Study

Internet blocking

balancing cybercrime responses in democratic societies

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.

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

Chapter 1 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.

What is Internet Blocking?

[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.

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.

Blocking 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

[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.

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 . 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 7.4

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 recognitiontect echnology 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[7], 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

[7] See above section 6.6 and 6.6.2.

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 Chapter 7 , 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[8], 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

[8] 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.

Chapter 2 SCOPE

This document represents the views of the authors on the subject of Internet Blocking performed by Internet Access Providers around the world. It is based on the combined knowledge and experience of the authors of over the last 30 years in the area of internet, regulation, self-regulation, law, cybercrime, cybercrime investigations, and new technologies.

This review includes Internet blocking systems which are already established in different countries around the world and information has been sourced from these countries.

Chapter 3 reviews the meaning of Internet blocking and considered different understandings of what Internet blocking means.

Chapter 4 covers the motivations why society currently believes that Internet blocking attempts might solve some major societal concerns and how other approaches do not appear to be very successful. 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. It also provides a list of which countries have already adopted Internet blocking systems.

Chapter 5 provides a technical overview of the major Internet blocking systems in use today, explains how these are applied to different Internet services and discusses the impact of these systems and the technical challenges created by these systems. The methods which are used to evade these blocking systems and an analysis of the effectiveness of these systems is included.

Chapter 6 provides an comprehensive overview of Internet Blocking and the Law and provides a review of relevant legal instruments which affect Internet Blocking systems. The key role modern liberal democracies have in their active respect for fundamental freedoms and civil liberties is clearly identified. The review includes national and International instruments and considers what fundamental rights are in opposition to Internet blocking and which fundamental rights support Internet blocking. It also considers the role of Internet Service Providers and the confusing situation they operate with regards to competing and sometimes contradictory legal requirements. This chapter discusses the complexity of these instruments and how they apply to Internet services and Internet blocking initiatives.

Chapter 7 develops the issue of balancing fundamental freedoms when different rights are in conflict and, through an analysis of processes adopted by the European Court of Human Rights, provides guidelines on how Internet blocking measures might be implemented. The development 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 chapter examines the legitimate aims of the Internet blocking initiatives and questions the validity of some systems. The chapter concludes with a sequence of steps which can be followed in order to evaluate Internet blocking proposals for their legitimacy in a democratic society.

2.1 Purpose

The purpose of this study is threefold:

- to stimulate public debate and to encourage more transparency and accountability of the decision-making processes;
- to document the effectiveness of the current solutions and describe alternative solutions;
- to indicate existing or potential collateral damage both in terms of the balance between security and rights as well as in terms of the extension of internet blocking to areas beyond child pornography.

This document is intended to identify the key issues and topics which are important to evaluate Internet Blocking systems as used by Internet Access Providers at a national or international level.

To ensure this study is as objective as possible, the report will be thorough in the analysis of the effectiveness of the current systems and will dedicate substantial space to discussing alternative solutions.

A short review of the different forums which debate the issues and blocking systems and how systems are adopted will also be included.

The objective of this report will be achieved if readers become more aware or more knowledgeable and informed on the complex subject of Internet Blocking systems.

2.2 Foreword

In various countries around the world, and especially in EU Member States, the blocking of child abuse websites is either in place (for example, in the Australia, Canada, Finland, New Zealand, Sweden, United Kingdom et al.) or planned (such as in France, Germany and Ireland).

The blocking list is sometimes prepared by the national hotline/tipline that receives reports of such sites (as in the UK), sometimes by the police (as in Finland, Sweden, Denmark and planned in Belgium), sometimes by an official national body such as the communications regulator (as in Australia) and sometimes by individual companies (such as AOL, etc.)

The current debate highlights the interest of states as well as international organisations in restricting access to certain information. With regard to the differing international legal standards, blocking is seen as an alternative to the more time consuming and sometimes unsuccessful process of international cooperation and cybercrime investigations to remove the content at the source. In this context blocking technology is often used to attempt to re-territorialise the global Internet.

2.3 Outputs

The output of the study is a comprehensive document providing an 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.

