www.dtcc.edu/cs/rfc1855.html, 24.10.1995*
[55] *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*
[56] *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*
[57] *Barlow, John Peter (1996). Declaration of Cyber Independence, Davos (08.02.1996), http:www.worldtrans.org/sov/cyberindepenedence.html*
[58] *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*
[59] *Cf. Cerf, Vint (2012). Internet Access is not a Human Right. In: New York Times (04.01.2012)*

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.[60] The organisation has developed a number of instruments to deal with human rights challenges on the Internet, including 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-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 was 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.[61]

The role of governments in ICANN was restricteo a Governmental Advisory Committee (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 do not participate 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, namely 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, such as the At-Large Advisory Committee representing the at-large community organised on a regional basis.[62]

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 ICANN[63] also 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 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.[64] Another reason might have been the refusal by ICANN to include "global public interest" consideration in its new policy on generic Top Level Domains.[65] 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.

---

[60] *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*

[61] *Cf. Kleinwächter, op. cit., 15ff.*

[62] *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*

[63] *See Kulesza, Joanna (2012). International Internet Law, Routledge: London, 132ff.*

[64] *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*

[65] *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://internationallawandtheinternet.blogspot.com/2012/03/good-news-or-bad-news-on-ntia-icann-itu.html*

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 at the 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.[66]

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

The World Summit on the Information Society (WSIS) was organised by the United Nations at the request of governments that felt 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 organised 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. It 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."[67]

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 multi-stakeholder 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.[68]

Human Rights at the WSIS

Human rights have been called the "missing link" between technology-oriented and value-oriented approaches.[69] They have also been portrayed as the "pole star" of the Information Society.[70] Human rights concerns were discussed in the Geneva phase, mainly through the instigation of civil society, which had organised an international symposium on that topic, producing pertinent recommendations.[71] The Geneva phase 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 Article 19 on Freedom of Expression in particular.[72] 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" (paragraph 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" (paragraph 4).[73]

Relevance of the Multi-stakeholder 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".[74] Taken together, the multi-stakeholder approach to Internet Governance is therefore based on the co-operation 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";

---

[66] *Cf. ICANN, Benefits and Risks of Operating a New gTLD, http://newgtlds.icann.org/en*
[67] *See Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1) (2005), para. 34*
[68] *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*
[69] *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*
[70] *Hurley, D. (2003). Pole Star: Human Rights in the Information Society.*
[71] *See Statement on Human Rights, Human Dignity and the Information Society, 04.11.2003; www.pdhre.org/WSIS/statement.doc*
[72] *See Declaration of Principles, Doc. WSIS-03/GENEVA/DOC/4-E of 12.12.2003, paras. 1 and 4*
[73] *See Tunis Commitment, Doc. WSIS-05/TUNIS/DOC/7-E of 18.11.2005*
[74] *Geneva Declaration of Principles, para. 49*

(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".[75]

The international community called for the multi-stakeholder approach to be "adopted, as far as possible, at all levels"[76] of Internet Governance. With the creation of the Internet Governance 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)[77]. 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 2012) 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 Centre[78], 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)[79]. Issues discussed include how IGF can continue to be a multi-stakeholder forum, supported by multi-stakeholder voluntary funding mechanisms with an independent secretariat.[80] 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, to have an expanded secretariat located within the UN system, and even to 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.[81]

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'[82] 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 Multi-stakeholder 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

[75] *Tunis Agenda for The Information Society, para. 35*
[76] *WSIS, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E of 18.11.2005, 34*
[77] *http://2012.rigf.asia*
[78] *www.apnic.net*
[79] *http://www.apricot.net*
[80] *APRICOT/APNIC 2012 conference, http://meetings.apnic.net/33/program/igov*
[81] *RIGF Asia, http://2011.rigf.asia/summary-reports/APrIGF%20Summary%20Report_Final_August%202011. pdf*
[82] *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*

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.[83] 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, namely 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.[84]

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,[85] which was first presented at the IGF in Vilnius in 2010 and since further developed.[86] For example, a commentary on the draft charter has been elaborated[87] as was a very condensed version of the Charter in form of "10 Internet Rights and Principles", in 2011.[88]

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.[89] 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 co-operation" 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 IGF[90] 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[91], Asia[92] Australia and the Pacific,[93] the Americas,[94] and Europe, where the first EuroDIG (European Dialogue on Internet Governance)[95] 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.[96]

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.[97] 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.[98] While this addresses

---

[83] *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, Lituania, 14.-17.09.2010, United Nations, Nairobi*

[84] *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*

[85] *Internet Rights and Principles Coalition, Charter of Human Rights and Principles, http://internetrights andprinciples.org/node/367*

[86] *Charter of Human Rights and Principles for the Internet, Version 1.1, at www.Internetrightsandprinciples.org*

[87] *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*

[88] *See Internet Rights and Principles Coalition (IRP), www.Internetrightsandprinciples.org*

[89] *See United Nations General Assembly Resolution A/RES/65/141 of 02.02.2011*

[90] *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*

[91] *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*

[92] *Asia Pacific Regional Internet Governance Forum (APrIGF), http://2011.rigf.asia*

[93] *Pacific Internet Governance Forum, http://pacificigf.org*

[94] *Latin American and the Caribbean Regional Preparatory Meetings for the Internet Governance Forum, http://lacnic.net/en/eventos/mvd2008/igf.html*

[95] *European Dialogue on Internet Governance (EuroDIG), http://www.eurodig.org*

[96] *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*

[97] *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*

[98] *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*

the general concern for cyber-security already discussed for some time in the United Nations and also the Council of Europe,[99] 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 General Assembly 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.[100] 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)[101] of ITU's International Telecommunication Regulations (IRTs)[102] 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, for example, extending the reach of the ITRs to all ICTs has led some commentators to warn of an "U.N. Threat to Internet Freedom"[103] or to identify the start of a "World War 3.0" between the forces of "order" and "disorder".[104] 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, and 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,[105] NGOs are feeling excluded from the internet debate in the ITU.[106]

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-governmental forum in order to redistribute power away from the US and big business.[107] India and some other countries want a multilateral body to have oversight of standard-setting, decision-making and crisis 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.[108]

Countries like Singapore have laws restricting websites and blogs that promote hatred of ethnic and religious groups.[109] Some countries with single-party systems have also implemented restrictions in cyberspace, ranging from firewalls to the 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.[110]

---

[99] *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*
[100] *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*
[101] *ITU, 12th World Conference on International Telecommunications, http://www.itu.int/en/wcit-12/Pages/default.aspx*
[102] *ITU, International Telecommunication Regulations (IRTs), http://www.itu.int/ITU-T/itr*
[103] *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*
[104] *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*
[105] *Katz, Ian (2012). Web freedom, faces greatest threat ever, warns Google's Sergey Brin, The Guardian, 15.04.2012*
[106] *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*
[107] *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*
[108] *Gan et al, (2003). Asian Cyberactivism: Freedom of Expression and Media Censorship. Bangkok: Friedrich Naumann Foundation*
[109] *Details can be found in George, Cherian (2012). Freedom from the Press: Journalism and State Power in Singapore, Singapore.*
[110] *Gan et al, op. cit.*

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."[111]

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."[112] 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.[113]

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.[114]

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.[115] Mary Robinson, former UN High Commissioner for Human Rights, has said that anti-terror legislation can "undermine journalistic integrity and discourage critical voices.[116] The Committee to Protect 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.[117]

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 websites 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.[118]

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

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 through 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.[119] 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, the EuroDIG.[120]

With the help of various groups of experts and sometimes in co-operation with other stakeholders, the Council of Europe has elaborated and adopted a number of declarations, recommendations 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.[121]

Regarding the role of human rights in the Information Society and Internet Governance, the Council of Europe, as early as 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".[122] It adopted human rights guidelines for Internet Service Providers,[123] human rights guidelines for Online Game Providers[124] and

---

[111] *Oo, Zaw (2003). "Mobilising online: The Burmese Diaspora's cyber strategy against the Junta." In Gan et al, op. cit.*
[112] *Lee, Eun-Jeung (2003). E-democracy@work: The 2002 presidential election in Korea. In: Gan et al, op. cit.*
[113] *Long, Geoff (2003). Why the Internet still matters for Asia's democracy. In : Gan et al, op. cit.*
[114] *Reporters Sans Frontiers http://arabia.reporters-sans-frontieres.org/article.php3?id_article=3676*
[115] *Seneviratne, Kalinga and Yeo, Lay Hwee (2011). Balancing Civil Rights and National Security. Singapore: AMIC and European Union Centre in Singapore*
[116] *International Freedom of Expression eXchange network (IFEX), http://www.ifex.org/international/2011/09/13/shadow_of_terror_laws/*
[117] *Seneviratne and Yeo, op. cit.*
[118] *Ibid.*
[119] *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*
[120] *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*
[121] *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*
[122] *Council of Europe, Committee of Ministers, CM (2005) 56 final of 13.05.2005*
[123] *Human Rights Guidelines for Internet Service Providers, developed by the Council of Europe in Co-operation with the European Internet Service Providers Association (EuroISPA), Council of Europe, Doc. H/Inf (2008) 9*
[124] *Human Rights Guidelines for Online Game Providers, Developed by the Council of Europe in co-operation with Interactive Software Federation of Europe, Council of Europe Doc. H/Inf. (2008) 8*

a Recommendation on measures to protect and promote respect for human rights with regard to social networking services and search engines.[125]

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 the 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.[126] Another focus will be advancing privacy and data protection while freedom of expression and information remains a core concern, as does effective co-operation 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.[127] It pronounced a European Digital Agenda in 2010, which also propagates the development of "digital user rights".[128] 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 be replaced by a new regulation and a new directive.[129] Users should be given more autonomy over their data including "a right to forget", or in other words, to have their data deleted by Internet intermediaries and service providers after a period of time.[130]

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 ICTs, including the growing use of censorship and surveillance mechanisms by States.[131] 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 Co-operation 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.[132]

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.[133] It has since focused on freedom of expression and privacy in particular[134] and developed implementation.[135] The multi-stakeholder collaboration has also developed

[125] *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%20 and%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/standard setting/media/MC-NM/MC-NM(2010)004rev2*

[126] *Internet Governance – Council of Europe Strategy 2012-2015, Council of Europe, Council of Ministers CM (2011) 175 final of 15.03.2012*

[127] *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*

[128] *See Granada Ministerial Declaration on the European Digital Agenda of 19.04.2010, http://ec.europa.eu/ceskarepublika/pdf/press/ks7rada.pdf*

[129] *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*

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

[131] *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*

[132] *Organisation for Security and Co-operation 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*

[133] *Global Network Initiative, http://globalnetworkinitiative.org*

[134] *Global Network Initiative, Principles, http://globalnetworkinitiative.org/principles/index.php*

[135] *GNI, Implementation Guidelines, http://globalnetworkinitiative.org/implementationguidelines/index.php*

standards of responsible company decision-making,[136] 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.[137] 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.[138]

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.[139] 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.[140]

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.[141]

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.[142]

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.[143]

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 "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.[144] 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 Nakornthap.[145] 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

---

[136] *GNI, Governance, Accountability & Learning Framework, http.//globalnetworkinitiative.org/governance framework/index.php*
[137] *See Mares, Radu (ed.) (2012). The UN Guiding Principles on Business and Human Rights.*
[138] *See Global Network Initiative, 2011 Annual Report, http://global networkinitiative.org/files/GNI_2011_Annual_Report.pdf*
[139] *See Google Transparency Report, http://www.google.com/transparencyreport*
[140] *Google Transparency Report, Government Requests, http://www.google.com/transparencyreport/government requests*
[141] *The Stockholm Principles for Governmental Transparency Reporting on Net Freedom, http://stockholm principles.org*
[142] *Rao, op. cit.*
[143] *Ibid.*
[144] *The Independent (2012), http://www.independent.co.uk/news/world/asia/thailand-backs-twitter-censorship-policy-6297296.html.*
[145] *Ibid.*

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.[146]

"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.[147] 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".[148]

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.[149]

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.

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.[150]

Internet access is inseparable from freedom of expression and its cousin, freedom of access to information, according to rights activist Adam Wagner,[151] who also observes that Internet use may fall within Article 8 of the European Convention of Human Rights (ECHR) – the right to family and private life – as well, 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.[152]

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 of the 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.[153] 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.[154] Civil rights are granted universally by a governing authority. And "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 […]. [L]aws, 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"[155]

---

[146] *Rao, op. cit.*
[147] *Loo, Eric (2003) in Rao, op. cit.*
[148] *Stewart-Smith, Hana (2012), http://www.zdnet.com/blog/asia/north-korea-makes-cellphone-usage-a-8216war-crime-under-100-days-of-mourning/834*
[149] *Ershadi, Julie (2012), http://reason.com/blog/2012/01/24/iranian-exiles-protest-halal-internet*
[150] *See Frank La Rue, op. cit.*
[151] *Wagner, Adam (2012), Is Internet Access a Human Right?, Guardian, 11 January 2012 http://www.guardian.co.uk/law/2012/jan/11/is-internet-access-a-human-right*
[152] *Gapper, John (2012), Halt the Silicon Valley Histronics, Financial Times, January 18, 2012, http://www.ft.com/intl/cms/s/0/04b98446-4112-11e1-b521-00144feab49a.html?ftcamp=rss#axzz1l3bRZVGZ*
[153] *Daily Caller (2012), http://dailycaller.com/2012/01/08/internet-access-not-a-human-right-says-father-of-the-internet*
[154] *Coldewey, Devin (2012), Is the Internet a Human Right?, http://techcrunch.com/2012/01/05/is-the-internet-a-human-right*
[155] *Ibid.*

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?

