INFORMATION TECHNOLOGY: NO-FREE ZONE

Sujit Sinha Choudhury

Introduction

Whenever new communications and media platforms have been introduced, their innovation and application was met with scepticism, fear or outright banning by the ruling parties and authorities who feared the unknown medium, and its capacity to oust them from power. Therefore, new (mass) media historically face suspicion, and are liable to excessive regulation as they spark fear of potential detrimental effects on society, security and political power structures. This has proven true in the publication and transmission of certain types of content from the printing press through the advent of radio, television and satellite transmissions, as well as other forms of communication systems. During the 1990s, as attention turned to the Internet and as access to this borderless new communications platform increased, the widespread availability of various content, including sexually explicit content and other types of content deemed to be harmful for children, stirred up a 'moral panic' shared by many states and governments and certain civil-society representatives and concerned citizens.

Prior to the 1990s, information and content was predominantly within the strict boundaries and control of individual states, whether through paper-based publications, audio-visual transmissions limited to a particular area or even through public demonstrations and debates. Much of the media content made available and the discussions it triggered remained confined within territorially defined areas. Today, however, information and content, with its digital transmission and widespread availability through the Internet, do not necessarily respect national rules or territorial boundaries. This dissolution of the "sovereignty" of content control, coupled with the globalization of information, comes along with an increased multilingualism observable in many countries. The increasing popularity of user-driven interactive Web 2.0 applications and services such as YouTube, Facebook and Twitter seem to eliminate virtual Internet borders even further by creating a seamless global public sphere. This, inevitably complicates state-level efforts to find an appropriate balance between the universal right to freedom of opinion and

expression, which includes the right to receive and impart information, and the prohibition on certain types of content deemed illegal by nation-state authorities or intergovernmental organizations. With the widespread availability of the Internet and increasing number of users, online content regulation became an important focus of governments and supranational bodies across the globe.

Typically, the stance taken by many states is that what is illegal and punishable in an offline form must at least be treated equally online. There are, however, several features of the Internet which fundamentally affect approaches to its governance and while rules and boundaries still exist, enforcement of existing laws, rules and regulations to digital content becomes evidently complex and problematic. Despite the introduction of new laws or amendments to existing laws criminalizing publication or distribution of certain types of content, in almost all instances extraterritoriality remains a major problem when content hosted or distributed from outside the jurisdiction is deemed illegal in another.6 Therefore, the question of jurisdiction over content adds to the challenges faced by the governments and regulators. Which country's laws should apply for content providers or for Web 2.0 based platform providers? Should the providers be liable in the country where the content has been uploaded, viewed, or downloaded or where the server is placed or where the responsible providers reside? Many of these questions remain unanswered. Some countries fear the Internet could undermine their judicial sovereignty; others embrace the Internet and praise its global nature. However, the Internet certainly has created challenges for governments and these challenges are particularly visible when analyzing measures aimed at regulating online content.

Based on the limited effectiveness of state laws and lack of harmonization at international level (despite some efforts at regional level that will be addressed in this study) a number of states, including some in the OSCE region, introduced policies to block access to Internet content, websites deemed illegal and Web 2.0 based social media platforms which are outside their jurisdiction. The new trend in Internet regulation seems to entail blocking access to content if state authorities are not in a position to reach the perpetrators for prosecution or if their request for removal or take down of such content is rejected or ignored by foreign law enforcement authorities or hosting and content providers.

Furthermore, in certain countries, governments went further and developed measures which could restrict users' access to the Internet. This new blocking trend has been triggered in a number of countries as a result of increased piracy and intellectual property infringements on the Internet. These developments, as well as new policy trends in Internet content regulation, are detailed in this study.

While the intention of states to combat illegal activity over the Internet and to protect their citizens from harmful content is legitimate, there are also significant legal and policy developments which directly or indirectly and sometimes have an unintended negative impact on freedom of expression and the free flow of information. Recent laws and certain legal measures currently under development have provoked much controversy over the past few years.

A. Internet Access

The Internet is increasingly becoming indispensable for people to take part in cultural, social and political discourse and life. The number of Internet users is expected to more than double in 10 years and will reach five billion worldwide. While more than 60% of the citizens of the world are Internet users, only 30% of the nations stated that they recognize access to the Internet as a basic human right or as implied in the fundamental right to freedom of expression. At the same time, in more than 12% of the nations access to the Internet can legally be restricted, primarily to protect national security, public health or in times of state emergencies. As will be seen below, some states that do not have provisions on general access restrictions may nevertheless restrict users' access in certain cases, such as repeated copyright infringements or when criminal content, such as child pornography, is evident.

