Study

Internet blocking

balancing cybercrime responses in democratic societies
(Executive Summary)

Prepared by

Cormac Callanan (Ireland)
Marco Gercke (Germany)
Estelle De Marco (France)
Hein Dries-Ziekenheiner (Netherlands)

This report has been prepared within the framework of Open Society Institute funding.

The views expressed in this document do not necessarily reflect those of the Open Society Institute.

Contact

For further information please contact:

Mr. Cormac Callanan

Tel: +353 87 257 7791
Email: cormac.callanan_at_aconite_dot_ie

Mr. Marco Gercke

Tel: +49 221 2707205
Email: gercke_at_cybercrime_dot_de

Ms. Estelle De Marco

Tel: +33 4 90 84 16 70
Email: estelle.de.marco_at_inthemis_dot_fr

Mr. Hein Dries-Ziekenheiner
Tel: +31 71 711 3243
Email: hein_at_vigilo_dot_nl

The views expressed in this document do not necessarily reflect those of the Open Society Institute.

The Authors

CORMAC CALLANAN IRELAND

Cormac Callanan is director of Aconite Internet Solutions (www.aconite.com) which provides expertise in policy development in the area of cybercrime and Internet security & safety.

Holding an MSc in Computer Science, he has over 25 years working experience on international computer networks and 10 years experience in the area of cybercrime. He has provided training at Interpol and Europol and to law enforcement agencies around the world. He currently provides consultancy services around the world and worked on policy development with the Council of Europe and the UNODC.

In 2008, in conjunction with co-author Marco Gercke, he completed a study of best practice guidelines for the cooperation between service providers and law enforcement against cybercrime (www.coe.int/cybercrime) adopted at the 2008 Octopus Conference. In 2009, in conjunction with Nigel Jones he produced the 2Centre (Cybercrime Centres of Excellence Network for Training Research and Education) study profiling international best practice for IT forensics training to Law Enforcement (www.2centre.eu).

Cormac was past-president and CEO of INHOPE – the International Association of Internet Hotlines (www.inhope.org). INHOPE facilitates and co-ordinates the work of Internet hotlines responding to illegal use and content on the Internet. He co-authored the INHOPE first Global Internet Trend report in 2007 which was a landmark publication on Internet child pornography.

Cormac was founding Chairman of the Internet Service Provider Association of Ireland (www.ispai.ie) in 1997 which he led for 5 years until February 2003 and served as Secretary General of the European Service Provider Association (www.euroispa.org). He was founding Director of the Irish www.hotline.ie service in 1998 responding to reports about illegal child pornography and hate speech on the Internet. He wrote the Code of Conduct for the ISPAI.

Cormac established the first commercial Internet Services Provider business in Ireland in 1991 - EUnet Ireland – which was sold in 1996. He is a board member of the Copyright Association of Ireland (www.cai.ie). He served on the Rightswatch (www.rightswatch.com) UK & Ireland Working Group developing best practice guidelines for Notice and Takedown procedures as they relate to Intellectual Property Rights (IPR).

MARCO GERCKE GERMANY

Dr. Marco Gercke is director of the Institute for Cybercrime Law (Institut fuer Medienstrafrecht) - an independent research institute on legal aspects of computer and Internet crime.

Holding a PhD in criminal law with a focus on Cybercrime he has been teaching law related to Cybercrime and European Criminal Law at the University of Cologne for several years and is visiting lecturer for International Criminal Law at the University of Macau.

The focus of his research is on international aspects of law related to Cybercrime. In this respect he is working as an expert for several international organisations among them the Council of Europe, the European Union, the United Nations and the International Telecommunication Union. One key element of the research are the challenges related to the fight against Cybercrime and the differences in developing a legal response in common law and civil law systems. The latest research projects covered the activities of terrorist organisations in the Internet, Legal response to Identity Theft, Money Laundering and Terrorist Financing activities involving Internet technology and the responsibility of ISPs.

Marco is a frequent national and international speaker and author of more than 60 publications related to Cybercrime. In addition to articles and books he published several studies including comparative law analysis for the Council of Europe. The aspect of responsibility of ISPs in the fight against Cybercrime was the topic of a study for the Council of Europe that was released in March 2009. His latest 255-page publication on Cybercrime is currently being translated into all UN languages.

Marco was co-chair of the working group set up by the Council of Europe to support the drafting of the Guidelines for the cooperation between law enforcement and internet service providers against cybercrime adopted at the 2008 Octopus Conference and member of the ITU High Level Expert Group. He is member of the German Bar and Secretary of the Criminal Law Department of the German Society for Law and Informatics

A full list of publications and speeches can be found at: www.cybercrime.de.

Estelle De Marco France

Dr. Estelle De Marco is an IT legal and regulatory consultant and Secretary General of a Centre of research on Information Security and Cybercrime (CRESIC, Montpellier).

Holding a Ph.D. in private law and criminal sciences, specialising in civil and criminal law, computer law and human rights, she has more than 10 years experience on IT legal issues and 7 years experience on legal and policy issues related to Internet illegal content (including Internet actors liability, IPR and data protection). She participates in the Europol Working Group on the Harmonisation of Cybercrime Investigation Training.

Estelle was Legal and Regulatory Affairs Counsel at the French Internet Service Providers Association (AFA) for 6 years. She has a strong understanding of IT technical issues. As manager of the AFA's hotline against illegal content, she was involved in a day-to-day cooperation with the French police cybercrime unit and participated in INHOPE projects. She represented French Internet industry at many international fora.

She was a member of the Council of Europe working group to support the drafting of the Guidelines for the cooperation between law enforcement and internet service providers against cybercrime adopted at the 2008 Octopus Conference. She completed several legal studies related to child care, cybercrime, IPR and technical threats to support the Industry's position before the Ministry of culture, the Ministry of economics or the European Commission. In coordination with AFA members she wrote the Industry policy on the fight against spam and the first specifications of the Signal spam mechanism, which allows ISP to receive notices about outgoing spam from their network (www.signal-spam.fr). She participated in the creation of Signal spam and was a member of its Board. Estelle also worked for 4 years at Montpellier's county Court.

Estelle is a member of Cyberlex (www.cyberlex.org), a French IT legal and technical specialists association, and of the Scientific Committee of Juriscom.net (www.juriscom.net), an online IT law specialised revue that regularly publishes contributions from professional lawyers, including academics. She has created and maintained for 10 years the Comité Réseaux des Universités (Universities Networking Committee) webpage on Internet "law and ethics", designed for technical experts (www.cru.fr/documentation/droit-deonto/index).

Hein Dries-Ziekenheiner The Netherlands

Hein Dries-Ziekenheiner LL.M is the CEO of VIGILO consult, a Netherlands based consultancy specialising in internet enforcement, cybercrime and IT law related issues. Hein holds a masters degree in Dutch Civil law from Leiden University and he has more than five years of technical experience in forensic IT and law enforcement on the internet.

Through his role as legal and regulatory counsel and representative of the Netherlands ISP industry association (NLIP), Hein has an extensive background and more than ten years of experience in internet networking and internet policy as well as law enforcement related issues.

Hein was delegate to the board of the European Internet Service Providers Association (EuroISPA) where he actively contributed to interventions and policy papers on a variety of topics including the 2002 regulatory package, the ISP liability regime and privacy related issues. He has represented the Netherlands ISP industry in many other (inter)national fora.

As a member of the very successful OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit), the Dutch telecommunications regulatory authority, internet-safety team Hein was responsible for the first major email spam fine under the 2002 EU regulatory framework and was involved in the infamous DollarRevenue spyware case. He headed several other anti-spam and anti-malware cases brought by OPTA, the Netherlands Independent Post and Telecommunications Administration.

Hein provides regular trainings to authorities in anti-spam and anti-malware forensics and has co-operated with many law enforcement agencies worldwide in spam cases, such as the US FTC and FBI, the Australian ACMA and the EU CPC network of consumer protection agencies. Hein is a member of the Netherlands association for Law and IT and his company, VIGILO consult, is an industry observer member at the London action plan on spam (LAP).

Hein regularly publishes and speaks on issues relating to internet law enforcement and cybercrime.

Contents

EXECUTIVE SUMMARY

1.1 Introduction

This report explains what Internet blocking is, what the motivations for implementing Internet blocking in society are, what technical options are available and what the legal issues which affect Internet blocking strategies are.

Note: Quotations in this executive summary are not immediately attributed to the author. These quotations are clearly presented between quotation marks and can be found again in the main body of the study, with the deatiled reference to the author and source. No further reproduction of theses quotations are allowed, when taken from the present study, without referring to the original author of the quotation AND the relevant page of the relevant chapter of this study, where the name of the original author of the quotation is indicated.

1.2 What is Internet Blocking?

This study provides a comprehensive analysis of the current state of Internet blocking, a review of the current regulatory and legal environment relating to Internet blocking and a commentary of the effectiveness of Internet blocking and its impact on the fight against cybercrime and the support of democracy and individual safety.

The most appropriate balance between the protection of children and democratic freedoms is a very complex issue which needs to be finally determined on a national level through extensive debate among relevant stakeholders in each country and with regard to relevant binding international instruments such as the European Convention on Human Rights.

According to the members of the European Parliament, unimpeded access to the Internet without interference is a right of considerable importance. The Internet is "a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society" and is protected by the right to freedom of expression, even when it is not currently considered as a fundamental right in itself [1].