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".[156]

The UDHR assembles all human rights, including civil and political rights, as well as economic, social and cultural rights, under one normative roof. In its Article 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 Article 29 of the UDHR in full thereafter, which refers to duties and possible limitations.[157] It further lays down that in this way an information society shall be promoted where human dignity is respected.[158] 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.[159]

Further efforts to clarify the importance of human rights online come from civil society, which were already active during WSIS. The Association for Progressive Communication (APC), with a global membership, took the initiative and in 2006 drafted the "APC Internet Rights Charter",[160] 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.[161] Before, there have been various more limited attempts, like the "Charter for Innovation, Creativity and Access to Knowledge"[162] or the Declaration of Madrid on Privacy Standards in the Internet of 2009, prepared by civil society.[163] 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, 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 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	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

[156] *Geneva Declaration of Principles 2003, paras. 1, 3; Tunis Commitment 2005) and para. 2*
[157] *See WSIS, Declaration of Principles, paras. 4 and 5, op. cit.*
[158] *Ibid. para. 5.*
[159] *Ibid. para. 58.*
[160] *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*
[161] *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*
[162] *Charter for Innovation, Creativity and Access to Knowledge 2.0.1. – Citizens' and Artists' Rights in the Digital Age, http://fcforum.net/charter_extended*
[163] *The Civil Society Madrid Privacy Declaration, Global Privacy Standards for a Global World, 03.11.2009, http://thepublicvoice.org/madrid-declaration*

Rights Theme	Components
2. Freedom of expression and association	1. The right to access to knowledge 2. The right to freedom of information (e.g. from government) 3. The right to access to publicly-funded information
4. Shared learning and reation	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	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	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	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: APC[164]

Impact of Multi-stakeholder 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 Internet[165] 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, such as 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",[166] 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.[167]

So, is there a need for new digital rights? The Special Rapporteur on Freedom of Expression, Frank La Rue, in his report of 2011[168] 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*".[169] 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

[164] *APC, http://www.apc.org/en/node/5677/*
[165] *Internet Rights and Principles Coalition, Charter of Human Rights and Principles for the Internet, http://irpcharter.org/charter*
[166] *Geneva Declaration, para. 3*
[167] *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*
[168] *Report of the Special Rapporteur, La Rue, Frank (2011). Op. cit.*
[169] *Op. cit. note 158*

indicated in its Article 2, State parties are "to undertake steps, individually or through international associations and co-operation, … to the maximum of its available 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 on-going 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 context,[170] 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, and whether it will 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 b) Environmental sustainability
7)	**Freedom of Opinion and Expression** 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** a) Participation in Assembly and Association on the Internet b) Freedom to set up Online Communities and freedom of online protest

[170] *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)*

10)	**Privacy** 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** a) Protection of personal data b) Obligations of data collectors c) Minimum Standards on Use of Personal Data d) Monitoring data protection
12)	**Education** a) Education through the Internet b) Education about the Internet and Human Rights
13)	**Access to Knowledge and Culture** 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** 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** a) Respect for Workers' Rights b) Internet at the workplace
16)	**Participation in Public Affairs** 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)	**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),[171] 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),[172] international and intergovernmental organisations (e.g. OECD, OSCE, NATO, EU, UNESCO)[173] and non-state actors (e.g. Internet Rights and Principles Coalition).[174] 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.[175] 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 multi-stakeholder 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,[176] 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 multi-stakeholder-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, cybersecurity 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 2008[177] 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.

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.

---

[171] *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/inter national_strategy_for_cyberspace.pdf, 10*

[172] *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 Co-operation, 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*

[173] *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.os ce.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*

[174] *Cf. Internet Rights and Principles Coalition, 10 Internet Rights and Principles, http://internetrights andprinciples.org*

[175] *Council of Europe, Declaration by the Committee of Ministers on Internet governance principles, adopted on 21 September 2011, http://goo.gl/RxDWs*

[176] *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*

[177] *OECD Seoul Declaration for the Future of the Internet Economy 2008, http://www.oecd.org/dataoecd/49/28/40839436.pdf*

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 fulfils, by, for example, producing reports on Internet freedom like the Global Information Society Watch (GIS Watch) report[178] or the Freedom House report on "Freedom of the Net".[179]

Consequently, the promotion, protection and fulfilment of human rights on the Internet has become an issue of "mainstreaming",[180] or, in other words, 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.[181] 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 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, such as for video content access from countries other than the host country or region, or in the case of Spotify.[182] 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.[183]

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.[184] 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.[185]

---

[178] *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 Co-operation with Developing Countries (Hivos), www.giswatch.org/*

[179] *Freedom House, Freedom on the Net 2011, www.freedomhouse.org/report-types/freedom.net*

[180] *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*

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

[182] *The Economist (2010) http://www.economist.com/node/16941635*

[183] *Minkel, J. R. (2006), http://spectrum.ieee.org/computing/networks/could-the-internet-fragment*

[184] *Metz, Cade (2010), http://www.theregister.co.uk/2010/11/20/berners_lee_says_facebook_a_thret_to_web/*

[185] *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*

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.[186]

Net Neutrality

Net neutrality can be defined as a general principle requiring that all the information is channelled through the networks without any discrimination. This has to do with technical considerations, such as lack of capacity in peak periods, and economic or commercial considerations, such as pricing policy, 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.

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, as in Germany, or self-regulation as 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 pirated music or video. The provision allowing the user to be disconnected for a year has been cancelled by the Constitutional court.[187] 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, after two warnings addressed to the user, for a maximum of one month, which is the consequence of the necessity and proportionality principle applied to the constitutional freedom of expression.

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.[188]

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.[189]

Cited concerns of ISPs, both wireline and wireless, have been the rapid growth in file-sharing and video, and the 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.

III. Examples of Good Policies/Practices

Access to the Internet

Access to the Internet is crucial for benefitting from all of the opportunities connected with the Internet. As already mentioned, 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.

---

[186] *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/*

[187] *See note 185*

[188] *Berners-Lee, Tim, op. cit.*

[189] *The Economist (2010), op. cit.*

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 to achieve 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.[190] 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".[191]

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.[192]

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".[193]

In 2010, Finland amended its Communications Market Act with the provisions of Section 60 C declaring that broadband access is a basic right.[194] 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'.[195]

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.[196] 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.[197]

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 % for Sweden and 91,4 % for Luxembourg as

---

[190] *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 co-operation 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*

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

[192] *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*

[193] *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.*

[194] *Section 60 C, in: Communications Market Act, http://www.finlex.fi/en/laki/ kaannokset/2003/en20030393.pdf*

[195] *Boletin Oficial del Estado, 'Disposiciones Generales: Ley 2/2011, de 4 de marzo, de Economia Sostenible', documento BOE-A-2011-4117 in Boletin Oficial del Estado, No. 55, 05.03.2011, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-4117*

[196] *German Constitutional Court (BVerfG), 1 BvL 1/09, judgment of 09.02.2010, para. 135*

[197] *Organisation for Security and Co-operation 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*

the highest to 39,2 % for Romania and 46,9 % for Greece as the lowest ones.[198]

The EU is working on overcoming these gaps in Internet penetration and, more generally, to bridging the Digital Divide.[199] 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% of users thought Internet access should be a "fundamental right of all people".[200] Yet, more than two-thirds of the world's population does not have access to the Internet and many of those who 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).[201] In many developing countries of Asia, the penetration of cell phones has already exceeded the penetration of landlines; indeed, 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.[202]

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.[203] Mobile media have potential to bridge the digital divide in developing countries. Jonathan Donner[204] provides a detailed research review of how mobile media adoption and usage in developing countries, whereas Heather Horst and Daniel Miller[205] and Nicholas Sullivan[206] 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.[207] 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

---

[198] *Internet World Stats, Internet Penetration in Europe, http://www.internetworldstats.com/stats4.htm*
[199] *European Commission Information Society, 'European Broadband: Investing in Digitally Driven Growth'. In: Europa, http://ec.europa.eu/information_society/activities/broadband/index_en.htm*
[200] *Elsayed-Ali, Sherif (2012), http://www.egyptindependent.com/node/601891*
[201] *Techsparks: "Asia: Centre of the World's Wireless Explosion" http://www.techsparks.com/Asia-Centre-of-the-World-Wireless-Explosion.html*
[202] *Rao (2003), op. cit.*
[203] *Chen, Yi-Fan (2012). Mobile Theories and Frameworks. In: Bruck, Peter and Rao, Madanmohan (2012), Global Mobile. New Jersey: InfoToday Books*
[204] *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*
[205] *Horst, H. and Miller, D. (2006). The cell phone: An anthropology of communication. New York, NY: Berg*
[206] *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*
[207] *Quinn, Stephen. Mobile Journalism. In: Bruck, Peter and Rao, Madanmohan (2013-forthcoming), Global Mobile: Scenarios and Strategies. New Jersey: InfoToday/Perseus Publishing*

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% 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".

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% of the population is younger than 14; in Malaysia it is 29%. In the Middle East, more than 60% of the population is aged under 25.[208] 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".[209] The Tactical Technology Collective has documented a range of such examples of mobile activism: Ushahidi, documenting violence in Kenya; TXTpower, a consumer rights group in the Philippines; International Centre for Accelerated Development, monitoring elections in Nigeria; Women of Uganda Network, for 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 journalisms, 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.[210]

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.[211]

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.[212] It also has worked out together with the Association for Progressive

[208] *Ibid.*
[209] *Bahague, Rick and Banks, Ken (2008). Mobiles in a Box: Tools and Tactics for Mobile Advocacy, http://mobiles.tacticaltech.org*
[210] *Cf. Reporters without Borders, Enemies of the Internet Report 2012, http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html*
[211] *Council of Europe Recommendation CM/Rec(2007)/16 of 07.11.2007*
[212] *Council of Europe Recommendation CM/Rec(2009)/1 on Electronic Democracy (e-democracy) of 18.02.2009*

Communications and the United Nations Economic Commission for 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.[213] 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 Assembly[214] 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 IRP protection bills.[215] 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.[216] These protests resulted in the withdrawal of the controversial legislation before their adoption,[217] 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 cybercrime. Both the government and private companies would be authorised to monitor communications, and close down or block access to websites.[218]

With the Anti-Counterfeiting Trade Agreement (ACTA), the debate on how to protect IRPs while ensuring Internet freedom was internationalised. ACTA[219] 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 complement to the WTO Agreement on Trade-Related Aspects of Intellectual Property (TRIPS),[220] 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.[221]

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.[222]

Though some of the more fierce criticism is misplaced, the vague wording – including references to "fundamental principles such as freedom of expression, fair process, and privacy"[223] instead of "fundamental rights" – should invite critique, as should the high level of State autonomy in implementing surveillance in execution of ACTA.[224] Secondly, 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 Article 14 (2)

---

[213] *See Code of Good Practice on Information, Participation and Transparency in Internet Governance (October 2010), http://www.apc.org/en/node/11199*
[214] *See Giving World's Citizens a Voice, Campaign for a United Nations Parliamentary Assembly (UNPA), http:en.unpacampaign.org/index.php*
[215] *Sydney Morning Herald (2012), http://www.smh.com.au/opinion/politics/planned-us-antipiracy-laws-a-draconian-mess-20120118-1q5z0.html*
[216] *VOA (2012), http://www.voanews.com/khmer-english/news/US-Internet-Piracy-Bills-Find-Little-Support-in-Cambodia-137766413.html*
[217] *RT Network (2012), http://rt.com/news/poland-acta-protest-anonymous-823/*
[218] *See Reporters without Borders, Draconian cyber security bill would lead to Internet Surveillance and censorship, Press Release of 06.04.2012*
[219] *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*
[220] *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*
[221] *Cf. Article 6 ACTA*
[222] *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".*
[223] *Article 27 (2), (3) and (4) ACTA*
[224] *For a more comprehensive critique, see Opinion of European Academics on ACTA, http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opin ion_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*

of ACTA, are worded in a way that allows State parties to exclude application of ACTA,[225] 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 they wish, to use stronger police activity by ISPs.

The European Parliament has also taken a very critical attitude on the Anti-Counterfeiting Trade Agreement (ACTA),[226] negotiated by the European Commission largely without its participation although it is the one to ratify the agreement in the end.[227] 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.[228]

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 multi-stakeholder 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. Authors' 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.

IV. ICT/Human Rights Issues for Working Groups

Working Group 1: Freedom of Expression

Cybercensorship and Press Freedom

A number of watchdog organisations now track restrictions on freedom of expression around the world, both traditional and online, on a regular basis.[229]

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.[230] For the first time in eight years, global media freedom showed no overall decline. Freedom House found that 40.5% of the world's peoples live in a "not free" media environment, while 45% had a "partly free" press and just 14.5% live in counties with a "free press".[231]

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 the 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

---

[225] *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.

