SEMINAR REPORT

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.

Madanmohan Rao

Research advisor at the Asian Media Information and Communication Centre (AMIC) and Editor of The Asia-Pacific Internet Handbook; Bangalore, 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 organised by the Asia-Europe Foundation, Raoul Wallenberg Institute of Human Rights and Humanitarian Law, the French Ministry of Foreign and European Affairs, the Department of Foreign Affairs of the Philippines and the Korean Ministry of Foreign Affairs and Trade, 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 –

[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.

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 the organisers and the two main rapporteurs:

- Working Group 1: Freedom of Expression
- Working Group 2: Right to Privacy
- Working Group 3: Digital Divide
- Working Group 4: 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 working group topic was on the role of freedom of expression online. First, 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. The third topic addressed the most fundamental challenge to equitable and sustainable development in the age of the Internet: bridging the digital divide, and 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 also included a free press and broadcast media (with the rise of the mass media age). 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 online, there are differences in interpretation and application of this principle around the world. Many laws about expression are still linked to geography, for example, hate speech, 'taboo' topics, defamation, and child protection. An emerging challenge is the privatisation of censorship, where governments and private sector players (eg. social media sites) strike their own deals about what is permissible expression, without any public debate about 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 whether avatars or online 'gatherings' are a form of assembly. But it has been clearly proven that mobile social networking effectively enables 'smart swarms' and 'smartmobs,' i.e. the 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 registration duties are emerging, for example, for (i) Net/mobile connections, (ii) pre-paid SIM cards, (iii) online chats, (iv) cybercafes/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 (telecom/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, e.g. surveillance of women's use of mobile phones and the Internet by their spouse 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 (eg. social media). Governments have played a controlling role in each of these areas, as well as shared access in cybercafes and libraries (e.g. requirements to install filtering software).

Some Asian governments block access to certain Web sites 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 will not be affordable. Governments, device manufacturers and content providers are also becoming increasingly aware of usability issues, e.g. for differently abled citizens or 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-integrating with the workplace.

VII. Citizen Journalism

In numerous cases, citizen journalists have exposed the shortcomings of traditional media, for example, by exposing 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 such 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 the authorities.

X. How Governments are Promoting Freedom of Expression

Governments can support FoE 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 FoE and show their commitments to uphold 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 watchdog groups, such as Reporters Sans Frontiers, publish annual reports on incidents and legislations 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 the government and private sector in upholding FoE).

Vigilance

- All stakeholders need to be vigilant about infringements of rights and freedoms and need to keep up with the rapid pace of technology change and its benefits/abuses, (e.g. 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 (eg. citizen journalism).
- Self-regulation should be encouraged to 'shame' inappropriate behaviours online.
- More organisations, alliances and research programmes are needed to continuously monitor what governments and the private sector are doing in the area 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, member countries of 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 the progress made with regard to freedom of expression by governments and private sector players.

- For instance, ‘Friends of FoE’ awards can be given for countries and companies. Prizes should be given for progressive practices and policies in the areas of access to ICTs (e.g. making them affordable, increasing their reach, and increasing bandwidth).
- Recognition should be given to countries and companies that affirm Rights not just in 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: 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, ongoing discourses and regulatory challenges. Finally, the working group endorsed a set of conclusions and key messages which can be found at the end of the report.

II. Challenges to the Right to Privacy

ICTs have substantially enlarged both 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 working group 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 we insist on, and give up, privacy significantly affects the roles we play in society – as citizens, consumers, friends, family members, travellers, patients and partners.

The working 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 center 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 at the international, regional and national levels. They all regulate the collection, use and disclosure of information. Nevertheless, the working group pointed out that in some Asian countries, such as Japan and Malaysia, no legal definition of 'privacy' exists in the constitution nor 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 the 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 Harmonization 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 the 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 monetize 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 working 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, but this was considered imperfect, especially with regard to smaller companies without 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, Internet Service Provider 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 on 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 of 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 get access to remedies.