This report will reflect on the effectiveness of such blocking systems, their impact on their stated objectives, on online criminal activity and its impact on Internet users. The report will comment on which approach offers better benefits and whether such systems are appropriate or inappropriate in a modern society.

2.4 Fundamental rights and Internet Blocking

From the perspective of democracy, Internet blocking attempts can be problematic on two fundamental levels.

- Firstly and most importantly, Internet blocking appears to have limited effectiveness and it can be counter-productive in dealing with illegal (including child abuse) websites. The danger for democracy is that, since blocking is not completely effective,:
  - i) the necessity/proportionality principles (from ECHR) may be not respected as regard the collateral damages done by the blocking measure to the protection of other freedoms.
  - ii) the dangers exists of enabling governments and Internet Service Providers to promote their achievements on fighting of Child Pornography whilst in fact such contents are still online and this could lead in some cases to a reduction in political pressure to engage in the more difficult task of addressing the sources of the material, through international cooperation. Therefore, it might once more unreasonably restrict other rights and freedoms disproportionately.
- On a second level, it risks being the first step towards:
  - iii) a "normalisation" of ISPs being given (or taking) the role of deciding what consumers may or may not have access to.
  - iv) a broadening of the range of content being blocked and a broadening of the "policing" role of ISPs.

The draft 2009 European Council Declaration (which was not adopted in the end) actually referred, for example, to "identifying and blocking" illegal content. This would have extended the scope of blocking, even in countries that had already implemented such measures.

This comprehensive report is urgently needed in order to show definitively that blocking is far from being the complete solution that it is portrayed as being. It might have the benefits of:

- Reducing the momentum towards blocking that is coming from a wide variety of different sources at the moment;

- Encouraging a public debate on the issues at stake;

- Helping to address the problem of "mission creep" as blocking is increasingly seen as the solution for a wide range of issues, from terrorism and copyright to anorexia;

Blocking is now being either supported and/or discussed currently in the Intergovernmental Forum, the International Telecommunication Union, the Council of Europe, the European Council and individual initiatives such as the COSPOL Internet Related Child Abusive Material Project (CIRCAMP)

2.5 Target Audiences

The target audience of this document is primarily those who are responsible for developing and/or implementing legislation or regulation in the area of Internet Blocking including those who need to consider these issues at a national and international level. These stakeholders include national governments and administrations, politicians, Internet industry including fixed and wireless/mobile, trans-national governmental organisations, child welfare and child

rights organisations, national and international law enforcement, media, Internet users in each country and the general public.

2.6 Excluded from Report

The report will provide an overview comparison of web-blocking technologies with the blocking performed on other internet services such as email, news, etc. in order to provide a better understanding of the issue. However an in-depth analysis of other categories of blocking cannot be done in the time and space available but such complementarily/additional studies could be produced in the future if required.

Chapter 3 WHAT IS INTERNET BLOCKING?

3.1 Overview

If you speak to anyone about their experiences on the Internet, the response is usually very positive, often coupled with amazement about the power and flexibility of the Internet. However, some content and activities on the Internet is illegal as defined by national law and sometimes international treaty.

According to the members of the European Parliament, access to the Internet without interference is simply and entirely an important right. 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 [9].

Some content on the Internet is considered harmful. There are many different responses to harmful content which depends on the target audience and the level of potential harm. Creating a definition of harmful content[10] is a very divisive area and is an area of very active research and debate. Harmful content can only be fully understood with reference to the wider definition of 'risk of harm' which incorporates issues relating to content and types of behaviour when using new communication services (e.g. 'cyber bullying', 'happy slapping'), both online and offline. Harmful content is not the major focus on this report but is mentioned in Chapter 6 relating to legal issues.

In recent years, certain democratic states have promoted the use of Internet blocking technology in relation to various types of subject matter, 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. These cases varied in topic 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 to online media.

This chapter provides a short overview of Internet blocking today. Section 3.2 provides a brief description of what is Internet Blocking and some common misunderstanding relating to Internet Blocking. Section 3.3 explains the different technical systems of identifying content to be blocked on the Internet.