[226] *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*

[227] *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*

[228] *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)*

[229] *Reporters Sans Frontiers, http://march12.rsf.org/en/#ccmap*

[230] *YNet News (2012), http://www.ynetnews.com/articles/0,7340,L-4223280,00.html*

[231] *Relief Web: http://reliefweb.int/node/497932*

Asian bloggers have won "Reporters Without Borders" category awards, and moves by telecom authorities to block websites 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.[232] 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 websites have 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.[233] Forms of online activism can be either Internet-enhanced (e.g. coordination of physical activities) or Internet-based (situated entirely online). Another categorisation of online activism is: awareness/ advocacy, using the Web, email, encrypted documents; organisation/mobilisation, including 'armchair activism' or 'slacktivism' such as online petitions and signature campaigns, and lists of rallies and meeting places; and action/reaction, such as 'hacktivism' – taking down or defacing a website. Online activist equivalents of real-life strikes and boycotts have also emerged, for instance, in the form of the 'blackout' of websites 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, as the 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.[234]

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.[235] 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 hosting services, and Paypal which restricted access to WikiLeaks' account to prevent supporters from donating money.[236]

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

---

[232] *Reporters Without Borders, http://march12.rsf.org/en/*
[233] *McCaughey, Martha and Ayers, Michael (2003). Cyberactivism: Online Activism in Theory and Practice. New York: Routledge*
[234] *Glanville, Jo (2012), http://www.guardian.co.uk/commentisfree/2012/may/04/chen-guangcheng-exile*
[235] *APC, http://www.apc.org/en/pubs/briefs/wikileaks-human-rights-whistleblowers-under-attack*
[236] APC, http://www.apc.org/en/pubs/briefs/apc-says-stand-wikileaks-stand-freedom-information

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.[237]

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".[238] 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.[239]

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.[240]

Balancing Freedom of Expression and Hate Speech

Challenges can arise in balancing freedom of expression with freedom from discrimination, namely protecting free debate while not condoning hate speech, or promoting liberty without guaranteeing security. In the US, the government cannot restrict free speech except if necessary to prevent imminent physical harm, while European courts are not so insistent on a tight causal link between speech and violence.[241]

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 tolerance and arrest 'hatemongers' on the Net, though some politicians also advocate that breaches be handled through mediation instead of government intervention.[242]

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.[243] 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.[244]

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).[245] 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.[246]

---

[237] Article 19, http://www.article19.org/resources.php/resource/1755/en/supporting-freedom-of-speech-and-wikileaks
[238] 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/
[239] Inforrm, http://inforrm.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/
[240] Von Geldern, James and Jimenez, Ezequiel, http://macalester.academia.edu/EzequielJimenez/Papers/1036694/Diplomatic_Scandals_Leaks_and_Secrets_The_Case_of_Wikileaks
[241] Cherian, George (2011). Why Hate Speech Does Not Always Require the Red Card, http://www.straitstimes.com/BreakingNews/Singapore/Story/STIStory_740765.html
[242] Wong, Gillian. Singapore Jails Bloggers for Racist Speech, http://forums.yellowworld.org/archive/index.php?t-26498.html
[243] Cherian, George (2012). A conversation with UN Special Rapporteur Frank la Rue, http://hatespin.weebly.com/la-rue.html
[244] 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
[245] Cohen-Almagor, Raphael. Countering Hate on the Internet, http://ojs.ubvu.vu.nl/alf/article/view/138/264
[246] *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/*

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 (e.g. Cyber Patrol, Net Nanny, Cyber Snoop), though they have their limitations. There has also been concern about hate speech in game communities, through in-game chats that marginalise different groups, such as Muslims, African Americans, gays, and women. Online game communities should work towards creating a more welcoming and sensitive environment for players of every stripe.[247]

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.

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.[248] The European Court of Human Rights has already developed a significant case law around the internet.[249] The OSCE Representative on Freedom of the Media also engages into "Internet Freedom"[250] in the 56 countries belonging to the OSCE and the European Union is likewise committed.[251] 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.[252] These can be considered as examples of good practice in the struggle for human rights in the Internet.

Working Group 2: The Right to 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, together with new policies of Facebook and Google, which aim 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 younger generation is less concerned with privacy today because it is openly sharing a lot of information on itself through the Internet,[253] 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 in the workplace, where, according to laws and court decisions, employers must not read personal e-mail of their staff,[254] and with regard to privacy of consumers' data in general, which has recently been addressed by a publication of the White House on a possible "Consumer Privacy Bill of Rights".[255]

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 such as WikiLeaks or OpenLeaks.

---

[247] *Tan, Philip (2011). Hate Speech in Game Communities, http://gambit.mit.edu/updates/2011/03/hate_speech_in_game_communitie.php*
[248] *See Kettemann (2011). Op. cit.*
[249] *See European Court of Human Rights, Internet: Case-law of the European Court of Human Rights, Council of Europe, Strasbourg, June 2011*
[250] *OSCE Representative of the Media, Internet Freedom, Why it Matters, www.osce.org/fom*
[251] *See European Parliament resolution on freedom of expression on the internet of 06.07.2006*
[252] *Government Offices of Sweden, Enhancing Internet Freedom and Human Rights Through Responsible Business Practices, Ministry for Foreign Affairs, Stockholm 2012*
[253] *Though this is due mainly to changing notions of privacy. Cf. Rössler, Beate (2004), The Value of Privacy, Cambridge: Polity*
[254] *Cf. Privacy Rights Clearinghouse, Fact Sheet 7: Workplace Privacy and Employee Monitoring, http://www.privacyrights.org/fs/fs7-work.htm#4a*
[255] *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*

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 Article 12 of the Universal Declaration on Human Rights protects the right to privacy as does Article 17 of the International Convention on Civil and Political Rights. On the regional level, the European Convention on Human Rights in Article 8 protects the right to family life and privacy subject to certain limitations in the public interest. With regard to the European Union, Article 7 of the EU Charter on Fundamental Rights recognises the right to privacy and Article 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 must 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.[256]

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.[257] 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 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 stated 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.[258]

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.[259] 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.[260]

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 paragraph 4, which emphasises the right to freedom of opinion and expression and participation in the Information Society, corresponding

---

[256] *See supra, at p. 38*

[257] *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*

[258] *Ibid.*

[259] *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*

[260] *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*

to Article 19 of the UDHR, is immediately followed by the full text of Article 29 of the UDHR, reaffirming duties to the community and possible limitations (paragraph 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.[261] 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.[262]

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 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.[263]

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.[264]

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.[265]

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".[266] For example, the Data Retention Directive of the EU 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.[267] There is the issue of so-called "deep packet inspection" (DPI), which allows the analysis of data packets for network security or copyrights purposes, but is also used for censorship, for example, by keyword filtering.[268] On the other hand, there is little information on 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.[269]

---

[261] *See Arts. 2-4 of the Council of Europe Convention on Cybercrime of 2001*
[262] *See European Convention on Human Rights and Biomedicine and Additional Protocol to this Convention concerning Genetic Testing for Health Purposes of 1997*
[263] *See Council of Europe, Parliamentary Assembly, Res. 1843 (2011)*
[264] *Ibid.*
[265] *The Economist, Identifying a billion Indians, 27.01.2011, http://www.economist.com/node/18010459*
[266] *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*
[267] *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*
[268] *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*
[269] *See European Parliament, Study on Information and Communication Technology and Human Rights, by Horner, Lisa, et al on behalf of Global Partners (2010), 41ff.; EXPO/B/DROI/2009/24*

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 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.[270]

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.[271]

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 behavioural 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, including 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.[272]

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 and so forth.

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 allow 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 (CCTV) partly precedes the Internet. But services such as YouTube and the Google Street View have substantially enlarged the availability of audio-visual 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 was fined US$ 25,000 for impeding US investigations in its Street View Project by the Federal Communications Commission.[273] 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.[274]

---

[270] *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. 53ff.*
[271] *EDRI (European Digital Rights) – gram newsletter – Number 10.7 of 11.04.2012*
[272] *See Internet Rights and Principles Coalition, Draft Charter of Human Rights and Principles for the Internet, http://internetrightsandprinciples.org/node/367*
[273] *See the Guardian of 17.04.2012*
[274] *Cf. Geens, Stefan. Google Earth conspiracy watch — Sri Lanka war edition, http://ogleearth.com/2012/03/google-earth-conspiracy-watch-sri-lanka-war-edition/*

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?"[275] 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.[276] 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 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 engines[277] or social networks[278] 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.[279]

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 US, 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".[280] The background to this call is the divergence between US privacy principles and EU privacy law. The co-operation 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.[281] 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, meaning storage of data in a cloud, which can be anywhere.[282] Companies need to respect the rules on privacy and data protection, and States must provide quick, effective

---

[275] *See for the documentation http://thenextlayer.org/GoodbyePrivacy*

[276] *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.*

[277] *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*

[278] *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*

[279] *See Council of Europe Internet Governance Strategy 2012-2015, op. cit.*

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

[281] *See Mayr-Schönberg. "Delete", supra note.*

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

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.

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, which means 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.[283] 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.[284] Facebook had already made improvements to privacy settings in August 2011 giving users more control over their privacy.[285]

There is also a dialogue with 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 improve data protection for users, in particular the youth.[286]

Data Privacy in Asia

Asia Pacific Privacy Authorities (APPA)[287] 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).

Graham Greenleaf[288] surveys data privacy legislation developments across Asia, in terms of strength of protection provided by each law: the existence of a data protection authority (DPA); the 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. These were 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 further 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 Greenleaf[289]. In China, the Amendment to the Criminal Law of the PRC (February 2009) criminalises

[283] *Cf. the initiative Europe v. Facebook, http://europe-v-facebook.org/EN/en.html*
[284] *Cf. Ibid.*
[285] *See Facebook Changes Privacy Options, BBC News Technology, 23.08.2011, http://www.bbc.co.uk/news/technology-14633427*
[286] *Heise Online, 06.04.2012*
[287] *http://www.privacy.gov.au/aboutus/international/appa*
[288] *Greenleaf, Graham (2011). Asia-Pacific Data Privacy: 2011, Year of Revolution?, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1914212*
[289] *Ibid.*

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 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 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.

Working Group 3: The Digital Divide

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.[290] 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 (e.g. 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 (e.g. 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

[290] *Rao, Madanmohan (2009). ICT4D: Learnings and Best Practices. Singapore: AMIC*

Dimension	Active forces, challenges	Digital media responses
Livelihood	Poverty	Websites 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
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)[291]

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.

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-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 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), ICT4D: Learnings and Best Practices[292]

[291] *Ibid.*
[292] *Ibid.*

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 websites and email addresses	Percentage of departments with websites 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 websites
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)[293]

Working Group 4: The Right to Cultural Enjoyment of 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.[294]

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 (paragraph 19). This commitment is echoed also in the Tunis documents. But it is the Geneva Declaration which 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".[295]

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.[296]

[293] *Ibid.*
[294] *See WSIS I, Geneva Declaration of Principles, op. cit.*
[295] *Geneva Declaration of Principles, paras. 52*
[296] *Cf. ICANN, Internationalized Domain Names, http://www.icann.org/en/resources/idn*

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".[297] 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.[298] 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.

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.[299] The commitment of the International community also encompasses promoting the capacity of indigenous peoples to develop content in their own languages[300] 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".[301]

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 Internationalised 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.[302]

In the IGF the discussion was continued in several multi-stakeholder workshops on realising a multilingual Internet and 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.[303]

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, and 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 marginalisation 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 digitalisation. 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".[304] Through the Internet, harnessing and preserving cultural heritage for the future has become much easier. One example is the Google Art Project[305] 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 –

[297] *Geneva Declaration of Principles, para. 53*
[298] *Compare WSIS II, Tunis Agenda for the Information Society, op. cit.*
[299] *Cf. Ibid., para. 23 d)*
[300] *Ibid., para. 23 k)*
[301] *Ibid., para. 23 l)*
[302] *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, 167ff.*
[303] *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*
[304] *Ibid. para. 54.*
[305] *Google Art Project, http://www.googleartproject.com*

including traditional knowledge – providers in the Information Society".[306]

Regional Initiatives for Cultural Promotion and Diversity

The South Asian Association for Regional Co-operation (SAARC) set up a Cultural Centre in Sri Lanka as a regional centre to promote cultural co-operation 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 region[307] (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 co-operation for sustained human resource development, developing a platform for cross-sector dialogue, and co-operation 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).[308] Cultural practitioners take part in bi-regional co-operation, 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 Article 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 scientific, literary or artistic production of which he is the author. This includes intellectual property rights such as 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: 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 defence of cultural diversity is presented as an "ethical imperative, inseparable from human rights".[309] 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 – so called "digital literacy" – and the promotion of linguistic diversity in cyberspace.[310] 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 UNESO 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.[311] 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. Article 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, Articles 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 of 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 of the Internet related to Article 27 of the UDHR: the right to

---

[306] *Geneva Plan of Action, para. 23 b)*
[307] *The Daily Star, Bangladesh (2012). Cultural diversity declaration, http://www.thedailystar.net/newDesign/news-details.php?nid=233851*
[308] *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*
[309] *See Arts. 1 and 4 of the Declaration, http://unesdoc.unesco.org/images/0012/001271/127160m.pdf*
[310] *Ibid.*
[311] *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*

participate in the cultural life of the community; the right to access to quality and diverse information as well as different cultural content; the realisation of culture and linguistic diversity on the Internet in all forms, including 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.[312]

Cultural diversity has been proclaimed as a new principle, if not already an emerging right mainly in the context of media and globalisation.[313] The discussion on an audio-visual 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 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 protecting 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.[314] 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.[315]

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.[316] 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 it 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.[317] Disorganised 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".[318]

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 (IRPs) who are supposed to earn their living from them[319] or to benefit from an exclusivity during a certain period to 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" (paragraph 1) and, in paragraph 2, gives everyone the right

---

[312] Compare draft Charter on Human Rights and Principles for the Internet, op. cit.