In recent years, certain democratic states have promoted the use of Internet blocking technologies in relation to various types of content. They cite public interest to request specific blocks be implemented to uphold various aspects of public policy where the characteristics of the internet cause (international) enforcement issues. The subject matters vary from the availability of Nazi memorabilia via online marketplaces to gambling websites hosted in countries with liberal regimes in relation to online gambling. Similarly, states with less open information regimes have taken to blocking as a technical resource for extending their practice of information control into the online world.

[1] European Parliament resolution of 10 April 2008 on cultural industries in Europe, 2007/2153(INI), § 23, accessible at this address : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN. See section 6.3.2.2.

What is Internet Blocking?

Internet Blocking (sometimes called Internet filtering) is not a new activity. It has been around for many years. However, the term covers such a broad range of policies, hardware, software and services and it would be a mistake to think that all types of Internet blocking are the same or equally effective, legally equivalent or even that one system can easily be used in relation to more than one type of content.

The primary objective of Internet blocking is that content is blocked from reaching a personal computer or computer display by a software or hardware product which reviews all Internet communications and determines whether to prevent the receipt and/or display of specifically targeted content.

For example, an email might be blocked because it is suspected to be spam, a website might be blocked because it is suspected of containing malware or a peer-to-peer session might be disrupted because it is suspected of exchanging child pornographic content.

The term "Internet Blocking" itself is somewhat a misnomer since it seems to suggest that Internet blocking is easily implemented and it is simply a choice to switch on or switch off. Nothing could be further from the truth since the capabilities of Internet Blocking technologies are quite complex and often can be bypassed with little effort. There are various reasons for this, the most fundamental being that the Internet was designed to be decentralised, with a build-in capacity to ensure that data can flow "around" any barriers that are put in their way.[2]

Attempting to block Internet content that is legally made available outside the country but is considered to be illegal inside the country may sometimes also be considered as a possible option for countries to attempt to maintain their own national cultural standards in times of global access.

It can be said that Internet blocking began over 2 decades ago with the blocking of unsolicited emails (spam). This was started for many reasons but initially it was to prevent overloading of network capacity. This has been a constant area of research and development and an ongoing competition between anti-spam initiatives and spam activities. Despite these extensive initiatives over a long period of time, everyone who uses email today knows that spam blocking has not been totally successful since it has not eradicated spam from the Internet.

It is important to note that all Internet blocking systems are subject to false-negatives[3] and false-positive[4] problems and in advanced systems these are minimised during the design of the blocking technologies in use.

However, these problems can become more pronounced and have greater impact when Internet Blocking systems are applied to the public Internet and applied mandatorily to all users of the Internet in an area. They are therefore a significant issue for society as a whole to consider. Since these systems are often implemented with minimum and often inadequate public oversight or debate and applied without direct permission of the users of these Internet services, they need to be designed, developed, managed, implemented and audited in a much more transparent and accountable way.

There are different styles of Internet blocking. Personal filtering and network blocking are the two main styles of systems which are in everyday use. There are also systems which are hybrids of these two styles.

[2] The complex range of technology issues are summarized in Chapter 5

[3] A false-negative is when an email is allowed through the spam filter because when it is checked and scored negative to containing spam but none-the-less *is* actually spam. Therefore it is a false negative.

[4] A false-positive is when an item which should not be blocked is actually blocked by the filter because it scores a positive result by the blocking filter. Since the positive result is incorrect it is called a false-positive.

Blocking performed by the end-user enables the user to decide which type of content is blocked based on criteria assigned to each individual computer user and can be individually tailored and configured for different categories of users (parent, child, teacher, student, etc). This type of blocking is the most specific but does not prevent users from accessing content which, though maybe illegal, they still chose to see and download.

With network-based Internet blocking, the service-provider (Internet access provider, employer, club, etc) can determine which type of content or activity will be blocked for ALL users of the service, at least with regard to content accessed directly via the upstream network equipment of the provider where the blocking technology is implemented. (Sometimes the system can be tailored to decide the blocking criteria based on identified users).

There are two key issues to debate when we consider Internet blocking:

- How do we technically specify what to block?

  The processes which collect, review, assess and catalogue content, to identify which content should be blocked, are complex and resource intensive. These processes need to be developed, tested and implemented and personnel need to be identified and trained.

    - Block lists are the most common blocking strategy
    - Automated identification is on the drawing board, but with limited results
    - Rating systems have been available for many years but have not succeeded
- Who should choose what should be blocked on the Internet?
    - In countries where the judicial authority is independent from the legislative authority and the executive authority, which should be the case of all liberal democracies, only a judge should have the competence to declare a piece of content, a situation or an action to be illegal.
    - This issue creates one of the major challenges for Internet blocking systems. Current national and international legal processes rarely work adequately with the cross-border challenges of the Internet or the communications speed of Internet services. As a result there is rarely sufficient participation by the judicial authorities in Internet blocking decisions.

The International Network of Internet Hotlines (INHOPE) organisation coordinates a network of hotlines in over thirty countries processing reports about child pornography on the Internet. The hotlines received over 500,000 reports during 2005 and 850,000 reports in 2006, over 1m reports in 2007 and these numbers are increasing each year. Exact numbers for 2008 have not been published yet. Of the reports received from September 2004 to December 2006 less than 20% were considered illegal OR harmful and only 10% of the total was considered illegal by the hotlines.

A critical issue surrounding blocking lists is security and integrity. A list of such content is highly sought after by those with a disposition to experience such material. Even without block lists being leaked directly on the Internet research indicates that it might be possible to reverse engineer the block list used by any services provider.

Internet Blocking of Child Pornography does not cause child abuse to stop. It does not cause the images to disappear or be removed from the Internet. The most effective response to child pornography/ child abuse images is to cause them to be removed from the Internet, combined with a criminal investigation of the producer of the images and to remove the child from an abusing situation to a safe environment for treatment and recovery.

Internet blocking sometimes makes it more difficult to access such content (depending on the blocking system adopted) so that only more determined and technically aware persons will find it (depending on the client software in use). Where the images contain personally identifiable information about the victim, blocking such images can protect the victim from further feelings of exploitation.[5]

Unfortunately, some of the illegal content relating to child pornography on websites is currently hosted in countries and by Internet hosting providers where national legislation and political oversight and intervention is not comparable to current best practice in international standards and where direct notice-and-take-down procedures are underdeveloped or do not work. Initiatives addressing this issue need to be encouraged.

It is important to note the intrusive nature of many blocking strategies. This is especially true for the more granular, content based filtering mechanisms which require insight into the content of the material being exchanged between users. This is not only problematic from an investment perspective (the required investment is, invariably, high in these scenarios) but also from a broader, societal point of view.

The proportionality of an Internet blocking measure is generally difficult to assess, because it mainly depends on the particular 'legitimate aim'[6] to preserve within each situation, on the usefulness of the measure to reach that legitimate aim in a particular circumstance, and on the blocking characteristics and their impact on other rights and freedoms.

The consequences of an Internet blocking measure in terms of interference in fundamental freedoms are highlighted in Chapter 6 and 7. However, other possible interferences are enabled by several Internet blocking measures, due to the nature of the mechanisms put in place to implement the blocking.

The proportionality of each measure which interferes with some freedoms has to be evaluated firstly as regards its stated legitimate aim, and secondly as regards its general effect, which must not go beyond what is necessary to reach the pursued legitimate aim and, in any case, must "leave some scope" for the exercise of the restricted freedom and not "extinguish" the latter.

Each time a blocking measure is allowed because of its value in pursuing a legitimate aim, its more basic functioning must not limit other freedoms in a disproportionate way and some guarantees must be implemented to prevent this blocking measure from being used in a way that would further endanger freedoms.

In any case, it should be noted that no strategy identified in this report that seems able to completely prevent over-blocking. This is of prime concern when balancing the needs for blocking child pornographic content versus the need for human rights and free speech. It seems inevitable that legal content will be blocked where blocking is implemented.

Since Internet content can be exchanged over several Internet technologies, the practice of blocking only a limited number of these (such as blocking only traffic to web-servers) may also easily cause substitution of an alternative content distribution method. Those who have set their mind on distributing illegal content on the internet have a myriad of options to do so despite the network blocking taking place. From a technical perspective, blocking attempts can, therefore, only achieve protection for users who might access content inadvertently. It seems unlikely that blocking strategies, as outlined in this document, are capable of substantially or effectively preventing crime or re-victimisation.

Attempts to block content can be characterised as an act of re-territorialisation where countries aim to ensure that the national standards apply with regard to global content available to Internet users inside the country.

[5] This is discussed more in Chapter 6
[6] Refer to Section 1.6

All types of blocking attempts are not the same, all types of content are not the same and all types of crime are not the same.

1.3 Internet Blocking Debate and Motivations

The debate about "Internet blocking" can not be limited to one specific issue. The debate is as complex as the topic itself. There are widely different areas of concern and the challenges faced by policy makers to respond to Internet content problems are complex.

There are many motivations why society currently believes (or in some cases hopes) that Internet blocking attempts might solve some major social concerns since other approaches do not appear to be very successful. There are many different entities who have currently implemented blocking. There is a wide range of material which is the target of such blocking attempts. Internet blocking attempts can be approached in many different ways depending on who would be the intended target of the blocking initiatives. Several countries have already adopted Internet blocking systems.

The Internet is a vast complex network of networks with a myriad of hardware systems, protocols and services implemented. The first step with an Internet blocking initiative is to select where blocking can be attempted on the Internet. A second key concern is to determine who chooses what should be blocked and to determine the various levels of knowledge and ability of different users and organisations to block Internet content. A wide range of content can cause different concerns in different societies and each blocking measure needs to describe the variety of content which it targets and how some governments have turned to Internet blocking attempts as a possible solution to some of these problems. The primary motivations which cause policy makers to consider Internet blocking are important to note and why, in some cases, alternative approaches appear to have failed. An Internet blocking measure is usually targeted at either the producers or consumers of illegal content and has different levels of effectiveness depending on this choice.