Everyone should have a right to participate in the information society and states have a responsibility to ensure citizens' access to the Internet is guaranteed. Furthermore, Internet access policies, defined by governments, should be in line with the requirements of Article 19 of the Universal Declaration of Human Rights as well as Article 19 of the International Covenant on Civil and Political Rights and (where applicable) with Article 10 of the European Convention on Human Rights. While certain countries and international organizations, such as the United Nations, may recognize Internet access as inherent to the right to free expression and as such to be a fundamental and universal human right, a number of governments are considering adopting content and access blocking measures. Countries such as Finland and Estonia already have ruled that access is a fundamental human

right for their citizens. According to a 2010 poll by the BBC World Service involving 27,000 adults across 26 countries, "almost four in five people around the world believe that access to the Internet is a fundamental right."

Asked **whether there are specific legal provisions on the right to access the Internet (Question 1)**, only 17 (30.3%) participating States confirmed that they have such provisions while 29 States (51.8%) stated that no such provisions exist. No data was obtained from 10 participating States (17.9%).

In some of the countries that responded positively, the right to access the Internet is interwoven with the right to information and communication, which is constitutionally protected in most cases. In some states, the right to access the Internet is guaranteed by specific laws, usually within telecommunication laws or regulations.

Asked whether **there are general legal provisions which could restrict users' access to the Internet (Question 2)**, 39 (69.6%) of the participating States stated "no", while only seven27 (12.5%) responded that they have general legal provisions which could restrict users' online access. No data was obtained from 10 (17.9%) of the participating States.

Asked whether **there are specific legal provisions guaranteeing or regulating "net neutrality" (Question 3)** in their jurisdiction, only **Finland** responded 'yes' (1.8%), while 45 States responded 'no' (80.4%). No data was obtained from 10 (17.9%) of the participating States. In **Finland**, since July 2010, subject to section 60(3) of the Communications Market Act,28 all Finnish citizens have a legal right to access a one megabit per second broadband connection, reportedly making Finland the first country to accord such a right.

Network neutrality is an important prerequisite for the Internet to be equally accessible and affordable to all. It is, therefore, troubling that more than 80% of the participating States do not have legal provisions in place to guarantee net neutrality. Finland and Norway stand out as best practice examples with Finland having anchored network neutrality in its corpus of laws while Norway, together with the industry and Internet consumers, developed workable guidelines. While it is commendable that several EU countries are planning to introduce rules on network neutrality by implementing the European Union's Telecoms Reform Package, participating States should consider legally strengthening users' rights to an open Internet. Users should have the greatest possible access to Internet-based content, applications or

services of their choice without the Internet traffic they use being managed, prioritized or discriminated against by the network operators.

B. Internet Content Regulation

Undoubtedly differences exist between approaches adopted to regulate content on the Internet. Content regarded as harmful or offensive does not always fall within the boundaries of illegality. Usually, the difference between illegal and harmful content is that the former is criminalized by national laws, while the latter is considered offensive, objectionable, or undesirable by some but is generally not considered criminal. While child pornography could be regarded as a clear example of content being criminalized in most, if not all the participating States, Internet content that is often labelled as "harmful" may include sexually explicit or graphically violent material. Strong or extreme political or religious views may also be regarded as harmful by states. Although this type of content falls short of the "illegality threshold", concern remains about possible access to this type of content by children. Highlighting this fundamental difference, in 1996 the European Commission stated:

> "These different categories of content pose radically different issues of principle, and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children".

More recently, the European Court of Human Rights argued that:

> "[…] the Internet is an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, […] is certainly higher than that posed by the press.

Policy and legal developments regarding the Internet in the OSCE region have shown that states differ in terms of categorizing or labelling certain types of content as illegal or "harmful". Harm is a criterion that depends upon various fundamental differences, which is recognized within the jurisprudence of the European Court of Human Rights. Such state-level differences undoubtedly complicate harmonization of laws and approaches at the international level.

Regarding speech- and content-related laws and legal measures, any restriction must meet the strict criteria under international and regional human rights law. According to the European Court of Human Rights jurisprudence, a strict three-part test is required for any content-based restriction. The Court notes that the first and most important requirement of Article 10 of the Convention is that any interference by a public authority with the exercise of the freedom of expression should be lawful. The second paragraph of Article 10 clearly stipulates that any restriction on expression must be "prescribed by law". If the interference is in accordance with law, the aim of the restriction should be legitimate – based on the Article 10(2) – and concern limitations in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals or for the protection of the rights and freedoms of others. Furthermore, any restrictions need to be necessary in a democratic society and the state interference should correspond to a "pressing social need". The state response and the limitations provided by law should be "proportionate to the legitimate aim pursued". Therefore, the necessity of the content-based restrictions must be convincingly established by the state. The Article 10 compatibility criteria as set out by the European Court of Human Rights should be taken into account while developing content related policies and legal measures by the participating States.

Asked whether **there are specific legal provisions outlawing racist content (or discourse), xenophobia and hate speech** in their jurisdiction **(Question 4)**, 45 (80.4%) of the participating States stated that there are such legal provisions in their country. The only country which responded negatively was **Kyrgyzstan**. No data was obtained from 10 (17.9%) of the participating States.

Asked whether **there are specific legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity** in their country **(Question 5),** 23 (41.1%) of participating States responded that they have such legal provisions in place. The same number of countries (23 - 41.1%) stated that they do not have such legal provisions, and 10 (17.9%) of the participating States did not provide a reply.