[313] 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, 189ff.

[314] Ibid., at 209

[315] 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

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

[317] 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

[318] 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

[319] 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 "courtesans" (in that respect, the author IPR was also linked with freedom of expression). Benefiting of a new right of property, 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.

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 paragraph 1 of Article 27, while opponents focus on the "material interests" protection clause of paragraph 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.[320] It suggests reframing the way patents are granted and IP is protected worldwide, including through the Berne Convention and TRIPS.[321] Further, it introduces the notion of "knowledge commons", the 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,[322] which allows creators of materials to share these while retaining certain rights. There are also considerations on new models to compensate author's rights, such as through 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, including new sources of revenue and visibility for publishers, or new business models for search engines. New forms of content and information have also 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.[323]

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 framing external content, rights and duties of commercial aggregators, authorised and 'unauthorised' translations, 'screen scraping' 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.[324] 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".

Lessig[325] 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 Bollier[326] 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 website or an ISP) liable for the presence of illegitimate content on their site.[327] Sites like Dropbox, YouTube and Facebook as well as emerging 'cloud' computing and hosting providers can be shut down 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.[328] 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 websites and thus does not hurt them. The site, which was launched in 2009, has over 10 million users.

---

[320] *Access to Knowledge Treaty (2005), http://www.cptech.org/a2k/a2k_treaty_may9.pdf*

[321] *Generally speaking, IPRs 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).*

[322] *Creative Commons, http://creativecommons.org/licenses*

[323] *Google Art Project, http://www.googleartproject.com*

[324] *Lessig, Lawrence (2006). Code. Version 2.0, New York: Basic Books, http://codev2.cc*

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

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

[327] *Harzog, Bernd (2012). SOPA and PIPA, http://www.virtualizationpractice.com/the-sopa-and-pipa-kerfluffle-14272/*

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

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'.[329] 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.

"The Internet will create a world where there is much more art, much more culture, much more learning and knowledge," according to Robin Gross,[330] 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 Center 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.[331] 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.

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,[332] 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 fewer 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 versus 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 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 on-going 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 'cybersecurity'. They want the identity of the user to allow for governmental surveillance. This would arguably be the end of privacy.

---

[329] *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*

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

[331] *Palfrey, John (2012). "Alternative Compensation Systems for Digital Media", http://blogs.law.harvard.edu/palfrey/alternative-compensation-systems-for-digital-media/*

[332] *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*

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"[333] 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 (e.g. 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.[334] 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.[335]

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 cyberwar. 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 December 2012 both have to consider the role of Internet Governance Principles and how they can be translated into practice.[336]

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

---

[333] *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*

[334] *See World War 3.0, op. cit.*

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

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

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.[337] 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 non-governmental organisations developing technologies to assist activists inside repressive countries to stay connected, regardless of government efforts to keep them silent.[338] The 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, however, 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.[339]

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;[340] Harris, 2004;[341] Howard, A. L., 2010;[342] Howard, P. H., 2004;[343] Kellner and Share, 2007;[344] Winston, 1998[345]).

Smart mobs, as first identified by Howard Rheingold,[346]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.[347]

With the convergence of Internet and mobile, tools like Ushahidi have emerged, which offer an open-source platform available to developers to create crowd-sourced 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 networks. Physicist Michio Kaku[348] 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).

---

[337] *The Economist (2012), http://www.economist.com/node/21542748*
[338] *Crawford, Jamie (2012), http://security.blogs.cnn.com/2012/01/30/the-unseen-global-revolution/*
[339] *Pamela Rutledge: Psychology of Mobile. In: Bruck, Peter and Rao, Madanmohan (2013-forthcoming), Global Mobile: Scenarios and Strategies. New Jersey: InfoToday/Perseus Publishing*
[340] *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*
[341] *Harris, R. J. (2004). A Cognitive Psychology of Mass Communication (4th ed.). Mahwah, NJ: Lawrence Erlbaum Associates*
[342] *Howard, A. L. (2010). Engaging the City: Civic Participation and Teaching Urban History. Journal of Urban History, 36 (1), 42-55*
[343] *Howard, P. H. (2004). Society Online: The Internet in context. Thousand Oaks, CA: Sage Publications*
[344] *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.*
[345] *Winston, B. (1998). Media Technology and Society: A History: From the Telegraph to the Internet. London: Routledge*
[346] *Rheingold, H. (2002). Smart Mobs. Cambridge, U.K.: Perseus Books*
[347] *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*
[348] *Kaku, Michio (2011). Physics of the Future: The Inventions That Will Transform Our Lives. New York: Penguin Books*

Table 11: Technology Evolution for the 21st Century

Technology category	Near Future (present to 2030)	Mid-Century (2030 to 2070)	Far Future (2070 to 2100)
Computing	- Internet-enabled glasses, contact lenses - Driverless cars - Four-wall screens - Flexible electronic paper - Safety chips in clothes	- End of Moore's Law - Ubiquitous augmented reality - Universal translators - Holographic Internet	- Machine control by thought (telekinesis) - Portable brain scans - Photographing dreams - Mind reading
Artificial Intelligence	- Expert systems in healthcare	- Modular robots - Robot surgeons and cooks	- Conscious machines - Human mergers with robots
Medicine	- Genomic medicine - Cloning; stem cells	- Gene therapy - Designer children	- Reversing aging - Resurrecting extinct life forms - Creating new life forms
Nano-technology	- Nanocars in our bodies - DNA chips - Quantum computers	- Shape shifting	- The Replicator
Energy	- Solar/hydrogen economy - Electric cars	- Global warming and flooding - Nuclear fusion power	- Magnetic cars and trains

Source: Adapted from Michio Kaku[349]

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 drive 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 explore further alternatives such as quantum computing or bio-computing.

References:

Annexe 2: Questions raised by the background paper

Annexe 3: Bibliography for the Background Paper

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

Concluding Remarks

Ambassador Olof EHRENKRONA
Political Ambassador/Senior Advisor to the Minister for Foreign Affairs – on behalf of the Raoul Wallenberg Institute

Ladies and gentlemen, excellencies and participants,

Let me start by thanking the organisers, our Korean hosts – the Department of Foreign Affairs and the National Human Rights Commission of Korea – the panellists, the moderators and all of you participants taking part in the debates and talks over the last three days. Heartfelt thanks also to the Asia-Europe Foundation, the Raoul Wallenberg Institute and their clever and competent personalities for their thorough preparatory work. We also thank the financiers, the European Commission, the French Foreign Ministry and SIDA, the Swedish Development Agency. And last but not least, many thanks to Dr Wolfgang Benedek and Dr Madanmohan Rao for their very comprehensive Background Paper. Let us give all of them a big hand.

Arranging the 12th Informal ASEM Seminar on Human Rights on the subject of ICT here in Seoul is actually most appropriate, since Korea is in every ranking made in recent years performing among the top three of the most advanced ICT nations in the world. This development of Korea as a global frontrunner in the technological revolution of today and tomorrow is of course strongly linked to its post-war economic success story, and the past decades of democratic transformation. Few countries, if anyone, pose a better example of the positive interaction between development, political reforms and technological progress.

If Seoul is an appropriate place, so is the theme of the 12th Informal ASEM Seminar on Human Rights. The debate on human rights on the Internet is climbing fast on the multilateral agendas. Only yesterday, Sweden and a group of countries put forward a resolution to the Human Rights Council in Geneva. The content is clear and simple; it states two things. Firstly, that human rights offline must be applicable also online. It particularly mentions Article 19 of the UN Universal Declaration on Human Rights – the article about freedom of expression. Secondly, it underlies the link between access to the Internet and the protection of human rights online. Up to now, seventy countries are co-sponsoring this resolution, which, if it is adopted, will represent a breakthrough within the UN framework for the recognition of the principle that human rights offline also must be protected online.

That Asia and Europe meet and exchange views on these issues is an important contribution to the wider global dialogue and typically what we should do within the ASEM framework. We will not always be of the same opinion but we live in the same technological environment. Ninety per cent of the globe is now covered by cell phone systems, and the combination of evermore powerful and sophisticated cell phone technology and cloud computing will help us to preserve the universal character and the oneness of the Internet.

Today there are between four and five billion devices on the Internet. In three years' time there will be three times that number, and before 2020 there will be 50 billion devices connected. We are entering the age of hyper-connectivity.

This seminar has had a strikingly optimistic undertone. The focus has been on the opportunities, while still not forgetting the important challenges. Human communication is, by definition, interaction, and interaction will never happen without conflicting interests, views and beliefs. This is actually an indispensable part of dynamic, pluralistic societies characterised by social change and development.

But the most important challenge , however, will not be to tackle the problems of ICT but, to be fast and smart enough to grasp all the opportunities emerging out there. ICT is a vital part of the most profound and fastest technological transformation ever in the history of mankind. Wherever we look when studying today's frontline research and the application of modern science and technology – be it in life sciences, in materials and nano-technology, in optics, in robotics and automation, in cosmology, in string theory and quantum mechanics – you find ICT and digitalisation as a common tool and denominator.

The theme of this seminar is consequently farther reaching than we may normally think. It is not only about our everyday use of the Internet for mailing, surfing or social interaction. It is very much about human progress per se. It is about our possibilities to fight poverty and hunger, our possibilities to meet environmental challenges and tackle climate change. In short, it is about our possibilities to create a better, more just and free world.

ICT is the technology driving two of the megatrends of our time – globalisation and individual empowerment. Human rights protection is a must, and must be so, in the modern information, international society.

Thank you.

Concluding Remarks

Mr Frédéric TIBERGHIEN
Technical Coordinator & Representative of the Ministry of Foreign and European Affairs, France, & State Counsellor - Conseil d'Etat

Excellencies and distinguished participants, ladies and gentlemen,

We have worked together to achieve a great deal as participants at this seminar. Together, we have identified the main issues regarding ICT and human rights. We have identified the main threats and opportunities, and have identified issues to promote and protect human rights in ICT. We have also formulated some key messages to be channelled to the next ASEM summit leaders, so we can congratulate ourselves for the results that we have achieved. When I was asked to deliver the conclusion, I wondered what to say after these three days of hard work. One possibility would have been to try to summarise the recommendations and conclusions. Another possibility would have been to record our convergences and divergences. But I have decided to put all this aside and to answer another question. What is the rationale, what is the logic, what is the coherence, what is the consistency of all our recommendations or all our conclusions? And what is the degree of certainty that we can put here and there? I dare say that I came to this seminar with some pre-formed ideas on human rights and ICT, and now, after working with all of you for three days, I have more doubts than certainties. I would like to elaborate on these doubts.

My first question is, are ICTs a real danger to human rights?

As I attended the side event, organised by the National Human Rights Commission of Korea, I spontaneously adhered to the point Professor Lee elaborated in his paper. He says in his briefing, that we live in a recording society, where everything is recorded. And I quote him - if only we could view society as inevitably possessing the nature of total surveillance of the collective. What Professor Lee has meant is that the surveillance of society at home leads one to enter the private sphere.

When I was a young student, I read the books of the famous philosopher Michelle Foucault, who wrote about surveillance and punishment. When States took their modern forms in the 18th and 19th centuries, their administrations tended to standardise the behaviour of citizens. They tried to control private life. They tried to separate abnormal or deviant citizens from the normal ones, sending them to hospitals, jails, or other places immune from laws. Following that analysis, ICTs can be seen as being on the verge of giving States the means to put in place that surveillance society which was the dream of many 19th century statesmen.

Traceability of goods, traceability of food, and traceability of capital-flows have been on the international agenda for years. But now, by adding personal profiling, we are able to add the traceability of individuals and their actions, deeds and thoughts. All of this is now in our reach, and so it seems that, from a human rights perspective, the main threat, the main source of danger, remains the State in that respect.

We must remind ourselves that human rights are, above all, the rights of individuals towards States. This relates back to the birth of human rights as we know them today, emerging from the ashes of World War II and the Age of Dictatorships. It was the protection of the individual against totalitarian states, which wanted total control over society. Human rights are thus commonly understood as absolute rights directed against totalitarian or intrusive states. I think our debates largely illustrated this conception, since we argued that we do not want too many data in the hands of States; perhaps it is better to have them in private hands. We wish to limit the power of the State. Furthermore, if we have to bestow greater authority somewhere, we would rather deliver such power to an independent authority, such as the data protection authority. Ultimately, we would rather have strong control by an independent justice, a sign of our remaining distrust toward the State.

However, our Background Paper and our discussions also pointed out a novel threat. This threat to human rights can now be found in large private corporations which collect personal data and re-sell them in order to make profits, irrespective of privacy rules. In addition, the emergences of social networks in more recent years have aggravated this threat, all the while standardising the behaviour of citizens. We therefore made recommendations in this direction, namely, that we must put some controls on these companies. We must prevent them from reusing the data without the permission of the citizens. In order to avoid the standardisation of behaviour, we also recommended promoting diversity of culture and languages through the Internet.