The complex range of approaches and motivations towards Internet blocking attempts need to be clearly differentiated in order to enable a comparison between these different approaches.

The first criterion that can be used to differentiate between the different blocking approaches is the target of the blocking instrument. In general there are four different targets blocking could focus on:

- Service-based approach e.g. email,
- Content-based approach e.g. hate speech, child pornography, gambling websites
- User-based approach e.g. users who download illegal music, send spam
- Search Engine based approach e.g. preventing search results for illegal websites

A second criterion that can be used to differentiate between the different Internet blocking approaches is to focus on the role of the decision-maker about illegal content. The decision-maker is the person or institution which makes the decision about ***what*** should be blocked.

- Individual Driven
- Institution Driven
- Legislator / Court

Internet blocking is discussed as a technical solution with regard to a wide range of illegal activities. To a large extent – but not necessarily - these acts are criminalised in the country that is intending to implement or has already implemented blocking technology but is not always criminalised in the same way in the country where the content is hosted. Child pornography is among those categories of content where the content blocked is covered by criminal law provisions.

Enforcement is difficult on the Internet where material is often legally made available on servers outside the country. This is a direct consequence of different national standards implemented with regard to the publication of material. Attempting to block content that is legally made available outside the country but is considered to be illegal inside the country could be seen as a possible option for countries to attempt to maintain their own national cultural standards in times of global access.

Other content which is the target of Internet blocking attempts include:

- Spam - E-mail provider organisations report that currently as many as 85 to 90 per cent of all e-mails sent are spam. Most spam blocking is performed with customer consent.

- Erotic and pornographic Material - often considered by policy makers within the context of preventing minors from getting access to content that is considered harmful. In some countries "*adult verification systems*" have been developed to prevent minors gaining access to adult content. Other countries criminalise any exchange of pornographic material even among adults.

- Child Pornography - is universally condemned and offences related to child pornography are widely recognised as criminal acts. Despite substantial efforts and costs, those initiatives seeking to control the network distribution of child pornography, have proved little deterrent to perpetrators.

- Controversial political topics / hate speech / xenophobia - Some countries criminalise the publication of racial hatred, violence and xenophobia while such material can be legally published in other countries that have a strong protection of freedom of expression such as the US.

- Illegal Gambling - The Internet allows people to circumvent gambling restrictions. Online casinos are widely available, most of which are hosted in countries with liberal laws or no regulations on Internet gambling.

- Libel and publication of false information - Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.

- Content published by terrorist organisations - the publication of propaganda and the publication of information related to the commission of crimes is common.

- Copyright violations - include the exchange of copyright-protected songs, files and software in file-sharing systems and the circumvention of Digital Rights Management systems. Peer-to-Peer (P2P) technology plays a vital role in the Internet.

Why Consider Internet Blocking?

- Missing Control Instruments on the Internet

  Since the Internet was originally designed based on a decentralised network architecture, resilient to failure and disruption, the Internet is resistant to external attempts at control. Blocking attempts could be considered as an approach to implement such control instrument that was not foreseen when the network was developed.

- International Dimension

  International cooperation based on principles of traditional mutual legal assistance is often very slow and time consuming. The formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations. Blocking attempts might therefore be considered as an approach to act even in those cases where the limitations of current international cooperation prevent measures to be taken in a timely manner.

- Decreased Importance of National Hosting Infrastructure

  The publication of content that is perfectly legal in one country might be criminal act in another country. Attempts to block content can therefore be characterised as an act of re-territorialisation where countries aim to ensure that the national standards apply with regard to global content available to Internet users inside the country.

Who to block?

Blocking of illegal Internet content can not only be seen as an instrument related to the offenders that make content available online (producers) but also as in instrument aiming to prevent the user from downloading illegal content (consumers).

- The producer of illegal content - the illegal content provider.

  The Internet has become a major tool for the distribution of child pornography as it offers a number of advantages to the perpetrators that make investigations challenging. In an analogous way, the modern digital camera and digital camcorder have become the major tool for the production of child pornography.

  The reason to implement blocking technology is therefore similar to the reasons to criminalise the exchange of child pornography i.e. to reduce the volume of crime and to protect children.

- The consumer of illegal content.

  In addition to the production, publication and making available of child pornography, a significant number of countries criminalise the possession of child pornography. The demand for such material could promote its production on an ongoing basis. Furthermore a number of countries go beyond the criminalisation of the possession of child pornography and even criminalise the act of ***gaining access*** *to* child pornography.

While the fact that Internet blocking does *not* remove content at the source hinders the instrument from being able to prevent the offence of making content available the instrument, if technically effective, has the **potential to prevent offences committed by some users, that are trying to access a website to either watch or download child pornography**. The success of this depends on the effectiveness of the blocking technologies in force and the level of motivation and knowledge of the user.

The main concerns about blocking are the missing removal of the content at its source and the many possibilities to circumvent the technology. These aspects have several implications:

- The content can still be accessed by using connections that do not block access.
- Once blocking technology is developed and implemented it could be used for other purposes. One of the main reasons for this concern is related to the non-transparent implementation of such technology.
- The fact that the content is not removed enables users to seek access by circumventing the technical protection solutions.
- There are several ways how these blocking approaches that are currently discussed can be circumvented.

- The fact that content is not removed, suggests to users that these are safer websites to access since the authorities have clearly failed to have them removed and investigated.
- Exchange of child pornography via file-sharing systems or encrypted e-mail exchanges are not covered by the current web based approaches.
- making such material invisible might mislead the political debate as it could create the impression that the problem of online child pornography has been adequately addressed and thereby reducing civil concern in this area.

In addition to systemic limitations of blocking approaches technical and legal concerns need to be taken into consideration.

Other non-blocking approaches

- improving the means of international cooperation in order to narrow the time gap between the identification of illegal content stored abroad an the removal.
- working towards the removal of such content to hinder serious offenders from getting access to it.
- Investigating child pornographic images to ensure the victims in those images is identified and removed from the abusive situation.

Several European countries such as Finland, Norway, Sweden, Switzerland, United Kingdom and Italy as well as non European countries such as Australia, China, Iran and Thailand use Internet blocking. The technical approaches, the aim of filtering as well as the level of industry participation varies.

In Australia, for example, a block-list generated by ACMA (Australian Communications and Media Authority (ACMA) is likely in future to become mandatory for all ISPs. In the UK the block-list is generated by the IWF (Internet Watch Foundation). The technology used is BT Cleanfeed or URL filtering. In Denmark the block-list is generated by National High Tech Crime Centre of the Danish National Police and Save the Children Denmark. In Finland blocking was initially based on a list of domains supplied by the Finnish police. Most ISPs today participate in the approach but based on DNS blocking.

1.4 Technical Aspects of Internet Blocking

The development and implementation of various types of Internet blocking technology on the internet is not a recent development. For a long time, spam, internet-based viruses and malware and many other content-types that are unwanted and unrequested by the end-user have been targets of blocking efforts undertaken by industry for security and usability reasons, or by the state in its role of developer and enforcer of laws and policies.

A technical overview of the major Internet blocking systems in use today is essential, as is an explanation on how these are applied to different Internet services. In addition to concerns about the effectiveness of such blocking systems, there are also significant technical impacts and challenges created by these systems. There are also many ways to evade these blocking systems and an analysis of the effectiveness of these systems is included.

Democratic states have promoted the use of Internet blocking technology in various policy areas, citing public interest to demand certain blocks be implemented to uphold various aspects of public policy where the characteristics of the internet caused (international) enforcement issues. Similarly, states with less open information regimes have taken to blocking as a technical resource for extending their practice of information control to online media.

All of these developments hinge on the availability of internet blocking technology. Depending on their technical characteristics, they differ in effectiveness and potential for circumvention. Techniques for blocking child pornographic content are the main focus, but it is important to note that many blocking technologies can be deployed for other types of content or activity with limited additional investment.

Specifying content

In order to attempt to block content, identifiers are needed whereby a blocking decision can be implemented. The content that this report focuses on is usually visual in nature, meaning that it contains either still pictures or video footage of child sexual abuse.

- IP addresses
- Domain names and DNS
- URLs
- File content and Filename
- Keywords
- Content Signatures (hash values)

Measuring Effectiveness

1. It is not possible to express effectiveness as the **amount of content that is blocked correctly in comparison to the total amount of available illegal content** since the total volume of available illegal content is unknown.
2. Since it is often unclear where hits on a website come from, **figures quoting volume of hits on an existing list are a very crude indicator** at best.
3. Analysis of **over-blocking and under-blocking potential** can be used as indicator of the effectiveness of Internet blocking technologies.
4. Another indicator for effectiveness is the **ease of circumvention of a block**. If it is easy to circumvent or disable a block, the availability of the blocked material is likely to remain unaffected.
5. **The availability of alternative methods of access to the same content**, by whatever means, can be seen as a measure for effectiveness of blocking in the absence of precise data.
6. T**he availability of other enforcement options** that offer other more effective methods of preventing access to the material can also be assessed - especially if they are less costly, less intrusive or more effective towards the availability of the material.