Asked whether **they have in place specific legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet (Question 6)**, 40 (71.4%) participating States responded positively, while only six (10.7%) stated that they do not have such legal provisions.39 No data was obtained from 10 (17.9%) of the participating States.

Asked whether **there are specific legal provisions criminalizing child pornography** in their country **(Question 7)**, the overwhelming majority of participating States (43 - 76.8%) stated that they have such laws in place. Only three (5.4%) (Azerbaijan,40 Kyrgyzstan,41 and Turkmenistan42) answered negatively. No data was obtained from 10 (17.9%) of the participating States.

Asked whether there are **specific legal provisions outlawing obscene and sexually explicit (pornographic) content** exist in their jurisdiction **(Question 8)**, 41 (73.2%) of participating States stated that they have such laws in place. In only five (8.9%) countries (Bosnia and Herzegovina, Croatia,43 Hungary, Liechtenstein, and Moldova) no such provisions exist. No data was obtained from 10 (17.9%) of the participating States.

Most legal provisions outlaw making available or showing obscene and sexually explicit (pornographic) content to children. In some states, the production, manufacture, dissemination or advertisement of pornographic content is criminalized per se. Sanctions vary from administrative fines to criminal sanctions. Possession of such content is generally not criminalized.

The participating States were further asked whether **there are specific legal provisions outlawing Internet piracy** in their country **(Question 9)**. 44 (78.6%) of the participating States confirmed the existence of such legal provisions. Only **Turkmenistan** stated that it

The responses received show that almost all participating States have general intellectual property laws that may be used to combat Internet piracy. Liability and sanctions may be provided in the form of administrative, civil and criminal liability. Graduated response mechanisms to limit users' access to the Internet for alleged copyright violations have been also developed in a few participating States.

Asked whether **they have specific legal provisions outlawing libel and insult (defamation) on the Internet (Question 10)**, 36 (64.3%) of the participating States responded with "yes", while eight states47 (14.3%) do not have criminal law provisions outlawing libel. However, although there are no criminal law provisions on libel and insult within these states, civil law provisions that could be applied to the Internet do exist. No data was obtained from 12 (21.4%) of the participating States.

In some participating States legal provisions on "extremism" or "extreme speech" exist. Asked whether **there are specific legal provisions outlawing the expression of views perceived to be encouraging extremism** in their

country **(Question 11)**, 20 (35.7%) of the participating States answered with "yes", 26 (46.4%) with "no", and no data was obtained from 10 (17.9%) participating States.

Asked whether **they have specific legal provisions outlawing the distribution of "harmful content" (i.e. content perceived to be "harmful" by law)** in place **(Question 12)**, 19 (33.9%) participating States responded that there are such laws in their jurisdiction. However, in 26 (46.5%) countries no such legal provisions exist. No data was obtained from 11 (19.6%) participating States.

Asked whether there are **specific legal provisions outlawing any other categories of Internet content (Question 13)**, 15 (26.8%) participating States responded positively, while so such legal provisions exist in 30 (53.6%) participating States. No data was obtained from 11 (19.6%) participating States.

Legal provisions that criminalize racism and hate speech, the denial, gross minimisation or justification of crimes against humanity, incitement to terrorism, child pornography, obscene and sexually explicit content, libel and insult, and the expression of views perceived to be encouraging extremism, exist in many participating States. A considerable number of legal provisions have been introduced and existing provisions have been amended within the past few years.

Most of the legal provisions criminalizing content are applicable to any medium and are not specific to the Internet. Therefore, legal measures and criminal sanctions can also be used to regulate online content and conduct. However, content regulation developed for traditional media cannot and should not simply be applied to the Internet. Recognizing this, some participating States have developed new legal provisions specifically designed for online content; often without recognizing that freedom of expression and freedom of information equally apply to the Internet. This increased legislation of online content has led to challenging restrictions on the free flow of information and the right to freely impart and receive information on and through the Internet.

Definitional problems and inconsistencies exist regarding certain speech-based restrictions. Clarifications are needed to specify what amounts for example to "extremism", "terrorist propaganda", "harmful" or "racist content", and "hate speech". As set forth in Article 19 of the Universal Declaration and in 10 of the European Convention on Human Rights, freedom of expression is subject to exceptions. These must be construed strictly, and the need for any restrictions

must be established convincingly by the states.48 Under the established principles of the European Court of Human Rights, citizens must be able to foresee the consequences which a given action may entail,49 and sufficient precision is needed to enable the citizens to regulate their conduct.50 At the same time, while certainty in the law is highly desirable, it may bring excessive rigidity as the law must be able to keep pace with changing circumstances. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree to the content in question, the field it is designed to cover and to the number and status of those to whom it is addressed.