[9] 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.

[10] http://www.coe.int/t/dghl/standardsetting/media/mc-s-is/MC-S-IS%282005%29012_en.pdf

3.2 Internet Blocking

Internet Blocking[11] 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 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 (including requests for web content) 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. The complex range of technology issues are summarized in Chapter 5

Attempting to block Internet content that is legally made available outside the country but is considered to be illegal inside the country could also be anticipated 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. However, false-negatives[12] are a minor inconvenience for most Internet users as the benefit of removing most of the unwanted emails from the Internet outweighs the problems caused by not attempting to block spam.

With different technologies it was later applied to blocking attempts of all types of malware (including viruses, spyware, trojans, etc) and later to illegal content contained in usenet newsgroups.

In recent years, different Internet blocking technologies have been applied with various levels of success in a wide range of networks attempting to block access to or activity in different areas of Internet technologies and services.

Traffic shaping[13] has now become a common aspect of Internet services. This is where Internet Access Providers, especially those involved in the triple-play[14] space, attempt to

[11] Sometimes the word blocking is replaced with filtering.

[12] 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.

[13] Traffic shaping (also known as "packet shaping") is the control of computer network traffic in order to optimize or guarantee performance, lower latency, and/or increase usable bandwidth by delaying packets that meet certain criteria More specifically, traffic shaping is any action on a set of packets (often called a stream or a flow) which imposes additional delay on those packets such that they conform to some predetermined constraint (a contract or traffic profile). [Wikipedia]

actively manage flows of data relating to different services on the public Internet using different priorities and bandwidth.

The extent to which the measures listed above amount to an interference with fundamental human rights and liberties has to be determined by taking into account:

- The inherent characteristics of the measure that might lead to some freedoms being limited
- The inherent characteristics of the measure that could allow further functionalities that would limit freedoms to be implemented, even if the pursued aim is not intended to lead to the implementation and use of such functionalities
- The characteristics and functionalities that are expected from the measure to reach a particular aim

It is important to note that all Internet blocking systems are subject to false-negative and false-positive[15] problems and in advanced systems these are catered for in the design of the blocking technologies in use. For example, in spam blocking, the spam is rarely deleted but is placed in a sub-folder to enable the user to access emails which have been placed there by mistake. Blocked websites using software installed on the user's home computer enables blocking to be bypassed when wrong websites are inadvertently blocked. This level of design is more challenging with Internet blocking systems implemented in Internet Service Providers.

Most Internet Blocking systems which are in use in the home and in business offer local network administrators the ability to fine tune the level of Internet Blocking so that it minimises the false-negatives and false-positives. Unfortunately it is necessary to choose which of these is preferred over the other since it is impossible to remove both completely.

However, such problems can become more pronounced and have greater impact when such 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.

For example, one key difference between blocking a piece of unsolicited e-mail (i.e unrequested content) and blocking a website (i.e. requested content) is that:

- A spam email is inbound to a known email-server and is therefore has one final path available to be delivered directly to the consumer.
- A request for a "blocked" website can take a wide range of paths across the Internet, making the task of blocking the site by the ISP substantially more complex and challenging if the user actually wishes to access that site.

Some systems also prevent outbound content of certain types which is particularly useful for organisations which are very responsive about protecting their reputations from harmful or illegal activity being conducted form their corporate computers by malware or employees – either malevolently or accidentally.

[14] In telecommunications, the triple play service is a marketing term for the provisioning of two bandwidth-intensive services, high-speed Internet access and television, and a less bandwidth-demanding (but more latency-sensitive) service, telephone, over a single broadband connection. Triple play focuses on a combined business model rather than solving technical issues or a common standard.

[15] 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.

3.2.1 Public and Private Blocking

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.

Blocking 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. (Sometimes the system can be tailored to decide the blocking criteria based on identified users).

There is a major difference between blocking systems implemented on a network owned by a school, club or employer and that implemented on a public Internet services.

- The club, school or business has full control over their network. The network configuration, the equipment used and the software installed is decided by the organisation.