Characteristics of Blocking Strategies

- **Allow-list versus Block-list** - Filters that are configured by default to "allow" content to pass unhindered but have specific lists of content to block are usually called block-lists, whereas filters that are configured by default to block all content except specific listed content are called *allow-lists*.
- **Human intervention (dynamic and non-dynamic blocking)** - Typically, child pornography filters are based on consumer complaints and law enforcement investigations. The contents of the filter will usually be manually selected since the content is reviewed and matched against the block-list criteria personally by the list administrator. On the other hand, many filters such as email filters and certain virus scanners will often use pre-defined criteria to filter the content to block without human intervention. These criteria can be multi-faceted and complex.
- **Blocking Point** - Blocking strategies can be differentiated by the level at which they are executed. User level filters allow parents and computer administrators to select and

block content types. Other filtering techniques are employed at the organisation, ISP or even state level. They typically require sending all traffic through central machines that analyse incoming traffic.

Level of Detail or Specificity

- **IP Addresses** - Blocking an *IP address* means that other Internet services and users that use the same address will also be blocked.
- **Domain-Names** - Blocking by a domain-name will block ***all*** content residing under that domain.
- **Uniform Resource Locators (URL's)** – Best results in terms of specificity will be obtained by filtering on a URL basis. Due to the ease of evading these filters, blocking by this identifier can lead to a significant risk of under-blocking.
- **Content Signatures** - content can be blocked using signatures that allow for classification of content that was previously categorised as illegal. New content is easily missed by the filter. Encryption of the content will render this method useless.
- **Keywords** - blocking based on keywords found either in the filename or the URL or the text at the location of the content being accessed. Complex analysis of the recognised keywords in the context of their use needs to be performed.

Internet distribution methods for Child pornography

Child pornography can be distributed across the Internet using various methods via high speed broadband Internet connections. In addition to the distribution of static content (pictures and video material), they also serve as a launch pad for other, related activities such as *grooming* and *cyber bullying*. The increased use of social networks is especially important in this latter area.

- Websites

  Websites are one of the foremost distribution methods for content on the internet. Usually, web content resides on the server but content can also be retrieved dynamically or created dynamically, whereby a database is often used to hold relevant data. It is common for many different web-servers operated by different owners to be attached to one IP address.

- Email and Spam (unsolicited email)

  Email is still the most widely used service on the Internet, even more than web or social networking websites.

- Usenet Newsgroups

  The important difference between newsgroups and email is that streams of messages passed between Usenet servers (often called "newsfeeds") are organised into groups that suggest references to the content of the messages being exchanged.

- Peer to Peer networks (P2P)

  Peer-to-peer file-sharing is based around the exchange of files directly between end users' computers, bypassing intermediate servers. Although the technology has legitimate uses it lends itself to the sharing of music and movie files, causing major challenges for copyright holders.

- Search engines

  By indexing the content of websites, search engines are able to identify relevant content by way of keyword searches and complex search algorithms.

- IM and Other

  Another important tool for exchange of child pornographic content is instant messaging. The IM channel serves more as a vetting and introduction mechanism, whereas content is exchanged directly, using other technologies.

Blocking Strategies & Effectiveness

- Website Blocking

  Blocking of websites is usually executed using one of two different identifiers.

  - the server that contains the website could be blocked at the level of its IP address, preventing anyone using the filter from accessing that address. A block-list would then contain only IP addresses of known illegal content.
  - a blocking measure could be adopted based on the domain name or even on the URL of a specific file or page hosted on a website.

  If this type of blocking attempt takes place in the access network rather than in the user's equipment, circumvention is, relatively speaking, more challenging for the user since the user would need some basic knowledge about how the Internet works.

- Email Blocking

  Most email filters operate on, or right before, the **receiving** mail-server that takes incoming mail for users on a network. There are two ways of email filtering:

  - there are connection based filters that check the originating IP address of the sending mail-server against a number of blacklists.
  - filters can use the content of messages to filter out unwanted content.

  Potential for over-blocking is present where IP addresses or even entire originating mail-servers are blocked due to incidents involving child pornography.

- Usenet Blocking

  Blocking attempts of Usenet content is traditionally done by blocking access to parts of the group hierarchy or refusing to host a particular newsgroup. Internet Access Providers have observed that, when deprived of access to more suspicious hierarchies, users will be inclined to move their illegal content under less conspicuous names, potentially leading to more incidents of accidental access to illegal material.

- Search engine results blocking

  It is possible to prevent access to search results at the level of search engine providers. An important question is the visibility of filtering, as displayed in the results pages of search engines. Some providers clearly state their policy regarding the filtering of results, others do not. Circumvention of this filter is easy: simply accessing the content directly would be sufficient.

- Peer-to-peer and IM Blocking

  Blocking attempts of peer-to-peer traffic is a substantial task. Many p2p protocols are distributed - meaning that files being downloaded will be constructed from several sources and so no one stream of data contains the whole file.

  - The first option to attempt to block access to P2P content is by analysing the p2p network content by acting as a user of the service. By requesting certain files or monitoring the request and answers from other users it is possible to find users that have parts of a file on their hard drive. Blocking access to their IP address or disconnecting these users if legally and technically feasible, however, is then the only extreme remedy available.

- The second option with maximum effectiveness in the attempt to block content in these networks is to use technologies akin to Deep Packet Inspection to recognise the files as they are being exchanged

Summary

This table lists characteristics of every blocking strategy discussed. It shows the likelihood off over- and under-blocking according to our estimates, lists the resources required to execute the blocking strategy, the block-list type and maintenance effort required for such a list and, in the last column indicates whether the communications contents needs to be analysed extensively for this strategy (DPI technology or alike) for blocking to be effective.

Medium	**Blocking**	**Effectiveness**				**Blocklist**		**DPI**
		OVER-blocking	*UNDER-blocking*	*Resources required*	*Circumvention*	*Maintenance effort*	*Identifier*	
Web	*DNS*	Very Likely	Likely	Low	Easy	Medium	Domainname	-
	Domain	Very Likely	Likely	Medium	Medium	Medium	IP address to domainname	-
	URL	Less likely	Very Likely	Medium	Medium	High	URL	+
	IP	Very likely	Likely	Low	Medium	Medium	IP address	-
	Dynamic	Very Likely	Very Likely	High	Medium	Low	Keywords, graphics recognitiontechnology or other	+
	Signatures	Less likely	Very Likely	High	Medium	High	Hash	+
	Hybrid (IP+signature/URL)	Less likely	Very Likely	Medium	Medium	High	Ip and Hash or URL	+
Email	*Dynamic*	Likely	Likely	Medium	Harder	Low	Keywords or other	-
	URL	Likely	Likely	Medium	Harder	High	URL	-
	IP address	Very likely	Likely	Medium	Harder	High	IP address	-
	Signatures	Less likely	Likely	High	Harder	High	Hash	+
Usenet	*Per Group*	Likely	Likely	Low	Easy	Low	Groupname	-
	Per hierarchy	Very Likely	Less Likely	Low	Easy	Low	Group hierarchy	-
Search	*Keyword*	Very Likely	Very Likely	High	Easy	Medium	Keywords	-
P2P	*Per protocol*	Very likely	Less Likely	Medium	Harder	Low	Protocol recognition	+
	Per file (signature)	Less likely	Very Likely	High	Harder	High	Hash	+
	Per file (dynamic)	Likely	Very Likely	Very high	Harder	Low	Advanced algorithms	+

Whilst the distribution methods may vary, each method can function as a reasonable substitute for each other method. Regardless of the effectiveness of blocking the content on one of the media, any flaw in blocking the same content on any of the others will lead to changing the distribution method.

Most child pornographic activity on the Internet today involves the use of multiple Internet services and systems. There are several investigated cases where contact between an adult and a child started in public chat rooms, moved to private chat rooms, progressed to personal emails and private SMS (Short Messaging Service) text messages across the mobile phone network with final face-to-face meetings arranged via personal phone calls on mobile phones.

Investigating such activity is very challenging and requires broad knowledge on behalf of the investigators of all aspects of internet technologies and telecommunications.

Evading Internet Blocking

- Proxy-Servers

  Circumventing this type of filter is quite trivial. To circumvent a filter blocking access directly, a user can ask a foreign proxy server to access the blocked content on his/her behalf and, as long as that foreign proxy server itself is not being blocked, and the user can thus gain access to the content to bypass local filtering.

- Tunnelling

  Tunnelling software allows users to create an encrypted 'tunnel' to a different machine on the Internet which prevents the filtering software from seeing web requests. Once a tunnel is created to the other machine, all Internet requests are passed through the tunnel, through the machine on the other side, and on to the Internet.

- Hosting or URL rotation

  From the point of view of the content publisher, changing the website configuration to a different address (domain-name, URL or even IP address) is also trivial, and would effectively bypass IP, URL or domain-name based filters.

- Botnets

  Domain name rotation or IP address hiding is often done using botnet technology whereby compromised innocent end-users machines are used to act as a portal to the content of the web server. In essence, the user's computer is turned into a non-caching proxy.

- Evading DNS based filters

  Even easier to bypass is blocking at the level of the DNS query. Merely changing the DNS server of the provider to a different one (which is not part of the blocking system) is enough to totally circumvent this blocking method.

Where blocking is done on anything other than a full url (path name) or a content signature, there is a significant potential for over-blocking. However, conversely, url or content signature blocking offers significant potential for under-blocking.

Blocking web traffic effectively, (i.e. blocking the access of the user to the content and not merely using DNS filters) requires significant investment in proxy deep packet inspection infrastructure and substantial interception of all Internet communications.

Filters have the possibility of providing useful intelligence to criminals operating illegal child pornography websites. If they operate a website which has been placed on a blocking list they then know that the website has been identified by the authorities and is then highly possible to be under investigation and monitoring by law enforcement.