Furthermore, a considerable number of participating States have yet to decriminalize defamation. Harsh prison sentences and severe financial penalties continue to exist in defamation suits. The European Court of Human Rights recalled in a number of its judgments that while the use of criminal law sanctions in defamation cases is not in itself disproportionate, the nature and severity of the penalties imposed are factors to be taken into account. Within this context, it is important to remember that the Council of Europe's Parliamentary Assembly urges those member states which still allow incarceration for defamation, even if they are not actually imposed, to abolish them without delay. Criminal defamation lawsuits continue to present a serious threat to and a chilling effect for media freedom in the OSCE region. In the Internet age, decriminalization of defamation becomes a prerequisite for free media to report without fear of criminal prosecution about issues of public importance – beyond national borders and jurisdictions. In countries where a free media scene is yet to be established, it is often foreign correspondents assuming the watchdog function. If, however, journalists face criminal charges for online publications outside their home countries, the freedom to report freely and unhindered will be severely hampered. Journalists might be subject to defamation charges in many countries where their stories have been read or downloaded.

The increased use of so-called "three-strikes" legal measures to combat Internet piracy is worrisome given the growing importance of the Internet in daily life. "Three-strikes" measures provide a "graduated response", resulting in restricting or cutting off the users' access to the Internet in cases where a user has attempted to download pirated material. The third strike usually leads to the user's access to the Internet being completely cut off. This disproportionate response is most likely to be incompatible with OSCE commitment on the "freedom to hold opinions and to receive and impart

information and ideas without interference by public authority and regardless of frontiers." In the Charter for European Security, the participating States in 1999 "reaffirmed the importance of independent media and the free flow of information as well s the public's access to information [and committed] to take all necessary steps to ensure the basic conditions for free and independent media and unimpeded trans-border and intra-State flow of information, which [they] consider the be an essential component of any democratic, free and open society." Any interference with such a fundamental human right, as with any other human right, must be motivated by a pressing social need, whose existence must be demonstrated by the OSCE participating States and must be proportionate to the legitimate aim pursued.59 Access to the Internet must be recognized as a human right, and therefore "graduated response" mechanisms which could restrict users' access to the Internet should be avoided by the OSCE participating States.

Finally, it should be noted that a considerable number of OSCE participating States did not provide statistical information on convictions under relevant law(s) pertaining to online content regulation. In the absence of reliable statistical data, or any data with regards to prosecutions and convictions involving the above mentioned content related legal provisions, it is not possible to reach conclusions on whether content related crimes were committed over the Internet. Participating States should therefore study the effectiveness of laws and other measures regulating Internet content, improve their data gathering and keeping and make such data publically available.

C. Blocking, Filtering, and Content Removal

Despite the introduction of new laws or amendments to existing laws, and the criminalization of the publication or distribution of certain types of content, in almost all instances extraterritoriality remains a major problem for Internet content regulation. Content is often hosted or distributed from outside the jurisdiction in which it is considered illegal. Laws are not necessarily harmonized at the OSCE level, let alone on a wider scale. What is considered illegal in one state may be perfectly legal in another. Different rules, laws and regulations exist based upon different cultural, moral, political, constitutional and religious values. These differences will continue to exist and undoubtedly complicate efforts to find an appropriate balance between the right to freedom of expression and the prohibition of certain types of content deemed to be illegal by state authorities.

Based on the limited effectiveness of state laws, and lack of harmonization at the international level a number of states have started to block access to websites and social media platforms that allegedly contain illegal content which are situated outside their legal jurisdiction. Blocking access to content seems to be faster, easier and a more convenient solution in cases where state authorities are unable to reach the perpetrators for prosecution, where mutual legal assistance agreements are not in place or where the request for removal of such content is rejected by hosting or content providers in the countries in which the allegedly illegal content is hosted.

However, as will be seen below, blocking measures are not always provided by law nor are they always subject to due process principles. Furthermore, blocking decisions are not necessarily taken by the courts of law and often administrative bodies or Internet hotlines run by the private sector single handedly decide which content, website or platform should be blocked. Blocking policies often lack transparency and administrative bodies (including hotlines) lack accountability. Appeal procedures are either not in place or where they are in place, they are often not efficient. Therefore, increasingly, the compatibility of blocking with the fundamental right of freedom of expression must be questioned.

Asked about **specific legal provisions which require closing down and/or blocking access to websites or any other types of Internet content (Question 14)**, 28 (50%) of the participating States stated that no such legal provisions exist while 17 (30.4%) of the participating States do have laws in place which could be used to block access to websites. No data was obtained from 11 (19.6%) of the participating States.

The participating States were also asked whether they have **specific legal provisions which require blocking access to web 2.0 based applications and services such as YouTube, Facebook, or Blogger** in place **(Question 15)**. Only **Italy** responded positively to this question. 44 (78.6%) states responded negatively and **Albania**, **Azerbaijan**, **Belarus**, **Kazakhstan**, **Kyrgyzstan**, **Latvia**, **Lithuania**, **Norway**, and **Poland** explicitly stated that there are no specific provisions which require blocking access to Web 2.0 based applications and services. No data was obtained from 11 (19.6%) of the participating States.