  In addition, there is a common philosophy or morality (expressed by the board of the organisation) and a user community which have a common purpose such as being members of the club, employees of the organisations, staff and pupils of the school. Therefore an Internet blocking system can be implemented which attempts to reflect this common ethos.

  Network based filtering has been adopted in businesses and schools for many years. These are environments which lend themselves to easier management and control systems since the complete network environment is under the control of the organisation management team.

- The public Internet Access Provider can only control what equipment is installed and configured on the access network. In a public network there are many different technologies in use which are not under the control of a single network organisation.

  The Internet Access provider usually has no common morality which he can express representing the shared views of the whole population of customers. It ensures that their Internet service, which is a public service, stays neutral6.8.2[16]. The choice of equipment and services adopted by the users of its services, are outside its control. The equipment and users can interact in unpredictable ways. Such users have a range of personal beliefs and share few consistently common traits except perhaps that they belong to the same society.

  Choosing whether content or services should be blocked or what content to block should not be a choice of the Internet Access Provider but that of society which represents the views of these people. In situations where Internet blocking is a path chosen by the Internet Access Provider for a variety of motivations as outlined in Chapter 4 , there are a wide range of technical considerations to review which are outlined in Chapter 5 and a complex array of legal concerns and responsibilities which are outlined in detail in Chapter 6 Chapter 7 explains how a conflict between Freedoms can be mediated and what steps need to be taken to ensure Internet Blocking is compatible with fundamental rights.

[16] See 6.8.2

Voluntary network filtering on a public network has been adopted increasingly in recent years as a service to customers through products and services offering enhanced protection. This protection option is usually deliberately adopted by the customer for specific areas of concern i.e. different types of malware including anti-spam, anti-phishing and anti-virus protection.

Mandatory blocking on the public internet began 20 years ago as a business decision of the organisations concerned and as a benefit to customers and society by enforcing certain types of blocking. The current trend is increasingly towards the blocking of content requested by users, expanding beyond the initial motivation of blocking content (malware, spam, etc).

3.3 Identifying which Content to Block

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

- How do we technically specify what to block?
- Who should choose what should be blocked on the Internet?

3.3.1 How do we technically specify what to block?

The content which is blocked is often contained on a list called a blocking list. After spam and malware blocking, the most common type of Internet blocking is performed on child abuse/child pornography images hosted on websites. The types of content which can be filtered are restricted only by the contents of a blocking list.

It is important that a wide range of issues be debated in order to determine if mandatory internet blocking is the appropriate choice for specific countries

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.

There are many different methods in use to identify which content should be filtered/blocked.

3.3.1.1 Block-Lists

The first most common type involves a "block-list" indicating which content should be blocked. A blocking list can be created which contains the detailed listing of content to be blocked on the Internet.

Some lists which are called "allow lists" indicate age-appropriate/work-appropriate content which can be viewed and blocks anything NOT on this allow list.

This list is often generated and reviewed manually and content checked by trained professionals.

There are many different types of lists and many different methods of generating and distributing these lists. A list containing links to illegal content is a particularly sensitive item and of special value to those who are criminally inclined. Security and confidentiality around the list is of prime importance.

Block lists of child pornography generated by the Australian Communications and Media Authority and generated by the police in Finland have been leaked onto the public Internet, which is a major cause of concern. A single international database of URLs of child pornography/ child abuse images gives rise to significant technical, security, legal and administrative issues.

3.3.1.2 Automated Identification

A second method of identifying content to be blocked involves automatically reviewing the image and/or text and/or video content using sophisticated modern software to determine the probable level of harmful or illegal content contained in the target content.

3.3.1.3 Rating Systems

A third method involves filtering using self-determined or third-party determined rating of Internet content. The content is catalogued (called "rated") using specific and detailed guidelines to determine how much nudity, violence, sex or foul language is contained in the content and then the content is blocked by configuring the system to reject specific categories of content.