- The criminals can then take steps to destroy any evidence AND take steps to relocate their services to a new location anywhere else in the world.
- They can test their hiding technologies against the detection system to research which techniques provide longer protection against detection and blocking.
- Blocking activities also cause disruption to those accessing such websites thereby forcing the web operators to move their content more frequently. These movements can also be tracked and can offer useful intelligence to investigators tracking their movements and may provide useful research data.

The resources and effort required as a result of constant evasion of blocking activities whilst staying anonymous should not be underestimated. It is likely that this will lead to mistakes occurring sooner. However, it is important to note that the resources and effort are to create and maintain an Internet blocking system are just as significant especially when required to constantly respond to evading activities.

Implications for a democratic society

- Security issues

  The infrastructure required to execute a blocking strategy is capable of interfering with many critical elements of end users' internet connections. In addition, the content of block-lists is of prime interest to paedosexual offenders since they have strong motivation to use the blocking list for the opposite reason to the one that it was designed:

- Over-blocking and Under-blocking

  No strategy identified in this report that seems able to prevent over-blocking. This is a major concern when balancing the need to protect children versus human rights and freedoms. It seems inevitable that legal content will be blocked where blocking is implemented. Under-blocking is also a universal phenomenon especially present in the more proportionate and focussed blocking strategies.

- Mission creep potential and re-territorialisation

  Many of the blocking strategies are very intrusive into Internet communication. The more granular, content-based filtering mechanisms require insight into the content of the material being exchanged between users.

It is important that public debate take place and that this debate consider the essential technical and legal differences between different types of content and the proportionality of blocking to other methods of harm reduction, crime prevention, and cybercrime investigations.

1.5 Internet Blocking and the Law

Attempting to block illegal material is not the definitive removal of access to specific images, videos or web pages. The inevitable circumvention possibilities, under-blocking, over-blocking, mission creep, conflicts of laws and the problem that blocking leaves material online all mean that the issue at stake is not simply "to block or not to block" but rather what blocking measures can be introduced that are proportionate and acceptable in a democratic society. As a result, it is crucial to review the legal and democratic challenges that Internet blocking raises.

A comprehensive overview of Internet blocking and the law requires a review of relevant legal instruments which affect Internet blocking systems. Modern liberal democracies play a key role by their active respect for fundamental freedoms and civil liberties. Both national and international instruments need to be considered to determine what fundamental rights are in opposition to Internet blocking and which fundamental rights support Internet blocking. The role of Internet Service Providers is fundamental to Internet blocking measures and they operate in confusing circumstances with regards to competing and sometimes contradictory legal requirements.

In the eyes of the law, Internet blocking is a measure that would give, in the aim of protecting a particular interest, a right to block, a right to choose the technological means to achieve this and the right to choose the content to block, in the knowledge that this will result in some citizens being deprived of a right of accessing content or the right to make available some content.

Internet blocking therefore is a measure that would be provided for to protect particular rights or freedoms, while having direct and immediate impact on other rights and freedoms. Since rights and freedoms are governed by law, the analysis of the legitimacy of Internet blocking (therefore) requires a thorough analysis of the elements of law that are relevant to, and could be in conflict with, such a measure.

Since Internet blocking is a measure which is internationally debated, this study will especially focus on international law and European law, while some examples of application by sample national laws will be given.

Within these legal systems, Internet blocking may be inconsistent with two areas of law, namely human rights and fundamental freedoms and some specific provisions related to electronic communications. It might be consistent with some of aspects of these rights and freedoms depending on the proportionality of the Internet blocking measure adopted.

The challenge is to determine to which extent one freedom can be limited in order to preserve another. Each of these freedoms needs to be reviewed in detail to enable a conclusion on the conditions under which Internet blocking might be considered acceptable under legal principles.

Numerous national legal systems, as well as the European and international legal systems, give an important place to Human Rights and Fundamental Freedoms, which might be invoked to justify a blocking measure, or which would be inappropriately affected by such a measure.

The preservation of Human Rights, and in particular the ones that could be in conflict with an Internet blocking measure, i.e. the right of private life or the right to freedom of expression, are often considered as intrinsic in democracy. There are three aspects where the relationship between democracy and freedoms can be seen.

- Elections - The principle of participation of everybody in public life.
- Separation of Powers - The institutional structures for the separation of powers
- Fundamental Rights - The State’s willingness and engagement to respect freedoms

The difference between Human Rights, Fundamental Freedoms and Civil Liberties mainly lies in the *holder* of the rights, who depends on the content of the awarded right, and in the legal value of the text and the importance of its protection. A particular right can receive the three qualifications, as the rights to protection of private life and of freedom of expression do in numerous countries. Civil liberties are limitations of the powers of the public authority towards citizens.

To the notions of Human Rights and Civil Liberties, has been added the notion of “Fundamental Rights” or “Fundamental Freedoms”. Fundamental Rights and Freedoms are,

- protected against the executive and against the power of the Parliament;
- are guaranteed not only by the Law but above all by the Constitution or by international and supranational texts.
- secured from the executive and the legal power, through the application of the Constitution (or international texts), the competence not only of the ordinary judges, but also of constitutional judges and even international judges

The first texts that declared Human Rights and Fundamental Freedoms were national. International texts came after the Second World War and contributed to modifying national legal systems. Their content was also recognised by the European Union institutions.

Internet blocking attempts need to be analysed in the light of the main fundamental freedoms that seem in conflict with it – including Freedom of Expression and Right to Respect for private and family life - or which seem to support of it – including children’s right to be protected against violence and exploitation.

International instruments related to Human Rights and Fundamental Freedoms have been adopted within the framework of the United Nations and the Council of Europe including:

- Charter of the United Nations
- UN Universal Declaration of Human Rights (UDHR)
- UN International Covenant on Civil and Political Rights
- UN Convention on the Rights of the Child
- UN Convention on the Rights of Persons with Disabilities
- UN Convention on the elimination of all forms of racial discrimination
- Council of Europe European Convention on Human Rights (ECHR)
- Council of Europe Convention on Cybercrime

Although the European Union has not yet adhered to the European Convention on Human Rights the European Union recognises the necessity to preserve Fundamental Freedoms and to respect the ECHR. The European Union also emphasises certain categories of rights as well as international texts analysed, such as children rights, rights of disabled people or the right to not being discriminated.

Fundamental freedoms that might be in opposition with blocking

Internet blocking can have impact on some Human Rights and Fundamental Freedoms.

- Internet blocking attempts can interfere with **the right to private life**, permitting or requiring the retention of Internet data that is protected by confidentiality, or preventing individuals from availing of some Internet potential and therefore preventing the possibility to create certain connections or to make some connection choices, which comes under the right to freedom of the private life. This is particularly the case with regard to the inevitable over-blocking that impacts on completely innocent websites
- Internet blocking attempts can interfere with **the freedom of expression**, by preventing people access to online information or to make available such information. It has a negative impact on information broadcasting, communication and reception.
- Internet blocking interferes with the specific rights awarded to some categories of persons, such as **the right for disabled persons** to access electronic communications.
- Internet blocking may be seen as a substitute for respecting the obligations in the Child Rights Convention requiring states to take all appropriate international steps to prevent the exploitation of children for pornographic purposes.

The right to respect for private and family life is a Human Right and a Fundamental Freedom, and is therefore a Civil Liberty. It directly concerns adults and children, even if the United Nations Convention on the Rights of the Child supplements this with a specific declaration on children’s right to respect of private life in article 16.

Right to Private Life

These texts protect individuals from arbitrary interference with their privacy, family, home or correspondence and from attacks upon their honour and reputation. The UDHR declares that “*Everyone has the right to the protection of the law against such interference or attacks*”. The ICCPR declares the same and adds that **interferences must be lawful,** which calls into question some industry-lead blocking initiatives, which have no legal underpinning. The ECHR allows some interferences at the conditions described within the so called “public order clause”, including the lawfulness principle.

The principle of privacy of correspondence, which the European Court of Human Rights interprets to "*protect the confidentiality of private communications*", is one of the Fundamental Freedoms that could be directly undermined by an Internet blocking measure.

Depending on the target to block (type of content, communication protocols) the means used for blocking and the additional rules potentially put in place to reach the particular aim of the whole mechanism, Internet blocking attempts can sometimes lead to the retention of the content of a communication, or to some details of this content in relation to a specific person, without the consent of this person.

Even if the communications received or sent by a person are not categorised as correspondence, they are nonetheless protected by the right for private life. On the basis of this principle, a blocking measure that would lead to monitoring or to retaining data about the content that a person receives, sends or consults, even if it is only about the consultation of a website of a particular nature, would be in interference with the right for private life. It would also be in interference with the right to protection of personal data.

The principle of protection of personal data implies the confidentiality of this data, when it is combined with data that enables identification directly or indirectly of a natural person. Each piece of data enabling the surveillance of people is considered dangerous, even if it is not used, especially in a democratic state.

Freedom of private life can be understood as the freedom to establish and maintain relationships, also via electronic communications, but also to make online cultural, leisure or consumption choices, or to freely surf and access information on the network. The freedom of correspondence, which is the power to correspond with chosen persons, is itself protected by the right to secrecy of the correspondence

An Internet blocking measure that would have a negative influence on the freedom to correspond would therefore be in conflict with article 8 of the ECHR.

Internet blocking can be considered as being in conflict with a fundamental freedom as long as it presents **the risk of interfering in such a freedom, *even if it does not have for purpose to use the functionality* that presents such a risk**.