Based on the responses received, there were no general legal provisions involving blocking in 10 participating States. These are **Austria**, **the Czech Republic**, **Germany**, **Luxembourg**, **the former Yugoslav Republic of**

Macedonia, **Moldova**, **Montenegro**, **Poland**, **Serbia** and **Slovakia**. However, there may be some removal provisions or other sanctions provided for in those countries. Furthermore, some participating States have **specific legal provisions** in the absence of **general legal provisions** which require closing down and/or blocking access to websites regarding individuals.

Several international organizations have recognized the need to protect children from harmful content. The European Commission developed an Action Plan on safer use of the Internet, the Council of Europe Parliamentary Assembly recommended that the needs and concerns of children online be addressed without undermining the benefits and opportunities offered to them on the Internet and the Committee of Ministers also recommended that safe and secure spaces similar to walled gardens should be developed for children on the Internet. In doing so the Committee of Ministers noted that "every action to restrict access to content is potentially in conflict with the right to freedom of expression and information as enshrined in Article 10 of the European Convention on Human Rights." The need to protect children from harmful content was highlighted and the development of a pan-European trustmark and labelling system was encouraged. However, the CoE Committee decided not to recommend state-level blocking or filtering mechanisms for the protection of children but allowed for exceptions for the protection of minors and member states can consider the installation and use of filters in places accessible to children such as schools or libraries. The need to limit children's access to certain specific types of Internet content deemed harmful should not also result in blocking adults' access to the same content.

Asked whether **specific legal provisions requiring schools, libraries and Internet cafes to use filtering and blocking systems and software (Question 18)** exist in their countries, 38 (67.9%) participating States responded with "no" while legal provisions do exist in 6 (10.7%) states.64 No data was obtained from 12 (21.4%) of the participating States.

The assessment of blocking, filtering and content-removal provisions and policies revealed that the total suspension of communications services, including Internet access related services, is possible in some participating States in times of war, states of emergency, as well as imminent threats to national security. Although there is no so-called 'Internet kill switch' mechanisms in those countries, legal provisions may allow the authorities to switch off completely all forms of communications, including Internet communications, under certain circumstances. An 'Internet kill switch' idea

was considered by the **United States** where it was envisaged that the President can authorize the shutdown of critical computer systems in the event of a national cyber emergency, U.S. Senate did not act on the proposed measure.

In several participating States the legal remedy provided for allegedly illegal content is removal or deletion; other participating States provide access-blocking measures in addition to the removal measures. In some participating States such as in **Belarus** and the **Russian Federation** "prohibited information lists" maintained by government authorities exist. Access may be blocked if "prohibited information" appears on the Internet. Some countries also started to develop country-level, domain-name blocking or seizure policies (the **Czech Republic, Moldova**, **Switzerland**, and the **United Kingdom**).

Turkey provides the broadest legal measures for blocking access to websites by specifying eleven different content-related crimes, but does not reveal the number of websites blocked under the law.

Legal provisions for blocking access to child pornography exist in **Bulgaria**, **Finland**, **Italy, Liechtenstein, Romania, Turkey**, and **Ukraine**. At EU level, 'mandatory blocking' of websites containing child pornography was not recommended but the member states "may take the necessary measures in accordance with national legislation to prevent access to such content in their territory".66 However, in a number of countries, so-called 'voluntary blocking measures' to block access to known child pornography websites exist. **Canada**, **Denmark**, **France**, **Finland**, **Netherlands**, **Norway**, **Sweden**, **Switzerland** and the **United Kingdom** are among the participating States where such voluntary arrangements exist. While **Canada** and the **United Kingdom** rely on the British Telecom-developed Cleanfeed system for ISP-level blocking, other ISP-level blocking systems are used in other participating States where voluntary blocking measures exist. In almost all instances, blocking lists and blocking criteria are not made public. Only in **Italy** the blacklist for blocking access to international or unlicensed gambling websites is transparently made available.

There is concern that voluntary blocking mechanisms and agreements do not respect due process principles within the states in which they are used. In the absence of a legal basis for blocking access to websites, platforms and Internet content, the compatibility of such agreements and systems with OSCE commitments, Article 19 of the Universal Declaration, Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights is arguably problematic. Although the

authorities' good intentions to combat child pornography and other types of illegal content is legitimate, in the absence of a valid legal basis in domestic law for blocking access to websites, the authority or power given to certain organizations and institutions to block, administer and maintain the blacklists remains problematic. Such a 'voluntary interference' might be contradictory to the conclusions of the Final Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE and in breach of Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights unless the necessity for interference is convincingly established.68 Both, the 1994 Budapest OSCE Summit Document and the European Court of Human Rights reiterated the importance of freedom of expression as one of the preconditions for a functioning democracy. In Budapest "The participating States reaffirm that freedom of expression is a fundamental human right and a basic component of a democratic society. In this respect, independent and pluralistic media are essential to a free and open society and accountable systems of government." Genuine, 'effective' exercise of this freedom does not depend merely on the state's duty not to interfere, but may require positive measures to protect this fundamental freedom. Therefore, a blocking system based exclusively on self-regulation or 'voluntary agreements' risks being a non-legitimate interference with fundamental rights.