But two enemies are not enough! So we identified a third threat. It is what I call the 'criminals'. With ICT, criminal organisations have, in fact, developed greater opportunities, and gained strengths and a better reach to the mainstream public. At the top of their criminal lists, States place terrorists who have attempted to threaten public security. In order to address that issue, we have expressed recommendations to accept exceptions to human rights in order to fight against cybercrime and criminal organizations, and to answer to the

security of transactions on the Internet. I also noted that the Council of Europe Convention on Cybercrime (2001) is one of the international conventions on ICT, and it remains open to signatures outside Europe.

Another very important point we noted was the trend to also criminalise the violation of intellectual property rights. We cited counterfeiting among many more crimes. I have to recall here that the exercise of freedom is also linked to property rights. I remember that the revolutions of the 18th century, whether American or French, also recognised the right of property as a fundamental right. This philosophy seems to be colliding today with some of the aforementioned rights. Hence, we recommended accepting infringements of human rights by the State, whether in property rights or private life, given the superior interests of public security. This mind-set is the basis of security and respect for private property in liberal societies, which is also a legacy of the revolutions of the 18th century.
We also discovered a new threat: the users themselves on the Internet. This is because, behind human rights, there is also the fundamental concept of the dignity of the person and the equality of all human beings. However, through the Internet, we have seen that there are various forms of violation of human dignity, such as racism, prostitution, pornography, and paedophilia. We therefore also made recommendations in that direction, stating that we must protect minors and the vulnerable so that their dignity is secure even within the realm of ICT.

We could be tempted to call a provisional conclusion here. We have, after all, identified four different threats to human rights through ICT. Perhaps we have to safeguard human rights in four directions altogether. We have identified four isolated forces or threats pursuing different goals.

But allow me to hypothesise that all of these actors were finally sharing the common interests of developing ICTs as they are. Let me assume that the digital society is in a way the synthesis of three or four driving forces. First of all, the welfare state is regarded, according to its 20th century design, as putting the accent on social justice. Professor Lee perfectly underlined that ICTs helped the welfare state to recover the efficiency that it had lost in the past decades.
The second driving force is what I call the market society which has been promoted since the 1970s. In brief, it is technology-driven, and the thought is that the market will bring all the solutions and all the consumer satisfaction our societies need. ICT is therefore a sort of legacy of the market society.

The third force is unlimited individualism, which is in turn the legacy of the Enlightenment of the 18th century. With distrust towards any institution, we are above all confident in the individual. In that way, I think that the Internet is the starting point where all types of freedoms triumph without any restrictions. It is the perfect accomplishment of the individualistic approach of the human rights of the 18th century.

I also have to mention the recent arrival of crime in international relations. We could elaborate greatly on this. Crime has developed in recent decades owing to the liberalisation of international commerce and the increasing flow of capital, tax-free harbours, the withdrawal of the State in many domains, globalisation and the emergence of new technologies. Now we see the emergence of criminal states acting in international relations. That is a new-born of the three aforementioned forces.

Now that we have consensus on all these actors who develop the ICTs, perhaps we can ask *why is there so little consensus to develop ICTs as they are developed?*

A hypothesis could be that we have entered into a 'soft democracy', a term loosely connected to the terminology of 'soft diplomacy'. The Internet is a tool of soft democracy. I shall come back to that concept later, but it is also in many ways an introduction to a soft salvation, one might say. Since the internet society brings everything, transforms citizens into consumers, and makes users happy, or happier, we are now witnessing a digital society which accompanies a kind of soft salvation where everybody is happy with the State, with private companies, with the possibility of connecting people, with the access to universal knowledge. It is a kind of happiness for everybody through ICT and that is an importance that we cannot sweep away.
Some signs of that consensus among the different actors are that the States are the first to promote the development of ICT. They have developed, of course, e-administration of the e-democracy, they strive to fight against the digital divide, and they have developed and sustained e-commerce. So we can see that even States are promoting the development of these new technologies. The investment, of course, is in the network and so forth.

So, we can perhaps conclude that there is an objective alliance between these three driving forces: the states, the private sector and the consumers. One point that ought to be underlined is that I have not heard anybody here protest or plead for any limitation of the quick expansion of ICT. I can thus conclude that there was a total consensus to continue to develop this technology. As Jeremy Rifkin pointed out as early as the year 2000 in his book The Age of Access, there is no longer any difference between communication, communion and commerce. So we are all happy together with communication, communion and commerce as a perfect synthesis of the trends of ICT.

My second question is a difficult one: is ICT a real threat to democracy?

The underlying assumption in the United Nations is that

human rights flourish in democratic regimes, and that is a pre-condition for democracy to expand. I have noticed two achievements of ICT from the democratic perspective. First of all, the development of fora. We talked about line assembly, but a forum in the time of the Roman Republic was a place where citizens gathered to debate, to exchange common views so as to decide on public interests, and to elect their representatives. So they consulted, they debated, they participated. We can remark that there existed a fantastic outreach for political democracy, because it allows people to connect and to access information. In that sense, I think it is a ground for the democracy nowadays and we understand better why some totalitarian states want to curb or to censor this e-democracy.

The overachievements of ICT are the famous social networks. I recall that the Greek philosophers, from Plato to Aristotle, told us that human beings are firstly defined as social beings. This is characterised by the primacy of society over the individual. Through social networks, I have noted that citizens share their common interests, tastes, hobbies, political ideas, cultures, and forms of expression. In that respect, social networks reinforce networking inside civil societies. They also strengthen cohesion and give a voice to minorities. The working group thus insisted on the necessity to protect and promote diversity, minority rights and I believe it is also one of the roles of social networks to promote cultural diversity through the sharing of cultural knowledge and of language. If we look at these achievements globally, ICTs are human rights enablers. Indeed, they have links with freedom of association and freedom of expression, and we can recognise the fundamentally positive role of ICT towards democracy. It is my conviction that as democratic citizens, it is our duty to accompany this phenomenon. Having said that, one may ask to whom is this new form of democracy beneficial?

There are four types of interpretation on the relationship between ICT and democracy. For some commentators, the Internet is not a tool for democracy or popular sovereignty, it is a tool for the majority. We can see this in a hypothesis put forward by Thaled in 2007, that on the Internet, the dominant version is on the top of the pages. The minority views are exiled to the bottom of the list. So in that sense, it suppresses what we call 'black swans'. In that respect, the recommendation should be to protect minority rights, to prevent the overwhelming power of the majority on the Internet.

For other commentators, such as Daniel Cardon, the internet allows for self-government of society, out of the control of the State, of political parties, or of unions. It favours freedom of expression with anonymity and supports unconditional equality between citizens. This point is also very interesting. According to the philosopher, Jacques Ranciere, democracy is power exerted by incompetent people. On the Internet, all the incompetent people have a voice and use it. That is democracy: to give a voice to the incompetent people to decide on public affairs. In that case, the problem should be to escape from the State and increase the self-government of society. That, of course, is perceived by States as a threat. According to a third analysis, other commentators underline that ICTs contribute to and develop the autonomy and diversity of society. Here, again, we find the famous opposition between the State and civil society. The Internet contributes to the self-organization of citizen-to-citizen activism. The risk here, which we highlighted over the last two days, is the fragmentation of the political public sphere through the division brought by the Internet.

Yet, for other commentators the Internet allows for a permanent test and evaluation of public decisions. Pierre Rosanvallon, in his 2006 book Counter-Democracy: Politics in an Age of Distrust, suggests that the Internet is the expression of the powers of screening, of vigilance, of denunciation, and of evaluation, which categorizes counter-democracy. The concept of counter-democracy is also very important because it is, in that sense, a political ecosystem of democracy with a power-base which permanently evaluates its criticism and interacts with the official power.

These four interpretations, in my view, are very interesting as they do not lead to the same recommendations. As a future step, we need to be clear on the analysis we have on the role of ICT towards democracy to promote such recommendations, because they do not all have the same effect on democracy.

I would like to address the third very difficult question. Of course, we aspire to and recommend new regulations for ICT, but can ICT and the Internet be regulated? If yes, by what kind of rules? How, again, do we find different analyses?

Some argue that the internet cannot be regulated, as it is not a traditional mass media. There is no content, nor network of diffusion. It is only a user-centric communication tool which cannot be regulated. Moreover, internet networks are private networks. A more substantial agreement is that ICT development is driven by two major forces which cannot be controlled: science and technology, one the one hand, and competition in the market on the other.

I will end with this notion: ICT cannot be controlled because it is first driven by science and technology. On that thought, Professor Lee said that the challenge is to establish a counter-surveillance model which can minimise the dangers that ICT imposes on individual privacy. But here I depart from him. I think that the challenge is not to establish a counter-surveillance model with the help of ICT, but to use ICT to limit personal data infringement and the breaches of human rights. I believe that our work touched on very sensitive recommendations regarding privacy by design, and

privacy-enhancing techniques, meaning the use of science and technology to limit the breaches of human rights. We thus recommended the proactive regulation of science and technology by incorporating, right from the development phases, the tools to limit the breaches when software is developed.

Another way to regulate the internet is through the use of competition laws. We touched very lightly on that subject. I think that some private actors are in a dominant position here. We have noticed also that the European Union uses competition laws to sue American firms which are in a dominant position in the field of ICT. It is my thought that we did not insist enough on the leverage of competition law to regulate the sector. The high technology sector is subject to regulation, on grounds of anti-competition or dominant positions. It can also be regulated with the leverage of the investment in the infrastructure: under European law, for example, when infrastructure is qualified as essential, it has to be regulated by an independent authority.

One can also leverage through the pricing and the return of the investment on the infrastructure and, for example, for freedom of access. There are only two ways to develop access on economical basis. The first way would be to increase competition. The second way is to establish a social tariff to allow everybody to access the Internet. Some countries have chosen competition, others have established social tariffs.

A further way to regulate is to establish quality standards. That topic is behind the net quality aspect; perhaps it would be helpful to set quality standards to regulate this sector. Unfortunately, we did not dedicate enough time to reflect on this, even if it was mentioned in regards to consumer law, as access is between a private operator and a consumer. I think we could also encourage the suing of companies which have illegal or unbalanced clauses in their contracts. There is the possibility of favouring the cancellation of a contract and exit costs for Internet subscription which are very important and that is subject to the consumer law.

I will conclude by raising a last point because there are some possible disagreements about the question of privacy and identity in the real and virtual worlds. I was a little surprised by the draft Charter of Human Rights and Principles on the Internet. It is commonly accepted that anonymous traffic is a right, but are we sure that supporting the anonymity of the Internet is a clever solution? As the German philosopher, Jürgen Habermas, once said, the dignity of a person is in the face, and he elaborated the fact that human rights are the rights of a person, and a person is a face. So how do we implement human rights to a person who has no face, whom we cannot identify? Working Group 1 underlined perfectly that online meeting and online freedom of association raised question marks. How can we have rights if we cannot identify the face of the person with whom we meet? Are there risks with anonymity? How can we trust someone if we do not see him or her? How can we say, “we will increase our trust in the Internet”, while supporting the anonymity of these networks? I am not sure that we are really consistent when we promote anonymity on the Internet. I see many drawbacks. I do not see many advantages except the limited number of cases to protect, for example, asylum seekers, or human rights activists, or literature where one uses an assumed name from time to time. Except for these cases, I do not see the advantages of anonymity. I raise this as a question mark because it ought to be discussed at some point.

Finally, we can say with confidence that many challenges are ahead of us. I am, however, convinced that we can have more privacy and more human rights with ICTs. That is the road which we ought to follow, the first task being how to establish a virtuous cycle between these forces so that we can have a positive judgement on what the Internet really is. The second task that we have ahead of us is to design a digital culture. We have to invent one with a concept of what a digital culture is. We also have to design a multi-stakeholder governance of ICT. We talk about co-regulation, but also acknowledge that it is not yet perfectly functional. Everything has to be designed from scratch. Hence, a lot remains to be done.

Thank you ladies and gentlemen for your hard work and contribution.