Freedom of Expression

Freedom of expression is a Human Right and a Fundamental Freedom, and therefore a Civil Liberty. It applies to adults and children and the UN Convention on the Rights of the Child adds a specific declaration on children's right to freedom of expression.

This right includes "*freedom to hold opinions and to receive and impart information and ideas*", "*regardless of frontiers*". This right shall be exercised "*without interference by public authority*". The UDHR and the ICCPR add the freedom "*to seek*" information and ideas "*through any media*", while the ICCPR explains that this right can be exercised "*either orally, in writing or in print, in the form of art, or through any other media of his choice*".

The ICCPR and the ECHR state that the exercise of the freedom of expression carries with it "*duties and responsibilities*" and may be subject to certain restrictions.

Freedom of expression includes the right to receive information, notably through the Internet. Any Internet blocking measure that would prevent a person from accessing content would therefore be in conflict with that freedom. It would be worse for a measure which advocated suspending Internet access, thereby preventing or impeded a person from using the whole Internet network or a part of it.

Within the framework of the reform of telecom legislation, the European Parliament restated, on 6 May 2009 that "*no restriction may be imposed on the fundamental rights and freedoms* *of end users, without a prior ruling by the judicial authorities (…) save when public security is threatened.* Several authors and European Parliament members believed that this was recognition of Internet access as being a fundamental right

Regardless of whether or not Internet access is an *independent* fundamental right, it is at least protected as a means of exercising freedom of expression, and each Internet blocking measure that attempts to prevent people from accessing information is therefore in conflict with that freedom. Each blocking measure limits the right to freedom of expression, to a greater or lesser extent depending on the blocking characteristics and the degree of over-blocking, as the necessary aim of such a measure is to limit the accessibility of specific content.

Rights of the Child

Each Internet blocking measure that would prevent children accessing information which would be useful for their development and education towards a responsible life would be in conflict with the Convention on the Rights of the Child and certainly with the right to freedom of expression, especially if it is not under parents' control.

Rights of Disabled People

Disabled people have the added problem that their disability might sometimes restrict them from fully exercising their rights. They can be assisted through the use of electronic communications - including Internet services. As a consequence, an Internet blocking measure that would prevent disabled people from accessing electronic communications might prevent some of them from exercising some fundamental rights that non-disabled persons would still be able to exercise despite a prohibition of using the Internet or a part of it.

Fundamental Rights and Freedoms that might support Internet blocking

The protection of some other rights and freedoms might support Internet blocking. Three of these rights are:

- the children's rights to be protected from violence
- the right of people to not be discriminated against
- Intellectual property rights

Children are highly protected against violence. There are two aspects of child welfare protection which is of particular interest.

- The large number of texts which emphasise the prohibition of mental and physical violence towards children, especially of a sexual nature.
- The prohibition of the image itself of a crime of sexual nature committed against a child, through the prohibition of child pornography.

The importance of the fight against child pornography, as well as the importance of protecting children against violence and an impaired personal development, is very often an argument to justify the implementation of Internet blocking measures. It is often the only justification by governments or private entities which support the implementation of Internet blocking.

If one is to accept the arguments put forward to support blocking, it is legally difficult to understand why a blocking measure would be restricted to child pornography only, since the law also specifically protects other categories of people from threats, notably from those threats that are generated by discrimination.

Human Rights and Fundamental Freedoms are awarded to each individual without distinction. However, as discrimination has been and still might be a problem in some countries, several texts were signed to emphasise specifically the right to any individual to be protected against discrimination. Internet content that comes under these prohibitions can be texts encouraging discrimination, but also images of torture or murders, committed for racial considerations. These images are very disturbing and would also offer an equally valid justification of Internet blocking, in addition to child pornography.

Intellectual property rights (IPR) are protected by numerous treaties at the international level. The general declarations of such rights, notably includes copyrights and related rights, which "*protect the rights of authors, performers, producers and broadcasters, and contribute to the cultural and economic development of nations*". The right to protection of IPR is therefore considered as a Human Right and a Fundamental Freedom, and might also be a civil liberty in some countries. This right might therefore be evoked to justify an Internet blocking measure, as long as such a measure would, in reality, serve to protect it.

Specific provisions related to electronic communications

A blocking measure provided for within the European Union must furthermore comply with European rules applying to electronic communications.

- Those rules include the Internet Service Provider's obligations in terms of **quality of service** and **universal service obligations** and the Internet Service Provider's **obligation of neutrality**.
- The rules concerning Internet Service Provider **liability** are a further basis for Internet Service Providers to argue against blocking measures that are implemented outside the framework of a law.

Services included within the scope of **universal service** are basic communications services, including voice communications and a connection to the Internet. Any blocking measure that would prevent an Internet user from accessing the public telephone network would therefore be in conflict with the universal service obligation. Allowing citizens to access the Internet stays an objective that has to be balanced with other rights or freedoms and the general interest of the public.

If high-speed Internet is recognised in the future as a component of universal service, and if the current modifications of the EU telecom legislation are finally approved, a state would therefore not be authorised to take any user-blocking measure without respecting the European Convention on Human Rights, especially as regards the need to respect the public order clause and the right to a due process, before a court of law.

Electronic communications operators must also ensure a certain **quality of the access service** they provide. They are in charge of the carrying of public service information, in addition to the specific obligations they may have to respect when ensuring a universal service or a public service obligation.

Public computer networks are technically very complex and that most Internet blocking measures increase network susceptibility to breakdowns and latencies. As a consequence, **operating an electronic communications network and blocking are philosophically in opposition**, and asking an operator to implement a blocking measure could put it in a position where two obligations with contradictory effects have to be respected.

Internet Service Providers have an obligation to stay neutral vis-à-vis the content of electronic communications exchanged on the Internet, following the example of other categories of carriers (such as traditional telephony and postal services). As a result of these principles, an Internet Service Provider cannot choose to transmit or not transmit a message depending on its content, except on the basis consumer consent or of a legal obligation that would justify its non respect of the neutrality principle.

An Internet Service Provider cannot monitor contents that are exchanged through its network, except on the basis of a specific obligation stated by the law. Any blocking measure that would require monitoring of content that is exchanged on networks in order to identify specific illegal content would therefore not be allowed unless specifically provided for by a law respecting the European public order clause.

Without a law that obliges Internet Service Provider's to block specific content, Internet Service Providers cannot monitor and block web content without being in breach of the condition of their liability protections implemented by the EU Directive, and therefore risking liability for content they transmit.

An Internet Service Provider that would select some content to block, without being obliged to do so by the law, would be susceptible to fall outside the requirements laid down in the current liability regime. Such an Internet Service Provider would therefore take the risk to see its liability challenged before a court, for every piece of illegal content or activity that would be transmitted through its services. Such a situation would be legally very uncertain. It would endanger the Internet Service Provider activity itself, and more globally the technological development of the country.

1.6 Balancing Fundamental Freedoms

From the point of view of the International Covenant on Civil and Political Rights and European Convention on Human Rights, the issue of balancing freedoms comes always within the framework of a limitation on a protected freedom, in the aim of preserving another.

Within the framework of an Internet blocking measure, children's rights or the right of persons not be discriminated against or Intellectual Property Rights, have to be balanced with the rights and freedoms of family life and freedom of expression that are in opposition to them.

Some of the rights identified in the International Covenant on Civil and Political Rights and the European Convention on Human rights are "absolute", such as the right to life or to not be subjected to torture, while others are "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression.

The success of balancing conditional fundamental freedoms when different rights are in conflict can be achieved through an analysis of processes adopted by the European Court of Human Rights which can provide guidelines on how Internet blocking measures might be implemented. This needs to take into account **the strict 'public order' clause** which includes **the principles of necessity in a democratic society**. These principles are then applied to different Internet blocking initiatives by reviewing the objectives of these initiatives and how they might be judged using the ECHR guidelines. An examination of the legitimate aims of an Internet blocking initiative and the validity of some systems needs to be questioned. A sequence of steps can be followed in order to evaluate Internet blocking proposals for their legitimacy in a democratic society.

The "Public Order Clause"

The possibility to limit the exercise of conditional rights can take two different forms.

- Some provisions that proclaim conditional rights list restrictively the situations where a limitation is acceptable.
- Other provisions that proclaim conditional rights, as article 8 and 10 of the ECHR related to the right to respect for private life and the right to freedom of expression, hold as a general principle or a "*general public order clause*" that interferences must be "***prescribed by law***", have "***an aim or aims that is or are legitimate***" under the article that declares the conditional right and be "***necessary in a democratic society for the aforesaid aim or aims***".

This public order clause contains therefore three core principles which are:

- the **exclusive competence of the law in limiting freedoms**;
- the **need to pursue one of the legitimate aims listed by the Convention**;
- the "**necessity" of the interference "in a democratic country**", which is interpreted by the European Court of Human Right as implying that the interference, "*in a society that means to remain democratic*"
    - corresponds to a "***pressing social need***"
    - is "***proportionate to the legitimate aim pursued***".

The principle of lawfulness

Any blocking measure, at least within the framework of the ECHR, must be provided for by a law responding to this definition.

- "*the law* must be adequately accessible"
- "a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the *citizen to regulate his conduct*"

Only one kind of agreement that would allow a blocking measure would be the contract between the Internet user and the ISP. The legality of such a blocking measure would depend very much on the type of content being accessed and the nature of the breach and the evidence required. If not specified in a reasonable way, it is easy to envisage such contracts being considered to be in breach of the EU's Unfair Contract Terms Directive, particularly if it allowed the Internet Service Provider to take unilateral punitive action against the consumer.