Independent courts of law are the guarantors of justice and have a fundamental role to play in a state governed by the rule of law. In the absence of a valid legal basis, the issuing of blocking orders and decisions by public or private institutions other than independent courts of law is, therefore, inherently problematic from a human rights perspective. Even provided that a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued. Within this context, it is submitted that the domain-based blocking of websites and platforms carrying legal content such as YouTube, Facebook, Wordpress and Twitter could be incompatible with OSCE commitments, namely the conclusions of the Final Act of Copenhagen and the conclusions of the Final Document of the Moscow Meeting as well as with Article 10 of the European Convention on Human Rights, and regarded as a serious infringement on freedom of speech. Such a disproportionate measure would be more far reaching than reasonably necessary in a democratic society.

The Internet started to play an essential role as a medium for mass communication, especially through the development of Web 2.0 based platforms, enabling citizens to actively participate in the political debate and

discourse. These platforms provide a venue popular across the world for alternative and dissenting views. Therefore, banning access to entire social media platforms carries very strong implications for political and social expression.

State-level blocking policies undoubtedly have a serious impact on freedom of expression, which is one of the founding principles of democracy. Blocking orders that are issued and enforced indefinitely on websites could result in 'prior restraint'. Although the European Court of Human Rights does not prohibit prior restraint on publications, the dangers inherent in prior restraint are such that it calls for the most careful scrutiny on the part of the court. This is particularly valid for the press as news is a perishable commodity and delaying its publication, even for a short period, may well deprive it of all its value and interest. The same principles also apply to new media and Internet publications. Prior restraint and other bans imposed on the future publication of entire newspapers or, for that matter, websites and Internet content are incompatible with the rights stipulated in the European Convention on Human Rights. The Strasbourg Court requires the consideration of less draconian measures such as the confiscation of particular issues of publications, including newspapers or restrictions on the publication of specific articles. Arguably, the practice of banning access to entire websites, and the future publication of articles thereof (whose content is unknown at the time of access blocking) goes beyond "any notion of 'necessary' restraint in a democratic society and, instead, amounts to censorship".

It is worth noting that litigation in **Belgium** triggered an application to the European Court of Justice regarding ISP-level blocking and filtering of websites containing copyright infringement. Advocate General Cruz Villalón of the Court of Justice of the European Union indicated that a measure ordering an ISP to install a system for filtering and blocking electronic communications in order to protect intellectual property rights in principle infringes on fundamental human rights. The decision of the European Court of Justice will shed further light into blocking measures and their implications for fundamental human rights. Similarly, the European Court of Human Rights is currently considering two applications (regarding the blocking of Google sites and Last.fm) from **Turkey**. Both of these applications involve blocking measures. The European Court of Human Rights, therefore, may establish principles with regards to Internet and freedom of expression, and may comment on the issue of blocking access to websites. A decision surrounding

these issues will certainly have broader implications for the Council of Europe member states.

On issues related to search engine providers, the CoE Committee of Experts on New Media published a draft "Guidelines for Search Engine Providers" during 2010. The Committee stated that "search engine providers must promote transparency about systematic nationwide blocking or filtering about certain types of content and adhere to the principle of due process when removing specific search results from their index and provide access to redress mechanisms" regardless whether the origin of removal requests is governmental, co-regulatory or private.

Filtering software is mostly used in schools, libraries and Internet cafes within the OSCE region. In most cases, there are no legal requirements for their use but the laws of some participating States, such as **Belarus**, **Croatia**, **Lithuania**, **Poland** and **Turkey,** require filtering software to be used in academic institutions, libraries and Internet cafes. In other states, such as **Canada**, **the Czech Republic**, **Hungary** and **Norway,** the use of filters is voluntary and not subject to any laws or legal provisions. The International Federation of Library Associations and Institutions, in conclusion to its 2010 annual report, warned that "filtering could, however, very easily develop into general Internet censorship and any developments should be carefully monitored by library communities and other interested parties, so as to ensure that legitimate information needs of the general public can be satisfied. Finally, 'upstream filtering' of the Internet is a matter of serious concern." Here it should be noted that **Turkey** decided to introduce a country-wide mandatory filtering system that was supposed to go into effect in August 2011. If realized, this would have been the first government controlled and maintained mandatory filtering system within the OSCE region. However, subsequent to strong criticism, Turkish authorities decided to modify their decision.