It is not necessary to use any one specific software/hardware/network system to implement a blocking list. Different service providers use different technical approaches. Each approach has different levels of effectiveness and usefulness. There are substantial different levels of effectiveness in the different systems and it is important to specify methods to differentiate between the systems in use today.

Some countries prefer an "official" approach where Internet Access Providers only accept notice to block access from the police or another officially appointed state body.

Other States which are currently blocking access to child abuse images hosted abroad, apart from the UK, include Canada, Denmark, Finland, Italy (statutory régime), Norway, Finland and Sweden. The USA, Ireland, the Netherlands and South Korea are in the process of developing Internet blocking systems.

The degree of readiness to comply with a blocking régime (or to implement a statutory régime as in Italy) in other countries which have not yet started to do Internet blocking varies significantly.

3.3.2 Who generates and distributes a Blocking List

A second key issue is to determine what national or international organisation would be considered as having the necessary capability and legitimacy to operate a database intended for use by notice-giving authorities of illegal content.

No single international body currently has a mandate to do so but organisations such as Interpol or Europol are active in this area. Countries which have a formal legislative approach are more likely to agree that a mandate should be given to a body such as Europol rather than to any other voluntary body without statutory authority.

From the comprehensive legal overview in Chapter 6 ,we note that 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 as illegal. This exclusive power, provided for by the domestic legal system, implies that this piece of content, this situation or this action has to be qualified as "potentially" illegal until a judge has been enabled to give a decision on that illegality issue. 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.

Whatever method is used to identify and judge content there is also a debate about the creation of a single internationally shared list of illegal content. Some countries argue that a single international database identifying such content is neither possible nor desirable, in view of the fact that national legislation is not identical. This would mean that a single international database might have significant design challenges to accommodate diverse legislative instruments, languages and interpretations and effectiveness might suffer as a consequence.

The Scandinavian police forces exchange block lists between themselves which are subject to double validation (the receiving police force does a second check whether new content is prima facie illegal under local law). An alternative approach might therefore be an informal system for exchange of block lists between participating notice-giving authorities, as is in Scandinavia.

If a national list is to be shared with countries taking the judicial approach (and vice versa), it is important that a national law enforcement body be involved in the process of sharing outgoing and incoming blocking lists. However, this role needs to be clearly defined depending on each national legal context.

In the absence of a single international database, some organisations use a list generated by a home country without any double validation in the target country. The use of a national list compiled by other governments or by multi-national organisations in other countries other than the home country is fraught with problems and needs to be carefully reviewed. This is in fact more of a legal issue linked to national sovereignty and territoriality than an organisational one. It does signify that a foreign organisation is deciding what the citizens of a country are allowed to see on the Internet. In any case, a blocking list has to be regularly updated to ensure that legal contents are not blocked (which could be the case when the illegal content is moved and replaced by a legal content at the same url).

The International Network of Internet Hotlines (INHOPE) is currently funded by the European Community under the Safer Internet Action Plan. This organisation is in the course of developing a unified database containing URLs of known illegal child pornography. The

purpose of the INHOPE[17] is to fight illegal content and activity on the Internet with a primary focus on Child Pornography. The organisation coordinates a network of hotlines in over thirty countries and each hotline allows Internet users to report illegal content that they accidentally find whilst using 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 constantly increasing. Exact numbers for 2008 have not been published yet. This increase could be due to greater numbers of persons using the Internet or greater numbers of persons reporting illegal content to hotlines or caused by more stricter legislation and not necessarily indicative of an increasing crime rate.

However, a direct consequence of the hotline approach is that Internet users have to experience the consequences of viewing these images before they are reported to a hotline for processing. This can be quite upsetting to most individuals and can be harmful to young adults and minors. More research is needed in this area.

An organisation which implements Internet blocking services using the block list received from the list provider needs to consider which technology will be used to collect, store, implement, update and document the list of content to be filtered.

There are currently no known off-the-shelf systems available which can implement all the necessary functionality for public based Internet Access Providers. Some aspects of this functionality are available in off-the-shelf systems for use in businesses and schools.

The Internet Access Provider needs to purchase, install, configure, secure, document and operate the necessary software and hardware in order to provide these services.