The working 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 both 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 the underdeveloped data sensibilities of Internet users, one sensible approach is to commit companies to ensure 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 (e.g. for the banking sector) are necessary. Where applicable, states are asked to speedily update their data protection laws. Finally, fifth, the international level – through (inter)-regional cooperation 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 the 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 working group expressed concern about the increasing commercialisation of the 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 Cooperation

The working group further highlighted the role of alliances and cooperation 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 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 right, 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 his/her own data and 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 violations of human rights and to provide data protection by public authorities, but also (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 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 multistakeholder-based approach to data protection and privacy regulation should be followed.

Need for Effective Remedies

- Effective remedies need to be provided at 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 does often conflict 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 like 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 Cooperation

- 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 cooperation needs to be strengthened between state and private actors from Asia and Europe at all levels.

D. Working Group 3: Digital Divide

I. Introduction: Effectively Tackling the Digital Divide

Working Group Three 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.

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.

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 /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 the ones that are not able to use the electronic service modality worse off than before.

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's 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 ICTs. 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/ community will be required to define its own priorities, mix of policy interventions, as well as their related sequencing for effectively bridging the divide. According to one view expressed in the debate, this may require to move at a more measured pace and help 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 strictly, 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 technical differences in perspectives.

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 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 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. And with regard to Internet users and citizens, helping to defend the human rights of internet activists (e.g. citizen journalists or whistle-blowers) 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. And it again featured prominently 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 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 provider do not discriminate against or unduly privilege specific contents but guarantee a fair level of visibility and accessibility of 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:

- 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, for example by providing tools for weaving lateral connections that cross organisational or social hierarchies, or by helping individuals to more fully explore and articulate their identities and 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

closing digital divides in a more systematic and sustainable fashion.

Based on this debate the challenge to close the digital divide could be re framed 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. And, 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 realising a wide range of fundamental rights.
- Increasingly interlinked and complementary ICTs require looking beyond the Internet alone and considering an entire suit 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 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 maximise 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, as well as spaces for experimentation.

- Governments need to ensure inclusive infrastructure build-out, competitive ICT markets, sound regulatory oversight, ICT skill development for all, as well as inclusive access to essential ICT facilities, services as well as to government accountability information.
- Business, 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: 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 *Open Group Discussion: Governance on 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 of 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 strong consensus that the right to cultural enjoyment of 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 to 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 (e.g Indonesia, Cambodia, 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 their (traditional) knowledge and culture;
- Access education (e.g. learning ICT skills in one's own language); and
- Participate in society (e.g. the right of freedom of expression, right to information, the freedom to hold opinions and to receive and impart information, the right to access 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 extent possible in the global digital world and 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 of 1987, and most government departments and agencies have bilingual names (English and Maori). This is a great example of how governments 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 strong consensus from the working 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 the localisation 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 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/taxpayer funds but is not accessible by the public. There is increasing demand for public cultural institutions to digitize and make their collections available online and for government to release public/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 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 encourages 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

(1) 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, Art 8j 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 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 eg. publishing a Maori person's genealogy ('whakapapa') online.

(2) 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, to stimulate wide dissemination of knowledge and culture.

Historically, the balance in IP is achieved through specific public interest limitations and exceptions set out in IP legislation (for example research and study, library archive and preservation of culture, education, reporting the news, government/public administration, criticism and review, parody and satire).

It is important to note that public interest limitations and exceptions is 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/services.

(3) 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 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, 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 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 futher enforcement and protection provisions in international trade treaties and relevant IP law.

(4) Piracy vs. the Right to Earn an Income

The participants discussed the issue of online piracy and the resulting loss of revenue and sales of copyright works. Generally, it was agreed that the creator has a right to be appropriately compensated for the 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 copyright 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 (eg: live performances, 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.

(5) 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 harbor 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, 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 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 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 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.

- 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, right to information, 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 four 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 (eg. 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 cooperation.

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 monetize 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 to 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, coordinating 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 fully incorporate 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 Agreement (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. a provision ensuring that any interference with human rights needs to be provided by law, pursues a legitimate purpose and be proportionate;
    b. a provision that allows cross border sharing of copyright works created under an exception for the visually impaired;
    c. a requirement for open-ended exceptions in copyright including anti-circumvention law;
    d. a requirement for safeguards on internet enforcement policies to avoid undue threats to freedom of expression and freedom of Information;
    e. 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, right to information, right to privacy – are positively affirmed in both domestic legislation and international agreements on intellectual property.