D. Licensing and Liability related issues and Hotlines to report Illegal Content

The final part of this study analyzes licensing and legal liability provisions related to information society service providers including access, content, platform, and search engine providers. Regarding liability for carrying third party content, in most instances liability will only be imposed upon information society service providers (including ISPs, hosting companies, Web 2.0 based social media platforms, and search engines) if there is "**knowledge and control**" over the information which is transmitted or stored by a service

provider. Based on the "knowledge and control theory" notice-based liability and takedown procedures have been developed in Europe. For example, the EU Directive on Electronic Commerce provides a limited and notice-based liability with takedown procedures for illegal content. The EU Directive suggests that "it is in the interest of all parties involved in the provision of information society services to adopt and implement procedures" to remove and disable access to illegal information. Therefore, the service providers based in the European Union are not immune from prosecution and liability, and they are required to act expeditiously "upon obtaining actual knowledge" of illegal activity or content, and "remove or disable access to the information concerned". Such removal or disabling of access "has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level".

A European Commission analysis of practice on notice and take-down procedures published in 2003 claimed that "though a consensus is still some way off, agreement would appear to have been reached among stake holders in regards to the essential elements which should be taken into consideration". A further review was subsequently commissioned in 2007, and the study disclosed all but harmonized implementation policies because "the manner in which courts and legal practitioners interpret the E-Commerce-Directive in the EU's various national jurisdictions reveals a complex tapestry of implementation." Some further studies showed that ISPs based in Europe tend to remove and take-down content without challenging the notices they receive. In 2010, the European Commission announced it had found that the interpretation of the provisions on liability of intermediaries is frequently considered necessary in order to solve problems and subsequently launched a consultation.

In addition to notice-based liability systems, hotlines to which allegedly illegal Internet content can be reported to have been developed in Europe and extended to other regions, too. The majority of the existing hotlines try to tackle the problem of child pornography and most of the hotlines based in the European Union are co-financed by the EU Safer Internet Action Plan. However, according to a Euro Barometer Survey of 2008, reporting to the hotlines seems to be low and users seem to prefer to report illegal content they come across to the police rather than to hotlines. The survey results seem to indicate a rather low public awareness of the existence and purpose of these hotlines.

Regarding the formation of public or private hotlines, it should be noted that although hotlines could potentially play an important role in relation to illegal Internet content, there remain significant questions about their operation. Private hotlines are often criticized as there remain serious concerns regarding the "policing" role they might play. It is argued that decisions involving illegality should remain a matter for the courts of law to ensure due process, rather than left to hotlines operating outside a legal framework. This concern was recognized in the Martabit Report to the UN which stated that "while encouraging these initiatives, States should ensure that the due process of law is respected and effective remedies remain available in relation to measures enforced". The operation of private hotlines formed through self-regulatory means should be consistent with the principles underlying the European Convention on Human Rights. States may have a positive obligation to guarantee that hotlines respect due process principles, and their functions and practice do not contravene the principles underlying the European Convention.96 States must furthermore provide adequate and effective safeguards against abuse. These should include procedures for effective judicial scrutiny of the decisions taken by the hotlines.

Furthermore, the lack of transparency regarding the work of hotlines often attracts accusations of censorship. Leaked 'child pornography' blacklists maintained by hotlines in Finland, Denmark, and Italy (as well as from China, Thailand, Australia,) that were published on the whistleblower website Wikileaks have demonstrated that most of the hotlines also block access to adult pornographic content and even political content. In the absence of openness and transparency of the work of hotlines and by creating secrecy surrounding the blocking criteria and keeping the list of blocked websites confidential, concerns will continue to exist.

E. Results and Recommendations:

a) **Open and Global Nature of the Internet should be ensured:** Nations need to take action to ensure that the Internet remains as an open and public forum for freedom of opinion and expression, as guaranteed by OSCE commitments, enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights. All nations of the World should keep in mind the borderless nature of the Internet when developing online content regulation policies. The preservation of the global nature of the Internet requires nations a regional and alternative approach to online content regulation.

b) **Access to the Internet should be regarded as a human right and recognized as implicit to the right to free expression and free information:** Access to the Internet remains the most important prerequisite to be part of and take part in Information Society. Access to the Internet is one of the basic prerequisites to the right to freedom of expression and the right to impart and receive information regardless of frontiers. As such, access to the internet should be recognized as a fundamental human right.

c) **The right to freedom of expression is universal – also in regard to the medium and technology:** The right to freedom of expression and freedom of the media were not designed to fit a particular medium, technology or platform. Freedom of expression applies to all means of communications, including the internet. Restriction to the right is not acceptable if in compliance with international norms and standard. Any restriction should be against the public interest.

d) **New technologies require new approaches:** Typically, the stance taken by the participating States is that what is illegal and punishable in an offline form must at least be treated equally online. There are, however, several features of the Internet which fundamentally affect approaches to its governance. While rules and boundaries still exist, enforcement of existing laws, rules and regulations to digital content becomes evidently complex, problematic and at times impossible to enforce on the Internet. Participating States should develop alternative approaches adapted to the specific nature of the internet. nParticipatNNations should also place more emphasis and interest on media literacy projects for vulnerable groups, particularly children.