Security and Integrity

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[18]. On 26th May 2005, The Guardian Newspaper[19] in the United Kingdom reported

> *"BT's CleanFeed system, which blocks access to a register of websites containing sexual images of children, can also be used to discover the contents of the secret blacklist, according to new research.*
>
> *Technically skilled users of BT's internet service can use the system to find out which sites are blocked, says Richard Clayton, formerly internet expert at service provider Demon and currently a doctoral student at Cambridge University's Computer Laboratory. This means they are able to gain access to a secret blacklist provided by the watchdog Internet Watch Foundation (IWF).*
>
> *Clayton says CleanFeed can be used as an "oracle" to provide the addresses of IWF-listed sites - effectively turning it into an index of child pornography."*

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.

It does sometimes make 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

[17] http://www.inhope.org
[18] Failures in a Hybrid Content Blocking System by Richard Clayton *www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf*
[19] http://www.guardian.co.uk/technology/2005/may/26/onlinesupplement (last visited 1 September, 2009

feelings of exploitation. Conversely, the content owner can use a different address for the same content or distribute this content on a separate Internet protocol which will make such content accessible again. This is discussed further in Chapter 6.

Internet blocking may disrupt the revenue stream to criminal organisations which operate commercial websites selling images of child abuse for profit making purposes. This is discussed more in Chapter 4 since blocking can also help criminals to stay "one step ahead" by showing them when they've been identified as containing illegal material.

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.

In understanding the context in which Internet Blocking is occurring, it is clear that it can only be part of a broader approach to addressing the availability and access to child pornography online. The other components are law enforcement activity, hotlines for the reporting of child abuse images and education programs.

Nevertheless, various elements work together to provide a complementary set of solutions to tackle the problem of the availability of child pornography accessible online.

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.

However a large volume of content is also located in countries which have world-leading legal, regulatory and criminal investigation systems but yet fail to prevent the distribution of this content on the Internet.

The exact reasons for this are not completely clear. However, this is sometimes attributed to different philosophies surrounding law enforcement objectives and strategies. For example, some law enforcement agencies prioritise the identification, capture and prosecution of child abuse offenders above the prevention of distribution of content or the protection of child victims by the removal of online content. Therefore websites can remain accessible and online for long periods of time before removal. This is especially true in jurisdictions which permit legal undercover entrapment operations. Other Law Enforcement Agencies reverse this prioritisation and seek to remove content and prevent online re-victimisation of the children in the images above the investigation of perpetrators. Even though both strategies seek the same final goal – the

COUNTRY EXAMPLE – UNITED KINGDOM

In the United Kingdom, the Internet Watch Foundation (IWF) filtering list has been used by various IWF members as a basis for server-based-filtering of child abuse images. By the end of 2007, the Home Office intended that all Internet Access Providers "offering broadband internet connectivity to the UK public" will have implemented systems for this. If that target is not achieved, the government reserve the right to t consider legislation.

The UK approach is one where an NGO hotline, which is not part of law enforcement, supplies a list directly to Internet Access Providers which are subscribing members to the IWF as one of the "membership benefits". The IWF approach has been copied and adapted in other jurisdictions (such as Canada). The IWF is also exchanging with some other international organisations where bilateral agreements have been signed.

Some IWF members use the list to filter access for subscribers in other jurisdictions. At least one telecommunications operator uses the IWF list throughout its European network. (They are among ISPs who called for an "EU-wide list".)

British Telecom, UK (BT) actively promotes its url-filtering system usually referred to as BT Cleanfeed (which uses the IWF list) and makes the technology available to other organisations within the UK and world-wide under a non-disclosure agreement. It is not clear how many organisations are using it, in which countries they operate or on what basis they obtain the list of sites to filter.

removal of content AND the prosecution of offenders, the different styles can cause problems on the Internet.

It is important to note the intrusive nature of many of the blocking strategies that were discussed in this chapter. 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'[20] 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 . 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.

In conclusion, 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.

Whereas it is important that a public debate take place, this debate will need to 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.

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.