Annex 1

List of Acronyms and Abbreviations

e.g.	exempli gratia, for example
ff.	following pages
Ibid.	ibidem (in the work cited in the immediately preceding reference)
No.	numero, number
Op. cit.	opere citato (in the work cited above)
p.	Page
para.	Paragraph
pp.	Pages
vs	versus, as opposed to
A2K	Access to Knowledge
ACTA	Anti-Counterfeiting Trade Agreement
AoC	Affirmation of Commitments
APC	Association for Progressive Communication
APEC	Asia-Pacific Economic Cooperation
APPA	Asia Pacific Privacy Authorities
APRICOT	Asia Pacific Regional Internet Conference on Operational Technologies
APRIGF	Asia Pacific Regional Internet Governance Forum
ARPANET	Advanced Research Projects Agency Network
ARR	Afghan Recovery Report
ASEF	Asia Europe Foundation
ASEM	Asia Europe Meeting
ASO	Address Supporting Organization
AU	African Union
BNNRC	Bangladesh NGOs Network for Radio & Communication
BTRC	Bangladesh Telecommunication Regulatory Commission
CAT	Cyber Appellate Tribunal
CCNSO	Country Code Name Supporting Organisation
CCPR	Human Rights Committee
ccTLD	country-code Top Level Domains
CCTV	Closed Circuit Television
CERD	Convention on the Elimination of All Forms of Racial Discrimination
CIPA	Children's Internet Protection Act
CIRP	Committee on Internet-related Policies
CISPA	Cyber Intelligence Sharing and Protection Act
CSR	Corporate Social Responsibility
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoC	Department of Commerce
DOI	Digital Opportunity Index
DPA	Data Protection Authority
DPAI	Data Protection Authority of India
DPI	Deep Packet Inspection
ECHR	European Convention of Human Rights
ECJ	Court of Justice of the European Union
ECtHR	European Court of Human Rights
EU	European Union
EuroDIG	European Dialogue on Internet Governance
FOSS	Free and Open Source Software
G8	Group of Eight
GA	General Assembly
GAC	Governmental Advisory Council
GATS	General Agreement on Trade in Services

GIS Watch	Global Information Society Watch
GNI	Global Network Initiative
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
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communication Technology
IDN	Internationalised Domain Name
IG	Internet Governance
IGC	Internet Governance Caucus
IGF	Internet Governance Forum
IPRs	Intellectual Property Rights
IRP	Internet Rights and Principles Coalition
IRT	International Telecommunication Regulations
IRU	International Radio-Telegraph Union
ISP	Internet Service Provider
ITU	International Telecommunications Union
IWPR	Institute for War and Peace Reporting
MAG	Multistakeholder Advisory Group
MNCs	multi-national corporations
MoU	Memorandum of Understanding
MPEPIL	Max Planck Encyclopedia of Public International Law
NGO	Non-Governmental Organisation
NHRCK	National Human Rights Commission of Korea
NTIA	National Telecommunications and Information Administration
NWICO	New World Information and Communication Order
OAS	Organization of American States
OECD	Organization for Economic Co-operation and Development
ONI	Open Net(work) Initiative
OSCE	Organization for Security and Co-operation in Europe
PIPA	Protect Intellectual Property Act
RFC	Request for Comments
RFID	Radio-Frequency Identification
RSF	Reporters San Frontiers
SAARC	South Asian Association for Regional Co-operation
SMS	Short Messaging Service
SOPA	Stop Online Piracy Act
TPP	Trans-Pacific Partnership Agreement
TRIPS	Trade-Related Aspects of Intellectual Property
UDHR	Universal Declaration of Human Rights
UN	United Nations
UN-CIRP	UN Committee for Internet Related Policies
UNCSTD	United Nations Committee on Science and Technology for Development
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organisation
UNHRC	United Nations Human Rights Committee
UPU	Universal Postal Union
VoIP	Voice over Internet Protocol
WCIT	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	World Summit on Information Society
WTO	World Trade Organization

Annex 2

Questions Raised by the Background Paper

These questions arise from the background paper's review of the relevant issues and supplement those already identified in the Seminar's concept paper.

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, e.g. 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 (e.g. ASEAN in Southeast Asia)?
17. How can regional Internet co-operation go beyond infrastructure (e.g. backbone network design) to cultural issues (e.g. 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 (e.g. 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 (e.g. freedom of the press)?
12. How can new forms of 'publishing' on the Internet such as microblogging (e.g. 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 1-4):

1. 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, i.e. telecom regulation, broadcast media regulation, print regulation?
6. What new commercial forces pose challenges to freedom of expression, e.g. 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?

2. 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?

3. Digital Divide and Sustainable Development

1. What divides are successive waves of digital media closing – and opening? E.g. 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? E.g. 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?

4. 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 of 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 of 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, e.g. via message greetings and proverbs in endangered languages?

Annex 3

Bibliography for the Background Paper

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 Johannen, 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

Jörgensen, Frank Rikke (2006). Human Rights in the Global Information Society, Cambridge, MA: MIT Press, http://mitpress.mit.edu/catalog/item/default.asp?ttype=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#axzz1l3bRZVGZ

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.rsf.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 Co-operation, 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/nZ0lk
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

Annex 4

Seminar Programme

12th Informal ASEM Seminar on Human Rights
"Human Rights and Information and Communication Technology"
27 - 29 June 2012
Seoul, Korea

Conference Venue: Plaza Hotel, Seoul

	Arrival of Participants, Registration and Welcome Reception
09:00 - 12:00	Side Event with Korean Civil Society '*Balancing Freedom of Expression and the Right to Privacy in an Informatization Society*' organised by the National Human Rights Commission of Korea
14:00 - 15:30	Rapporteurs and Moderators' meeting (invitation only) 14:00 – 16:00 Registration of participants
	Opening Plenary
16:00 - 16:30	**Chair** Ambassador Michel Filhol Executive Director, Asia-Europe Foundation **Opening Speech on behalf of the National Human Rights Commission of Korea** Mr Byung-Chul Hyun Chairperson, National Human Rights Commission of Korea **Opening Speech on behalf of the Host, Republic of Korea** H.E. Kim Sung-han Second Vice Minister, Ministry of Foreign Affairs and Trade **Opening Speech on behalf of the Organisers** Ambassador Rosario G. Manalo Foreign Affairs Adviser, Department of Foreign Affairs, Philippines
	Keynote Address
16:30 - 17:00	**Chair** Mr Rolf Ring Deputy Director, Raoul Wallenberg Institute **Keynote Speech** Ms Agnès Callamard Executive Director, ARTICLE 19 **Keynote Speech** Mr Pavan Duggal Advocate, Supreme Court of India and President Founder of Cyberlaw Asia
17:00 - 17:10	**Presentation of Outcomes from the Side Event with Korean Civil Society** Professor Ilhwan KIM Professor of School of Law, Sungkyunkwan Law School

Presentation of Background Paper by Main Rapporteurs	
17:10 - 18:10	Professor Wolfgang Benedek Professor of International Law, Faculty of Law, University of Graz Dr Madanmohan Rao Research Director at the Asian Media Information and Communication Centre Open Discussion
Reception and Dinner	
18:15 - 18:45	Welcome Reception hosted by National Human Rights Commission of Korea (NHRCK)
18:45 - 19:45	Welcome Dinner hosted by NHRCK
Simultaneous Working Groups	
09:00 - 11:00	**Working Group 1: Freedom of Expression** Moderator: Mr Rolf Ring Raoul Wallenberg Institute Rapporteur: Dr Madanmohan Rao Asian Media Information and Communication Centre **Working Group 2: The Right to Privacy** Moderator: Mr Al Alegre Foundation for Media Alternatives Rapporteur: Professor Wolfgang Benedek University of Graz **Working Group 3: The Digital Divide** Moderator: Mr Kavi Chongkittavorn Southeast Asian Press Association Rapporteur: Dr Dieter Zinnbauer Transparency International **Working Group 4: The Right to the Cultural Enjoyment of the Internet** Moderator: Mr Paul Keller Kennisland Rapporteur: Dr Delia Browne National Copyright Unit, Standing Council on School Education and Early Childhood
11:00 - 11:15	Coffee Break
11:15 - 13:00	Workshops continued
13:00 - 14:00	Lunch
14:00 - 15:30	Workshops continued
15:30 - 16:00	Coffee Break

16:00 - 18:00	Workshops continued and Wrap-up
18:00 - 19:30	Working Group debrief for Rapporteurs / Free Time for Participants
19:30 - 21:00	Dinner hosted by the Ministry of Foreign Affairs and Trade, Republic of Korea

Closing Plenary

09:30 - 11:20 **Rapporteurs' Summary on Each Workshop**

Moderator: Ms Sol Iglesias
Director, Intellectual Exchange, Asia-Europe Foundation

Working Group 1: Freedom of Expression
Presentation: Dr Madanmohan Rao

Working Group 2: The Right to Privacy
Presentation: Professor Wolfgang Benedek

Working Group 3: The Digital Divide
Presentation: Dr Dieter Zinnbauer

Working Group 4: The Right to the Cultural Enjoyment of the Internet
Presentation: Dr Delia Browne

Discussion

11:20 - 11:35 Coffee Break

11:35 - 13:00 **Special Plenary: Governance of the Internet**

Moderator: Ambassador Lionel Veer
Ambassador for Human Rights, Netherlands Ministry of Foreign Affairs

Panellists: Dr Madanmohan Rao
Research Director at the Asian Media Information and Communication Centre

Professor Wolfgang Benedek
Professor of International Law, Faculty of Law, University of Graz

Dr Dieter Zinnbauer
Senior Programme Manager, Transparency International

Dr Delia Browne
National Copyright Director, National Copyright Unit, Standing Council on School Education and Early Childhood

13:00 - 14:00 Lunch

14:00 - 16:00	**Special Panel: Data Protection Authorities and NHRIs - Their role and responsibilities to protect individual privacy** Chair: Professor Yi-Jong Suh Professor, Department of Sociology, Seoul National University Presentation: Dr Chang-Beom Yi Doctor of Law, Fmr. Vice-President of Korea Internet and Security Agency Discussants: Professor Inho Lee Professor, Law School, ChungAng University Mr Hakyung Jeong Standing Commissioner, Personal Information Protection Commission Mrs Sophie Kwasny Head of the Data Protection Unit, Council of Europe Mr Philippos Mitletton Vice President, European Association of Human Rights
16:00 - 16:30	Coffee Break
16:30 - 17:30	**Concluding Remarks from the Organisers** Ambassador Olof Ehrenkrona Political Ambassador/Senior Advisor to the Minister for Foreign Affairs – on behalf of the Raoul Wallenberg Institute Mr Frédéric Tiberghien Technical Coordinator & Representative of the Ministry of Foreign and European Affairs, France, & State Counsellor - Conseil d'Etat

Annex 5

Concept Note and Working Group Questions

Background

The information society and its impacts on human rights

Information and Communication Technologies (ICTs) can be defined as those technologies that facilitate by electronic means the creation, storage management and dissemination of information.[1] While the term 'Information Technology' was introduced in the 1970s, the digital technology revolution in the 1990s reintroduced the concept of ICTs in their application to socio-economic development.

"ICTs have nowadays an immense impact on virtually all aspects of our lives … The capacity of these technologies to reduce many traditional obstacles, especially those of time and distance, for the first time in history makes it possible to use the potential of these technologies for the benefit of millions of people in all corners of the world."[2]

However, the emergence of a global 'information society', driven by the continuing development of converging technologies of telecommunications, multimedia broadcasting and information technology, poses a number of challenges in terms of human rights protection.

First of all, modern technologies have had an unprecedented impact on a variety of civil and political rights. On one hand, they ease the implementation of freedom of information or of association; they improve transparency and access to information. On the other hand, owing to the certain restrictions that ICTs impose on certain individual rights, such as the right to privacy, they require new or enhanced measures in order effectively to secure these fundamental rights and protect them from government or private intrusion.

Secondly, given the importance that ICTs have acquired in today's world, access to these new digital media could be understood as forming essential social, economic and cultural rights. Nevertheless, a large portion of the world's population is still deprived of these modern technologies, separated by a growing 'digital divide' from people in industrialised countries. Of the 30% of the world's population that has access to the Internet, only seven out of ten people in the developed and two out of ten people in the developing world have internet access. Internet penetration rates by geographic region are at 58.3% for Europe, while Asia lags significantly behind with only 23.8%.[3]

The enhanced protection of cultural rights and liberties seems, however, warranted by the fact that the Internet has become one of the prime vehicles through which people express their cultural heritage. With regard to economic matters, the increased vulnerability of intellectual property rights raises questions as to whether new (international) instruments should be created adequately to protect these rights from infringements by state and non-state actors alike.

Thirdly, though the traditional concept of the nation-state guaranteeing minimum standards of human rights continues to apply, the international character of the environment created by the information society poses some considerable and practical problems for states trying to fulfil this role on their own. Indeed, the state infringing on an individual's fundamental rights may not necessarily be the same state in which the individual is a resident. Moreover, considering that rules have inherently a very hard time keeping pace with scientific or technological progress, one could ask what type of regulation, if any, is best suited to cope with the challenges created by the ever-accelerating development of ICTs. For the moment, international standards specifically adapted to the new environment created by the development of ICTs over the last two decades are, to a large extent, still lacking. A notable exception has been the Council of Europe's work across the region on tackling cybercrime through the Convention on Cybercrime and its Protocol on Xenophobia and Racism.[4]

In sum, while access to ICTs has improved in recent times, issues of equity, sustainability, and complexity remain unresolved. The 12th Informal ASEM Seminar on Human Rights will address some of these key issues and explore the opportunities for ASEM collaboration on ICTs and human rights.

---

[1] *Swiss Agency of Cooperation & Development, Information and Communications Technologies for Poverty Reduction: Discussion Paper, Swiss Agency of Cooperation & Development 2003.*

[2] *Declaration of Principles, World Summit on the Information Society, 12 December 2003, Document WSIS-03/GENEVA/DOC/4-E*

[3] *Internet World Stats, accessible at www.internetworldstats.com*

[4] *The Convention on Cybercrime which entered into force in 2004 is the first international treaty on criminal acts committed via the internet and other computer networks. Its attendant Protocol on Xenophobia and Racism, which entered into force in 2006, extends the Convention's scope to cover the dissemination of racist and xenophobic propaganda via the internet or other computer networks. More information can be found at http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp*

Global Milestones

The international community, in particular the United Nations (UN), has been supportive of the confluence of ICTs and development; when the Millennium Development Goals were adopted in 2000, one of the key questions was how ICTs could be best utilised for their achievement, especially when one of the goals was to 'promote access to the benefits of new technologies, particularly in the realm of information and communications'.[5]

Sponsored by the UN and the International Telecommunications Union, the first World Summit on the Information Society (WSIS) was held in 2003 in Geneva with the intention to establish political will and take steps towards creating a global Information Society, especially in relation to development. The resultant Geneva Plan of Action was picked up at the second phase of the WSIS in Tunis in 2005; the second summit worked to update and implement the Plan, through the Tunis Agenda for the Information Society.