e) **Network neutrality should be respected** Legal or technical measures regarding end-users' access to or use of services and applications through the Internet should respect the fundamental rights and freedoms guaranteed by international human rights principles, especially freedom of expression and the free flow of formation. Online information and traffic should be treated equally regardless of the device, content, author, origin or destination. Service providers should make their information management practices of online data transparent and accessible. Furthermore, information society service provisiones should not subject to govt. barriers and strict licensing regimes.

f) **Internet 'kill switch' plans should be avoided:** Existent legal provisions allow several participating States to completely suspend all Internet communication and 'switch off' Internet access for whole populations or segments of the public during times of war, states of emergency and in cases of imminent threat to national security. Reaffirming the importance of fully respecting the right to freedom of opinion and expression, the nations should refrain from developing, introducing and applying "internet kill switch" plans as they are incompatible with the fundamental right to information.

g) **Nations should avoid vague legal terminology in speech-based restrictions** Definitional problems and inconsistencies exist with regard to certain speech-based restrictions. Clarifications are needed to define what amounts to 'extremism', 'terrorist propaganda', 'harmful' and 'racist content' and 'hate speech'. Legal provisions are often vague and open to wide or subjective interpretation. Any restriction must meet the strict riteria under international and regional human rights law. The necessity for restricting the right to speak and receive information must be convincingly established to be compatible with international human rights standards.

h) **Nations should refrain from mandatory blocking of content or websites:** Given the limited effectiveness of national laws and the lack of harmonization at the international level to prosecute criminal online content, a number of OSCE participating States started to block access to online content deemed illegal and Web 2.0 based social media platforms outside of their jurisdiction. Since blocking mechanisms are not immune from significant deficiencies, they may result in the blocking of access to legitimate sites and content. Further, blocking is an extreme measure and has a very strong impact on freedom of expression and the free flow of information. Participating States should therefore refrain from using blocking as a permanent solution or as a means of punishment. Indefinite blocking of access to websites and Internet content could result to 'prior restrain' and by suspending access to websites indefinitely states can largely overstep the narrow margin of appreciation afforded to them by international norms and standards. Blocking of online content can only be justified if in accordance with these standards and done pursuant to court order and where absolutely necessary. Blocking criteria should always be made public and provide for legal redress.

i) **Voluntary blocking and content removal arrangements should be transparent and open to appeal:** Voluntary blocking measures and agreements exist in a number of participating States. However, private hotlines do not always have legal authority to require ISPs to block access to websites or to require removal of content. Any blocking system based exclusively on self-regulation or voluntary agreements between state actors and private actors have to be conceived in a way as not to interfere with fundamental rights. Furthermore, blocking criteria of hotlines and private actors are not always transparent or open to appeal. Any blocking or removal system based on self-regulation and voluntary agreements should be transparent, compatible with international norms and standards and provide for redress mechanisms and judicial remedies.

j) **Filtering should only be encouraged as an end-user voluntary measure:** Nations should encourage the use of end-user filtering software on individual home computers and in schools if their use is deemed necessary. However, the deployment of state-level upstream filtering systems, as well as government-mandated ltering systems, should be avoided. If the use of filters is encouraged by the states, users should be made aware of potential limitations of filtering software as there are serious questions about the reliability of such tools as stand-alone solutions for child protection.

k) **'Three-strikes' measures to protect copyright are incompatible with the right to information** The development of so-called 'three-strikes' legal measures to combat Internet piracy in a number of participating States is worrisome. While countries have a legitimate interest to combat piracy, restricting or cutting off users' access to the Internet is a disproportionate response which is incompatible with commitments on the freedom to seek, receive and impart information, a right which in fact should be strengthened by the Internet. Participating States should refrain from developing or adopting legal measures which could result restricting citizens' access to the internet. A discussion on whether or not current international standards on intellectual property protection are suited for our information society might be necessary.

l) **Reliable information on applicable legislation and blocking statistics needs to be made available:** Despite the high responsiveness of the participating States to take part in the survey, many governments expressed major difficulties in collecting the requested data because

reliable or recorded information was not available or different governmental institutions and ministries are responsible for the different aspects of the Internet. Almost no participating State had an institutional focal point on Internet matters to rely on. It is recommended that participating States put mechanisms in place that allow for the maintenance of reliable information on internet content regulation and statistical data pertaining to questions of blocking statistics and prosecutions for speech-related offenses committed on the Internet. These statistics and information should be made available to the public.

F. Conclusion:

Computers and Information Technology are now the most essential part and parcel of everyone's life. As 'life' is to 'air', 'live' is to 'information technology'. For a prolonged use of computers and information technology for over more than two decades, it is high time we look back at our foot steps review our objectives. Development of this aspect is still on without the scope of getting an interval time for sitting back and looking back.

Information is now available on the net. But is such information viewable or downloadable? In most important cases, the answer is NO. Information has been monopolized by respective skillful companies. Those who have huge purchasing power or is somewhat bound to seek information buys the same from such companies, who earn immoral huge money in the process. Moreover, if somebody, like Assange, feels like revealing information get punished on doing so.

Has democracy increased with the development of information technology is really a big question. Public opinions must be formed against such commoditization and immoral monopolization of information.