The principle of a legitimate aim

The Convention on Human Rights and, as regards freedom of expression, the ICCPR, exhaustively lists the legitimate aims in which interference in fundamental freedoms can be legitimate.

A legitimate aim, pursued by the law that permits an Internet blocking measure, is however not sufficient to consider a limitation as legitimate under the European legislation. The measure must also be *necessary* in a democratic country.

As regards the right of private life, the ECHR allows interference (art. 8)

- "*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 or morals*
- *for the protection of the rights and freedoms of others*".

As regards the right to freedom of expression, the ECHR allows interference (art. 10)

- *"in the interests of national security, territorial integrity or public safety*
- *for the prevention of disorder or crime*
- *for the protection of health or morals*
- *for the protection of the reputation or rights of others*
- *for preventing the disclosure of information received in confidence*
- *for maintaining the authority and impartiality of the judiciary".*

As regards the right to freedom of expression, the ICCPR allows interferences (art. 19)

- *"for respect of the rights or reputations of others"*

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

To be legitimate, any blocking measure must therefore pursue one of the interests listed in the text that applies to it, depending on the Convention to which the country is party, and depending on the fundamental freedom the measure is limiting. One of the key issues can be to determine the pursued interest or aim of the measure.

- **Spam blocking**

  The aim of spam blocking is firstly the protection of the rights of the ISP to preserve the existence of its e-mail service, and secondly the protection of the freedom of correspondence of the users of this service. Therefore, the aim of a spam-blocking measure, which can limit the freedom of correspondence and therefore the right for private life, seems to be "*the protection of the rights and freedoms of others*", which *is* a legitimate aim accordingly to article 8 of the ECHR.

- **The aim to protect the interest of the victim**

  One of the aims of a blocking measure targeting illegal content could be the interest of the victim not to be seen within the framework of the scene of a crime. Therefore it fulfils the aim specified above as "*protection of rights of others*", when limiting either the right for private life or the right to freedom of expression. Since not all child pornography includes identifiable information it might not always have a legitimate aim and, due to the technological inadequacy of blocking measures, blocking can, at best, only partially claim to *fully* respect this criterion.

- **The aim of preventing people from seeing illegal content: morals or protection of individuals' sensitivity**

  An Internet blocking measure targeting illegal content in order to prevent people from seeing illegal content thereby protecting morals or protecting the sensibilities of weaker members of society can fit with the "*protection of health or morals"* interest. *If the aim of protecting the sensibilities of weaker citizens can be seen as legitimate,* the links with morals seems on the opposite very weak, especially in Europe, since people usually report illegal content for investigation. In this context, it is also worth remembering (as indicated above) that the vast majority of the material reported is, in fact, not illegal.

- **The aim to prevent crime**

  Another aim of an Internet blocking measure targeting illegal content could be the prevention of crime.

  - Viewing child pornography might cause some persons, who are not paedophiles, to develop such behaviour by regularly viewing illegal child pornography images, although there is very little evidence of this being the case.
  - Internet blocking attempts can disrupt commercial child pornography business and therefore prevent crime, if the business in question has not implemented technology to avoid the blocking system.

- **The aim to repress crime**

  Generally, Internet blocking has not the aim to repress crime, since an Internet blocking measure does not remove the content from the Internet. Internet blocking can always be circumvented and does not facilitate investigations to find producers, distributors or victims.

  Some countries could decide to block people from accessing the internet to sanction a crime or an infringement. This sanction could also drive to crime prevention.

The principle of necessity in a democratic society

The third and final principle contained in the public order clause is the principle of "necessity", which the European Court of Human Rights interprets as implying that an interference in rights and freedoms, "*in a society that means to remain democratic*", corresponds to a "*pressing social need*" and is "*proportionate to the legitimate aim pursued*". The principle of necessity implies therefore two elements: a pressing social need and proportionality between the interference and the legitimate aim pursued.

- **A pressing social need**

  For the European Court of Human Rights, "*the adjective necessary (…) implies the existence of a pressing social need*" and is not "*synonymous with "indispensable", neither has it the flexibility of* such *expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable".* An Internet blocking measure must therefore correspond to a real need of society and the effectiveness of the measure to achieve that needs to be proven.

  Such pressing 'social need' could include:

  - Protecting Intellectual Property Rights
  - Morality and Protecting People from viewing child pornography
  - Protection of victims
  - Prevention of Crime including preventing people from becoming paedophiles, disrupting Child Pornography business model, preventing Child Pornography exchanges
  - Repression of Crime

- **Proportionate to the legitimate aim pursued**

  Interferences caused by Internet blocking to a fundamental freedom have to be proportionate to the aim pursued, in addition to being prescribed by law, in order to pursue one of the *restrictive* aims prescribed by the ECHR and considered as responding to a pressing social need. There are a number of factors in determining where the balance lies in a particular case. One of these factors is "**the overall effect of a particular restriction**". Another factor is to know "**whether there was a sufficient basis for believing that a particular interest was in peril**". The European Court of Human Rights can also assess the proportionality of the "*very behaviour*" which is being restricted.

Internet blocking and proportionality criteria

The analysis of the proportionality of a blocking measure in comparison to the aim it pursues in the light of all the criteria analysed above requires clear demarcation between each measure, based on the aim of that particular measure.

- **Spam blocking**

  Spam blocking is based on the real peril that endangers email services, while the behaviour which is restricted is the right to send emails without respecting rules established to avoid spam. This seems to be a reasonable interference, as regards the danger of not being able to send emails anymore or of losing user confidence in the email service. Finally, it does not seem at that time that a ***less restrictive measure*** could preserve the aims followed by a spam blocking measure.

- **P2P or web blocking <u>in the interest of the IPR industry</u>**

  A web or P2P blocking measure that would serve the interest of the rights owner's would probably have a more negative overall effect.

  - Firstly, if P2P blocking can be shown to lead to the encryption of P2P communications in a way that would prevent any or most content monitoring, it could become almost or fully impossible to monitor those communications even under conditions when it is allowed
  - Secondly, it would imply high costs for the internet industry, the government and the internet users.

  - Thirdly, it will lead to the blocking of legal files

  Regarding the criterion requiring that there is "*a sufficient basis for believing that*" the rights owners interests are "*in peril*", we can say that there is no evidence of such a danger. There is no evidence of the nature and the extent of the possible losses suffered by the rights owners because of P2P or web infringements to their rights, as studies on that issue are insufficient or are proving the opposite result.

- **Web or P2P blocking of illegal content <u>in the aim of protecting the victim's image</u>**

  This proportionality seems acceptable in terms of the "general effect", as long as the blocking measure would not have the effect of blocking other content. Unfortunately, other content would probably be blocked due to the weaknesses of Internet blocking systems and also because a child pornography image can display a crime scene without enabling recognition of the victim

  As regards the "basis for believing that" the victims interest are "in peril", the victims interests might also be served by making people more aware about the crime the victims suffered, to encourage reports to hotlines, and stimulate increased pressure from citizens towards governments to act against such crimes and therefore to improve investigations and investigatory resources.

  The proportionality of the behaviour to access child pornography can be analysed in the light of the interest of the public of identifying such the victim, and will depend on the motivation of each person that will view the content. These motivations could be a desire or willingness to view a crime out of curiosity, which is not appropriate; the desire to know more about the existence of the crime in order to act against it; or the desire to report such images for investigation.

- **Web or P2P blocking of illegal content <u>in the aim of protecting morals</u>, or <u>in the aim of protecting the interests of sensitive people</u>**

  A blocking measure could lead to prevent these persons from accessing uncontroversial content, due to the weaknesses of the technical mechanism. It will furthermore not prevent criminals from such access. As one of the results, the general effect could be a depreciation of the right to freedom of expression, while criminals would still access to immoral or shocking content and people would still be able to access shocking or immoral content of other kinds. Such a situation would not be proportionate.

- **Web or P2P blocking of illegal content <u>in the aim of crime prevention</u>**

  The aim of crime prevention should attempt to prevent people from committing crime or to support crime by buying, downloading or selling illegal content. Its *proportionality* would depend on the percentage of the population who would no longer commit crime as a result of being unable to access illegal content balanced against the restrictions on civil liberties that would be caused by the measure. The effect of the measure could not be a significant reduction of the freedom of expression or the freedom of private life of *every* citizen.

  There is currently no evidence that a blocking measure would lead to reduce this crime, while it would restrict some legitimate and proportionate behaviour.

- **Blocking a person's Internet access <u>in the aim of crime repression and prevention</u>**

  The overall effect of blocking a person in the aim of crime repression and prevention is to prevent this person from accessing the Internet, and sometimes access to telephone and TV services. Such an effect is severe as it completely deprives a person of his freedom of receiving and communicating electronic information and of his freedom to exercise his private and family life, and his freedom to correspond, in the electronic world. It can only be proportionate if it is justified as regards the crime committed and the aim pursued through its repression or indeed its prevention.

Further consequences of the principle of the interference's strict necessity

Additional interferences are enabled by several Internet blocking measures, due to the nature of the mechanisms put in place to implement the blocking. For instance, some spam blocking mechanisms enable an ISP to scan each message sent or received, which allows other interference such as the retention of personal data in relation to a whole message or some words of this content.

The proportionality of each measure which interferes with some freedoms has to be evaluated firstly as regards its stated aim, and secondly as regards its general effect, which must not go beyond what is necessary to reach the pursued aim and, in any cases, must "***leave some scope*** **" for the exercise of the restricted freedom and not "*extinguish*" the freedom**.