While ICTs comprise of all types of communications technologies, current focus remains mainly on internet technology. The Tunis Agenda saw the development of a new 'multi-stakeholder policy dialogue' called the Internet Governance Forum (IGF). The IGF meets annually to discuss, amongst others, "public policy issues related to key elements of internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet."[6]

The Internet and Human Rights: Key Issues

The gap in social development is also reflected in the 'digital divide' whereby a large part of the developing world is unable to tap into the power of the Internet, that access to ICTs has indeed become a key issue. In a global public poll carried out by the BBC World Service in 2010, 87% of internet users felt that internet access should be a fundamental right, whereas 71% of non-internet users felt that they should have the right to access the web.[7]

Linking the Internet to human rights, the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, refers to the internet as "an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress"[8] and that "As such, facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States."[9]

This recent development prompts the question: should a set of new civil and political rights with respect to ICT be developed, or do the existing frameworks offer sufficient protection? This is especially important when 'Internet Access' by necessity includes issues such as freedom of expression and the right to privacy, yet must also consider the practical demands of the global fight against terrorism and transnational crime, as well as the protection of the rights of vulnerable groups such as women and children.

Another contentious area in an information society is the impact of ICTs on the protection and advancement of cultural rights. While international instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) protect the right to conserve and protect a community's culture, they also call for the right of everybody to enjoy the benefits from scientific progress – including benefits from advancements made in technology.

However, just like other aspects of globalisation, the use of ICTs has yielded both benefits in terms of connectedness and access to information, and detriments (in terms of marginalisation and exploitation of environmental resources[10] and communities). It has been difficult to regulate and reward intellectual property rights over traditional knowledge and practices once it enters the public domain. Moreover, the impact of ICT usage on indigenous traditions and customs also raises the issue of technological determinism – the influence and counter-influence of technology on societal attitudes, structures, community and culture.

Recognising the importance of cultural rights in its call for an Information Society, the Geneva Plan of Action stated that "Cultural and linguistic diversity, while stimulating respect for cultural identity, traditions and religions, is essential to the development of an Information Society based on the dialogue among cultures and regional and international cooperation. It is an important factor for sustainable development".[11]

The Way Forward

It has been universally acknowledged that all stakeholders in the Information Society – including governments, the public, civil society actors, the technological and private sectors – will need to engage in constructive dialogue

---

[5] *Target 8.F of the Millennium Development Goals, 2000*
[6] *The mandate of the IGF is found in Para 72 of the Tunis Agenda.*
[7] *BBC World Service, Internet Access is a Fundamental Right: Global Poll, 8 March 2010, accessed at http://news.bbc.co.uk/2/hi/8548190.stm*
[8] *LaRue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 10 June 2011*
[9] *Ibid.*
[10] *Such as the use of conflict minerals in the production of electronic gadgets including cell phones. For further reading please see Prendergast (2009), 'Can You Hear Congo Now? Cell Phones, Conflict Minerals and the Worst Sexual Violence in the World', EnoughProject April 2009*
[11] *C8, paragraph 23, Geneva Plan of Action, Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003,*

to ensure that ICTs can be included in the social and economic development of a nation. In its call for better internet governance, the Tunis Agenda defined this as "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".[12]

Cross-cutting Questions

1. What legitimate state interests and public policy concerns have emerged in the question of ICT regulation? What are the States' responsibilities and obligations to ensure protection of the public, particularly vis-à-vis private companies providing ICT services?
2. Is it the responsibility/obligation of governments to ensure the protection of the legitimate interests and public policy concerns in emerging ICT field? What are the advantages/disadvantages of a secured use of the Internet as opposed to zero regulation?
3. To what extent can the Internet be self-governed? How should internet governance be organised? What type of ICT regulation do states need? Does internet governance need international or national regulation?
4. To what extent and how do ICTs contribute to good governance and democratic processes?
5. Should a set of new civil and political rights with respect to ICT be developed, or are existing frameworks a sufficient protection? What about economic, social and cultural rights?
6. How can we address the social impact of the Internet vis-à-vis social rights?

Working Group Questions

Working Group 1: Freedom of Expression

1. How can ICT contribute to the full enjoyment of rights, particularly freedom of expression? How can this be balanced with such needs as protection against defamation or hate speech, crime prevention, protection of vulnerable groups (e.g. women and children, minority groups), and prevention of cybercrime and of terrorism?
2. Do existing frameworks provide for the right of association online? What about any protections to use ICT to organise social movements in the 'real' world?
3. How can dual concerns for and against the regulation of social networking sites like Facebook and Twitter be best addressed?
4. In what ways can ICT usage contribute to the implementation of rights such as freedom of information (FOI)? What experiences can be gained from the field of environment such as the Aarhus Convention[13] and emerging FOI legislation?
5. Have ICT tools contributed to the development of public participation in local or national democratic processes (e.g. referenda, public consultations or elections) or in environmental rights (Aarhus Convention) and of a better administration (nearer and quicker for any citizen), particularly at national and sub-national levels?
6. How can one reconcile the virtual and 'daily' democracy online with the real democracy where voters delegate the exercise of power to elected officials (with years between elections)?
7. How does ICT affect the traditional means of information dissemination, such as the print media? Does the emergence of 'citizen journalism' enrich public knowledge and discourse, or does it threaten the quality of information available?
8. The WikiLeaks cables in the past year have raised ethical and political concerns. In this regard, to what extent do private organisations such as access providers have a responsibility for hosting sensitive online content? What role does state regulation play? How has emerging jurisprudence helped to resolve these issues?

Working Group 2: The Right to Privacy

1. How does new technology intervene with the right to privacy (government and commercial databases, social databases, mobile and CCTV surveillance and tapping, as well as hacking and cyber-security)? What are the potential threats to human rights and how can they be mitigated?
2. What privacy protections should be introduced in individual profiling from data production and cross-usage of different databases, including official and social networks? What limits should be set for state agencies and private companies, particularly online social networks, alike?
3. What data is prima facie private and should therefore be protected? What regulatory framework would most effectively balance surveillance (data interception, wire-tapping, public CCTV video) for legitimate security and public policy concerns with the protection of individual rights?

---

[12] *Paragraph 72, Tunis Agenda for an Information Society*

[13] *This refers to the UN Economic Commission for Europe Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters. For more information see: http://live.unece.org/env/pp/welcome.html*

4. What are the different responsibilities of private companies (e.g. internet service providers, search engines) to both States and their users respectively, and how should competing interests be mediated?
5. How are vulnerable groups such as children and minors best protected within regulatory regimes that also protect online privacy?

Working Group 3: The 'Digital Divide'

1. Apart from the digital divides of 'north-south', 'rich-poor', 'educated-uneducated', 'rural-urban' populations, young digital 'natives' and elder digital 'migrants', what other groups are vulnerable to this divide (e.g. linguistic minorities, disabled people)? What is needed to overcome these divides and what public policies are in place to facilitate equal access to technology? In particular, for persons with disabilities, especially visual or hearing impairment, how can access be improved?
2. Do policies determining ICT infrastructure promote equal opportunity to access ICT? To what extent do governments impose conditions on private or public companies to promote equal access? Should States promote equal access through such measures as subsidies or direct provision of equipment?
3. What are the constraints against promoting equal access? What 'best' practices or experiences to promote better access can be shared?
4. How do disparities in ICT access have an impact on other rights, such as the right to education or access to information? Which rights are violated or potentially violated by lack of access?
5. Will promoting equal access to ICT eventually amount to 'free access'? Is access to ICT, particularly the Internet, a basic need and/or a human right?

Working Group 4: The Right to Cultural Enjoyment of the Internet

1. What is the cultural impact of ICT, particularly on access to culture and education, and on preservation or promotion of diversity or minorities rights in the face of globalisation? In particular, what is the impact of the Internet on linguistic diversity?
2. Does the Internet contribute to the enjoyment of cultural rights, access to culture and education, and preservation of minority cultures (including language)?
3. Should governments, as a form of special measures or affirmative action for the promotion and protection of minority and indigenous rights, provide technology and funding (but not editorial influence) for the ICT activities of minority and indigenous groups?
4. Is the right of cultural enjoyment of the Internet an emerging human right?
5. How can the right of cultural enjoyment and the legitimate protection of intellectual property rights be balanced?
6. Does promoting equal access to ICT amount to 'copytheft', or rather, copyright alternatives such as those espoused by Creative Commons or Open Source collaboration?
7. What are the human rights implications of anti-piracy measures such as the 'three strikes' laws, which prohibit internet access to repeat online piracy offenders for a certain period of time?

Annex 6

Participants

Australia	**Andrew Lowenthal** Executive Director, EngageMedia
	Anthony Skews Second Secretary, Australian Embassy Seoul
	Nigel Waters Policy Fellow, Privacy International
Austria	**Wolfgang Benedek** Professor of International Law, Faculty of Law, University of Graz
	Matthias Christoph Kettemann Research Fellow, Institute of International Law and International Relations, University of Graz
Belgium	**Jean-Philippe Moiny** Research Fellow F.R.S., CRIDS - Research Centre Information, Law and Society, University of Namur
	Mattias Van Hecke First Secretary – Deputy Head of Mission, Embassy of Belgium in Seoul
Brunei	**Saniah Haji Sani** Head of Human Resource / Senior System Analyst, E-Government National Centre, Prime Minister's Office
Bulgaria	**Jivka Marinova** Executive Director, Gender Education, Research and Technologies Foundation (GERT)
Cambodia	**Chealy Chet** Committee Member, Cambodia Human Rights Committee (CHRC)
	Chim Manavy Executive Director, Open Institute
China	**Shiqiu Chen** Head of the delegation, Ministry of Foreign Affairs, China
	Zhengrong Liu Director, Internet News Research Center
	Xiansheng Shi Vice Secretary General, Internet Society of China
Cyprus	**Philippos Mitletton** Vice-President, European Association of Human Rights (AEDH)
Czech Republic	**Jan Voboril** Law Expert, Iuridicum Remedium
Denmark	**Ashraf Mikhail** Project Manager, The Danish Institute for Human Rights

Estonia	**Eva-Maria Liimets** Director of Division of International Organisations, Ministry of Foreign Affairs, Estonia
	Ivar Tallo Member of the Executive Board, e-Governance Academy
Finland	**Satu Iivarinen-Roth** Embassy of Finland in Seoul
	Anita Kelles-Viitanen Chair, Asia Europe People's Forum (AEPF) Finland Chapter
France	**Agnes Callamard** Executive Director, ARTICLE 19
	Jacques Soulillou Chargé de mission, French Ministry of Foreign Affairs
Germany	**Daniel Domscheit-Berg** OpenLeaks
	Heike Jensen Researcher, Humboldt University
	Paul Keller Director, Kennisland
	Annette Knobloch First Secretary, Embassy of the Federal Republic of Germany in the Republic of Korea
	Dieter Zinnbauer Senior Programme Manager Emerging Issues, Transparency International
Hungary	**Zoltan Hernyes** Chief Counsellor, Ministry of Foreign Affairs of Hungary
	Ivan Szekely Counsellor, Open Society Archives at Central European University
India	**Pavan Duggal** Advocate, Supreme Court of India and President, Cyberlaw Asia
	Madanmohan Rao Research Advisor, Asian Media Information and Communication Centre
Indonesia	**Muhammad Anshor** Director for Human Rights and Humanitarian Affairs, Ministry of Foreign Affairs of the Republic of Indonesia
	Gustaff Harriman Iskandar Director, Common Room Networks Foundation
	Donny Utoyo Executive Director, ICT Watch
Ireland	**TJ McIntyre** Lecturer in Law, University College Dublin
	Ruth Parkin Deputy Head of Mission, Embassy of Ireland, Republic of Korea

Italy	**Giampiero Giacomello** Assistant Professor of International Relations, Department of Political & Social Sciences, University of Bologna
	Giuditta Giorgio First Secretary, Embassy of Italy
Japan	**Keisuke Kamimura** Executive Research Fellow, Center for Global Communications, International University of Japan
	Hiroshi Kawamura Board Member, DAISY Consortium
	Hideaki Ueda Ambassador in charge of Human Rights and Humanitarian Affairs, Ministry of Foreign Affairs, Japan
Korea	**Sang Jo Jong** Dean of the School of Law, Seoul National University
	Borami Kim Attorney at Lawyer (a Member of Korean Bar), Law firm Nanum
	Ilhwan Kim Professor of Law, School of Law, Sungkyunkwan University
	Yoojin Oh Deputy Director General, Human Rights Policy Division, Ministry of Justice
	Yi-Jong Suh Professor, Department of Sociology, Seoul National University
	Jong Soo Yoon Presiding Judge, Seoul Northern District Court
	Jeong A Yu Second Secretary, Human Rights and Social Affairs Division, Ministry of Foreign Affairs and Trade
Laos	**Khamphao Ernthavanh** Director General, Institute of Foreign Affairs, Ministry of Foreign Affairs
	Aksonsavanh Sihabandith Officer of International Human Rights and Humanitarian Treaties Division, Department of Treaties and Law, Ministry of Foreign Affairs
Lithuania	**Mindauga Kiskis** Professor, INVENT Institute / Mykolas Romeris University
Malaysia	**Sean Ang** Executive Director, Southeast Asian Centre for e-Media
	Siti Fatma Omar Assistant Secretary, Ministry of Foreign Affairs of Malaysia
	Sonia Randhawa Academic, Association for Progressive Communications
	Gayathry Venkiteswaran Executive Director, Southeast Asian Press Alliance (SEAPA)

Mongolia	**Nurgul Chaimardaan** Senior Researcher, Leading Researchers
Myanmar	**Myint Kyaw** Chief Editor, Yangon Press International
	Thein Oo President, Myanmar Computer Federation
Netherlands	**Walter van Holst** Senior Legal Consultant, Mitopics BV
	Lionel Veer Ambassador for Human Rights, Netherlands Ministry of Foreign Affairs
New Zealand	**Delia Browne** National Copyright Director, National Copyright Unit, Standing Council on School Education and Early Childhood
	Teanau Tuiono Maori Medium Publishing Coordinator, CORE Education
Pakistan	**Shahzad Ahmad** Country Director, Bytes for All, Pakistan
Philippines	**Al Alegre** Board Member, Foundation for Media Alternatives
	Benjamin Mora Officer-in-charge – Legal and Investigation Staff, Department of Science and Technology – Information and Communications Technology (DoST-ICTO)
	Ellen Tordesillas Journalist, VERA Files
Poland	**Aleksander Tarkowski** Director, Centrum Cyfrowe Projekt: Polska
	Jakub Wolasiewicz Director of Department for Proceedings Before International Organs of Human Rights Protection, Ministry of Foreign Affairs
Portugal	**Ademar Manuel Teixeira de Aguiar** Professor, Universidade do Porto – FEUP
Romania	**Bogdan Manolea** Executive Director, Association for Technology and Internet (ApTI - Romania)
	Anton Niculescu Special Representative on Human Rights, Ministry of Foreign Affairs
Russia	**Alexey Sidorenko** Director, Teplitsa of Social Technologies
Singapore	**Nur Syahidah Sahrom** Desk Officer, International Organisations Directorate, Ministry of Foreign Affairs
	Kum Hong Siew Vice President, MARUAH Singapore
	Harry Tan Director of CAPTEL (Centre for Asia Pacific Technology Law and Policy), Nanyang Technological University

Spain	**Juanjo Cordero** Secretary of the Board, Access Info Europe
Sweden	**Olof Ehrencrona** Ambassador/Senior Advisor to the Minister for Foreign Affairs, Ministry for Foreign Affairs
	Linda Sandberg Owner, Copylinda
Thailand	**Kavi Chongkittavorn** Chairperson, Southeast Asian Press Association
	Rataya Kobsirikarn Director, Human Rights Information Unit, Human Rights Promotion and Networking Coordination Bureau, Office of the National Human Rights Commission of Thailand (ONHRCT)
United Kingdom	**Andrew Puddephatt** Director, Global Dialogue
	Gavin Vessey Political Secretary, Foreign and Commonwealth Office, British Embassy Seoul
Vietnam	**Chu Thi Thuy Hang** Researcher and Lecturer, Vietnamese Institute for Human Rights
	Mai Phan Dung Deputy Director General, Department of International Organisations, Ministry of Foreign Affairs
European Union	**Rolf Timans** Head of Division Human Rights Policy Instruments, European External Action Service (EEAS)
International	**Sophie Kwasny** Head of the Data Protection Unit, Council of Europe

Observers	**Zhilun Yang** Member of the delegation, Ministry of Foreign Affairs, China
	Fabrice Leggeri First Counsellor and Deputy Head of Mission, Embassy of France in the Republic of Korea
	Frederik Janke Embassy of the Federal Republic of Germany Seoul
	George J. Geraldy ASEM Desk Indonesia, Directorate Intra-Regional Cooperation for America and Europe, Ministry Of Foreign Affairs of the Republic of Indonesia
	Atsushi Umino Director for International Policy Coordination, Ministry of Internal Affairs and Communications, Japan
	Namiko Yamashita Official, Human Rights and Humanitarian Affairs Division, Ministry of Foreign Affairs, Japan

	Xiao Ling Wu Policy Advisor, Asia and Oceania Department, Netherlands Ministry of Foreign Affairs
	Don Tan Intern, Singapore Embassy in Seoul
	Christine Lundberg First Secretary/Senior Programme Manager, Embassy of Sweden Bangkok/Sida
	Nguyen Thanh Son Director General, Permanent Office of Human Rights of Vietnam, Ministry of Foreign Affairs of Vietnam
	Le Thi Hong Tu Official, Department of Multilateral Economic Cooperation, Ministry of Foreign Affairs of Vietnam
	Ha Thi Thanh Huyen Desk Officer, Department of International Organisations, Ministry of Foreign Affairs of Vietnam

Organisers	**Michel Filhol** Executive Director, Asia-Europe Foundation
	Sol Iglesias Director, Intellectual Exchange, Asia-Europe Foundation
	Grace Foo Project Manager, Asia-Europe Foundation
	Ratna Mathai-Luke Project Officer, Asia-Europe Foundation
	Linyan Xue Executive Assistant to the Executive Director, Asia-Europe Foundation
	Frederic Tiberghien Coordinator & Representative of the Ministry of Foreign Affairs, France State Counselor (Conseil d'état)
	Rolf Ring Deputy Director, Raoul Wallenberg Institute
	Rosario Manalo Foreign Affairs Adviser, Department of Foreign Affairs, Philippines
	Luningning Camoying Acting Director / ASEM Contact Point, Department of Foreign Affairs, Philippines

Hosts – National Human Rights Commission of Korea	**Byung-Chul Hyun** Chairperson, National Human Rights Commission of Korea
	Younghye Kim Standing Commissioner, National Human Rights Commission of Korea
	Myungsook Jang Standing Commissioner, National Human Rights Commission of Korea
	Seokmo An Director General of Policy and Education Bureau, National Human Rights Commission of Korea
	Seokjun Ri Director of Human Rights Policy Division, National Human Rights Commission of Korea
	Yunkul Jung Chief of International Human Rights Team, National Human Rights Commission of Korea
	Balrae Lee Chief of Legislation and Policy Improving Team, National Human Rights Commission of Korea
	Seunggi Hong Human Rights Officer, National Human Rights Commission of Korea
	Mira Seo Human Rights Officer, National Human Rights Commission of Korea
	Seong-Hoon Park Human Rights Officer of the Legislation & Policy Improving Team, National Human Rights Commission of Korea
	Sook-Hyun Oh Editor/Interpreter of the International Human Rights Team, National Human Rights Commission of Korea
Ministry of Foreign Affairs and Trade, Republic of Korea	**Sung-Han Kim** Second Vice Minister, Ministry of Foreign Affairs and Trade
	Boram Kim Second Secretary of the Central European Department, Ministry of Foreign Affairs and Trade

Annex 7

About The Co-organisers

The Asia-Europe Foundation (ASEF)

The **Asia-Europe Foundation (ASEF)** promotes understanding, fosters relationships and facilitates cooperation among the people and institutions of Asia and Europe.

ASEF enhances dialogue, enables exchanges and encourages collaboration across the fields of governance, economy, sustainable development, public health, culture, and education.

Founded in 1997, ASEF is a not-for-profit, intergovernmental organisation located in Singapore. It is the only permanently established institution of the Asia-Europe Meeting (ASEM).

Together with about 700 partner organisations ASEF has run more than 600 projects, mainly conferences, seminars and workshops. Over 17,000 Asians and Europeans have participated in its activities and it has reached wider audiences through networks and web-portals, exhibitions and lectures.

For more information, please visit www.asef.org

Raoul Wallenberg Institute

The Raoul Wallenberg Institute of Human Rights and Humanitarian Law is an independent academic institution dedicated to the promotion of human rights through research, training and education. Established in 1984 at the Faculty of Law at Lund University, Sweden, the institute is currently involved in organising in Lund two Masters Programs and an interdisciplinary human rights programme at the undergraduate level. Host of one of the largest human rights libraries in the Nordic countries and engaged in various research and publication activities, the Raoul Wallenberg Institute provides researchers and students with a conducive study environment. The Institute maintains extensive relationships with academic human rights institutions worldwide. For more information, please visit our website: www.rwi.lu.se

French Ministry of Foreign and European Affairs

For more information, please visit our website: www.diplomatie.fr

Philippine Department of Foreign Affairs

The Department of Foreign Affairs is responsible for the coordination and execution of the foreign policies of the Republic of the Philippines and the conduct of its foreign relations and performs such other functions as may be assigned to it by law or by the President. For more information, please visit our website: www.dfa.gov.ph

Annex 8

About the Hosts

National Human Rights Commission of Korea

The National Human Rights Commission of Korea (NHRCK) is an independent government body established in 2001 to ensure protection of the inviolable and fundamental human rights of all individuals and promotion of the standards of human rights. The Commission also contributes to realization of human dignity and values, and safeguard of the basic order of democracy. http://www.humanrights.go.kr/english

---

The Ministry of Foreign Affairs and Trade, Republic of Korea

The Ministry of Foreign Affairs was inaugurated according to the Government Organization Act enacted by the Government of the Republic of Korea on July 17, 1948, to be in charge of diplomacy, external economic policy, overseas Korean nationals, international situation analysis and overseas promotional affairs.

After the Government of the Republic of Korea was founded on August 15, 1948, diplomatic relations were forged and overseas missions were established beginning with embassies or legations in friendly countries such as the United States of America, the United Kingdom and France along with representative missions in Japan and the United Nations.

On June 24, 1963, the Educational Institute of Foreign Service Officers (EIFSO) was established under Cabinet Order No. 1358 to be directly responsible to the Minister of Foreign Affairs. On January 5, 1965, EIFSO was reorganized as the Research Institute of Foreign Affairs (RIFA) under Presidential Decree No. 2030 as an educational institute for the improvement of the quality and efficiency of foreign service officers. On December 31, 1976, RIFA was reorganized as the Institute of Foreign Affairs and National Security (IFANS) under Presidential Decree No. 8377.

As a part of the government organizational reforms in 1998, the Ministry of Foreign Affairs was reorganized as the Ministry of Foreign Affairs and Trade with the incorporation of the newly established Office of the Minister for Trade, so as to comprehensively establish and conduct foreign policies on trade, trade negotiations and foreign economic affairs according to Presidential Decree No. 15710 of February 28 and Ministry of Foreign Affairs and Trade Decree No. 1 of March 3. In 2013, the Ministry was reorganized again as the Ministry of Foreign Affairs following the Park Geun-hye government's reorganization plan.

The Ministry of Foreign Affairs establishes and carries out foreign policies, economic diplomacy and economic cooperation, takes part in international economic communities, administers treaties and international agreements, protects and supports overseas Korean nationals, promotes cultural cooperation, and analyzes international affairs.

The Ministry of Foreign Affairs has continuously introduced complementary measures for effective diplomacy such as readjustment of manpower and budget befitting the changes in the diplomatic environment and the pursuit of substantial diplomacy to maximize the national interest of the ROK in the midst of a highly competitive international environment.

On the occasion of the first meeting of ASEM Foreign Ministers in February 1997 in Singapore, Sweden and France suggested that informal seminars on human rights be held within the ASEM framework. The aim of this initiative is to promote mutual understanding and co-operation between Europe and Asia in the area of political dialogue, particularly on human rights issues.

Previous seminar topics include:

- Access to Justice; Regional and National Particularities in the Administration of Justice; Monitoring the Administration of Justice (1997, Sweden)
- Differences in Asian and European Values; Rights to Education; Rights of Minorities (1999, China)
- Freedom of Expression and Right to Information; Humanitarian Intervention and the Sovereignty of States; Is there a Right to a Healthy Environment? (2000, France)
- Freedom of Conscience and Religion; Democratisation, Conflict Resolution and Human Rights; Rights and Obligations in the Promotion of Social Welfare (2001, Indonesia)
- Economic Relations; Rights of Multinational Companies and Foreign Direct Investments (2003, Sweden)
- International Migrations; Protection of Migrants, Migration Control and Management (2004, China)
- Human Rights and Ethnic, Linguistic and Religious Minorities (2006, Hungary)
- Human Rights and Freedom of Expression (2007, Cambodia)
- Human Rights in Criminal Justice Systems (2009, France)
- Human Rights and Gender Equality (2010, Philippines)
- National and Regional Human Rights Mechanisms (2011, Czech Republic)

The formula employed is as follows:

- Each ASEM partner nominates an official representative and the organisers invite two civil society participants from each of the Asian ASEM countries; and one from each of the European ASEM countries;
- An agenda structured around the main topics related to the subject of the seminar, with discussions held in working groups;
- Closed-door debates to allow free and direct exchanges of views; and
- A set of recommendations elaborated collectively to be sent to the relevant institutions in ASEM countries as informal contribution to the official Asia-Europe dialogue.

The Seminar series is co-organised by the Asia-Europe Foundation (ASEF), the Raoul Wallenberg Institute (delegated by the Swedish Ministry of Foreign Affairs), the French Ministry of Foreign and European Affairs and the Department of Foreign Affairs of the Philippines. ASEF has acted as the Secretariat of the Seminar since 2000.

Supervision of the seminar is entrusted to a Steering Committee, composed of the Seminar's four co-organisers and representatives of the Ministries of Foreign Affairs of China and Indonesia as well as the European Commission.

The Informal ASEM Seminar on Human Rights Series is a partnership between:

The 12th Informal ASEM Seminar on Human Rights was hosted by:

ISBN: 978-981-07-5715-1