Each time an Internet blocking measure is permitted, some guarantees must be implemented to prevent this blocking measure to be used in a way that would further endanger freedoms further than what is necessary to reach the stated aim. This is necessary even if the measure pursues a legitimate aim and its basic function does not block other freedoms in a disproportionate way. The measure can present one of the risks outlined in the first paragraph of this sub-section. These guarantees can be technical, by keeping in check the functionalities that would allow additional freedoms to be endangered, or legal, by prohibiting the additional functionalities or by prohibiting their use, when they are not key to the functioning of the blocking mechanism. A judge must each time be allowed to assess the proportionality of each a specific blocking measure.

The competence of the judge to oversee proportionality of interferences with fundamental freedoms

The European Court of Human Rights oversees the measures taken by the contracting states that interfere with fundamental freedoms and their assessment by national judges. The national courts are also entitled to make a judgment on disputes related to a blocking measure that has been applied to a citizen, or to a content that this citizen would have liked to send, receive or consult.

If having the right to challenge before a court a decision that limited one's freedoms is a fundamental right, it supposes that this limitation has already been put in place and that the citizen had already to suffer from its effects. Therefore, it is essential that a judge can intervene before such a blocking decision is taken. As regards Internet blocking, these situations are related firstly to the assessment and the declaration of the illegality of a content or of an action, and secondly to the appreciation of the proportionality of the response given to the illegal situation.

From above and detailed in **Error! Reference source not found.**, it seems that the only Internet blocking measures that should be allowed without obtaining the decision of a Court of law is *spam blocking* and *blocking on the aim of preserving morals* although the latter implies a range of other legal and practical objections.

Conditions under which Internet blocking could be acceptable

Liberal democracies must respect Fundamental Freedoms and the Court of Human Rights conditions of their limitation. Internet blocking measures can only be implemented correctly if the following steps are observed.

Step 1 Internet blocking would need to be implemented in a way that other rights and freedoms are not violated.

Step 2 Determining rights and freedoms that will be limited

Step 3 Determining the extent of the limitation

Step 4 Determining precisely the pursued aim(s)

Step 5 Establishing if blocking aim corresponds to a reality

Step 6 Determining if blocking in the determined aim answers a pressing social need

Step 7 Analysing the proportionality of the interference to the pursued aim

Step 8 Consider *the principles that must govern blocking in light of the European Court's criteria (necessity in a democratic society, a pressing social need)*

Step 9 Establish if a law is needed to prevent the use of certain functionalities of the blocking mechanism

Step 10 Providing for blocking within law

Studies Required

During the process of analysing the process of balancing fundamental freedoms several studies were identified as needed in order to enable sufficient evaluation of the proportionality requirements. In the absence of this research, proportionality cannot be shown. These include:

- Internet Blocking and Prevention of Paedophilia
- Disrupting Commercial Child Pornography Business Model
- Internet Blocking Reducing Child Pornography Exchanges
- Internet Blocking Protecting Sensitive Persons or Morals
- Internet Blocking Protecting Victims Interests
- Internet Blocking Protecting IPR

1.7 Conclusion

Due to the fundamental impact on our rights to communicate freely, there is an urgent need for society to understand the impact of Internet blocking activities, even if the everyday understanding of Internet blocking, at first, seems clear. There are many well-meaning motivations why society considers the imposition of Internet blocking but the human rights, legal, policy, political and technical issues are very complex. In cases where blocking attempts have been implemented there are often frustrated expectations and confusions surrounding the effectiveness or even the goal(s) of such systems. Internet blocking also has major privacy and security implications for all citizens. This report reviews the meaning of Internet blocking and considers its practical and legal consequences.

The report describes the motivations for attempts at Internet blocking and how other approaches appear to be failing. It reviews who is doing the blocking, what might be blocked, how the blocking can be approached and who would be the target of Internet blocking attempts.

A technical overview of the major Internet blocking systems in use today and how these are applied to different Internet services highlights the increasing range of content and services which are being considered for blocking initiatives. An analysis of the effectiveness of Internet blocking systems highlights the many unanswered questions about the success of these systems and their ability to achieve their stated aims. Nearly all systems have a technical impact on the resilience of the Internet and add an extra layer of complexity onto an already complex network. All Internet blocking systems can be bypassed and sometimes only a small amount of technical knowledge is required to achieve this. There are widely available software solutions on the Internet which assist in evading an Internet blocking measure.

A comprehensive summary of Internet blocking and the law especially relating to human rights, fundamental freedoms and civil liberties creates substantial concerns about the currently implemented blocking systems The legal review includes national and International instruments and considers what fundamental rights are in opposition to Internet blocking and which fundamental rights support Internet blocking. The complexity of balancing rights which are in conflict needs to be assessed by judges, who are trained in managing such complexities.

Internet Service Providers are commercial profit-making entities who are increasingly being asked to implement social policy without appropriate oversight or accountability. They operate in a very confusing situation with regards to competing and sometimes contradictory legal requirements. For example between providing high levels of quality of access to the Internet, on the one hand, and blocking access to services, on the other.

The core issue of balancing fundamental freedoms when different rights are in conflict must undergo detailed analysis mimicking processes adopted by the European Court of Human Rights which indirectly provides guidelines on how Internet blocking measures might be put into operation if deemed appropriate, proportionate and technically feasible. This analysis needs to take into account the strict public order clause and the principles of necessity in a democratic society. These principles are then applied to different Internet blocking initiatives by reviewing the objectives of these initiatives and how they might be judged using the European Court of Human Rights guidelines. The report examines the legitimate aims of the Internet blocking initiatives and questions the validity of some systems in use today.

The technical implementation of Internet blocking measures cannot exist in isolation and must take into account the actual impact on the crime they aim to prevent. They must also consider the accuracy and effectiveness of the blocking measure and clearly identify the negative consequences on *legal* content and *legal* uses of the Internet. The assessment of technological effectiveness needs to be explicitly brought into the evaluation of the balancing of rights.

Many blocking measures are easy to circumvent and are therefore totally ineffective for many of the stated aims. Surprisingly, one of the easiest systems to evade, either intentionally or accidentally, is DNS blocking, which is a system used by many national blocking systems today. It is acknowledged that there are substantial frustrations about the lack of effectiveness of current international cybercrime co-operations and the lack of response by some countries to significant criminal issues including child pornography, hate speech and terrorism. However, rather than throwing our hands up in defeat and resorting to national protectionist strategies we need to improve these International systems and make them effective in the 21st century.

There are very few currently implemented Internet blocking measures which exist as a result of informed public debate held in a transparent and accountable manner. Since, there are complex human rights and legal issues influencing the adoption of Internet blocking services, this report prescribed a sequence of steps to follow in order to evaluate Internet blocking proposals for their legitimacy in a democratic society.

It is strange that illegal content such as child pornography which is widely illegal in many countries, and especially content which is universally condemned and almost universally illegal[7], is allowed to remain online for some Internet users to access and download. It is also strange that private industry and non-elected representatives are empowered and encouraged by governments to implement widespread blocking of content in a non-transparent, non-accountable way. After appropriate research and legal review if blocking is adopted, it is the role of the legislature to clearly specify what can be blocked on the Internet, how it can be blocked and how such systems should be audited and publicly accountable. It is surprising that many EU governments which are unable to directly legislate for Internet blocking continue to encourage and support industry initiatives in this area. Ironically, sometimes the

[7] As of December 2008, 193 countries have ratified the UN Convention on the Rights of the Child including every member of the United Nations except the United States and Somalia. However, even the USA has child pornography legislation in place.

blocking lists in these countries are generated for the Internet blocking activity by state supported organisations without independent auditing of the blocking list.

The key consideration with any Internet blocking measure is proportionality. The measure must have a proportionally more negative effect on illegal content and criminal activities on the Internet than on legal content and legal activities. Such a measure must be provided for by law and needs to be implemented in a way that other rights and freedoms are not violated.

In short, Internet blocking is built on technological solutions which are inadequate in themselves and which are further undermined by the availability of alternative protocols to access and download illegal material. As a result, assessments of proportionality need not just to balance the various rights at stake, they also need to bear in mind the inadequacies of blocking technologies to protect the rights in question and the risks of unintended consequences, such as reduced political pressure for comprehensive solutions and the possibilities of the introduction of new strategies by providers of illegal sites to avoid blocking, which could render law enforcement investigations even more difficult in the future.

The results of the study show that the practical, technical and legal issues surrounding blocking confirm that the issue is not simply a choice "to block or not to block". Countries which have already implemented varying types of blocking mechanism and those planning to do so need to take two concrete actions:

- The fact that blocking is one of the options under consideration is recognition, if not an implicit acceptance, of failures in international cooperation on an issue of fundamental human dignity and protection of the most vulnerable in society (as it relates to child pornography on the Internet).

  Proper analysis of the exact nature of this failure is needed so that it can be better addressed. On the basis of this analysis, all countries should provide formal reports of their efforts to comply with Article 34 of the UN Convention on the Right's of the Child, to be published annually and included in the periodic reports filed under article 44 of that instrument. This would create an incentive for countries to become more active in this field with the consequence of more sites being removed from public access and more children being removed from abusive situations.

- A review of the practical impact (on accidental access, deliberate access, the child pornography "business" and the use of alternative methods of illegal content distribution) is possible and needed, using data from existing blocking systems. Without this review, the proportionality of blocking – and therefore legality under core human right's instruments – remains highly questionable. Failure to undertake such a review creates a long-term question mark over commitment of many countries to key principles of the rule of law.

- Blocking systems need to be implemented through national legislation or otherwise not implemented at all. Self-regulatory blocking systems have inadequate transparency and accountability.