[20] Refer to Section 7.4

3.4 Basic Terminology

Interception	A court mandated ability to monitor all traffic to and from a specifically targeted suspect.
Take down notice	A notice generated by a knowledgeable and trusted agency to an Internet Service Provider indicating the exact location of content on their servers with reasons why it should be removed for legal reasons.
Child Pornography[21]	(a) "child" shall mean any person below the age of 18 years; (b) "child pornography" shall mean pornographic material that visually depicts or represents: (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i); (c) "computer system" shall mean any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, perform automatic processing of data; (d) "legal person" shall mean any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations.
Child Abuse Images	as above
Content Provider	A content provider is an organisation/user that provides information to an Internet target audience. These can be single individuals which specific knowledge of a particular geographical region, a small group of people with specific interests, or a large corporation with products for sale. With the arrival of Web 2.0 many end-users become content providers in their own right, so the role of content provider needs to be divided into professional content providers such as news organisations, etc., and non-professional content providers such as home users, etc.
Internet Access Provider	Providers of on-demand or dedicated access to the Internet (and to Internet services such as e-mail, News, etc. However, dedicated e-mail providers are not access providers nor news providers. A user can also use an e-mail service not provided by the access provider).
Internet Hosting Provider	Organisations who permit the location of third-party computers to be directly connected to their Internet access point. These organisations often do not manage or operate a network connection directly but take advantage of the network in place at a registered ISP or telecommunications provider.

[21] Definition used from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML

Contact Offender	A person who abuses a child
Illegal Content	Internet content which is clearly specified by law as illegal and declared so by an authorised agency.
Harmful Content	Content which is subjectively felt to cause harm. The level of harm depends on the nature of the content and the physical, emotional and spiritual maturity of the person who see the harmful content.
SPAM	unsolicited emails
URL	Uniform Resource Locator is the name for a string of characters which clearly identifies the protocol, the domain name, the subdomain name, the directory hierarchy, the file name, the file extension type and, if needed, the access information and returned form parameters for a web page to retrieve and display.
DNS (Domain Name System)	A service that translates website names, which usually use alphabetical letters, into number sequences which are known as IP addresses.
IP (Internet Protocol) address	A numeric address that identifies a computer on specific computer network.
ISP (Internet Service Provider)	A company that offers customers internet access.
DDOS (Distributed Denial of Service) attack	A cyber attack that involves sending so many requests to a server that it stops operating under the volume of traffic
Botnet	A collection of computers configured to transmit messages to other computers on command usually for malicious reasons
Malware	Malicious software, designed to infiltrate your computer or damage it or to collect private date without your knowledge
Trojan	a piece of malware that appears to be performing some useful function, while it is in fact infiltrating your computer

Chapter 4 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. This chapter provides an overview about general aspects of the choices at stake. In this context the chapter provides a structured approach to highlight the widely different areas of concern and the challenges faced by policy makers to respond to Internet content problems.

The purpose is to outline the complex range of approaches and motivations towards Internet blocking attempts to enable a comparison between these different approaches.

Section 4.2 discusses where Internet blocking attempts can be done on the Internet. Section 4.3 investigates who chooses what should be blocked and the various levels of knowledge and ability of different users and organisations to block content. Section 4.4 describes the variety of content related issues which occur on the Internet and how some governments have turned to Internet blocking attempts as a possible solution to some of these problems. Section 4.5 outlines the primary motivations which cause policy makers to consider Internet blocking and why in some cases alternative approaches appear to have failed. Section 4.6 looks at the targets of our Internet blocking attempts – either the producers or consumers of illegal content – and describes the effect of blocking attempts on these targets. Section 4.74.8 clearly summarises the conclusions reached from the research conducted on Internet blocking. Finally, section 4.8 briefly lists a range of countries around the world which have already adopted Internet blocking measures.

4.1 Forums where the issue of Internet Blocking is debated

4.1.1 Academia

Blocking is currently intensively discussed within the academic field.22 The discussion is not limited on legal aspects of blocking but covers technical issues as well.23

4.1.2 European Union

The question of ISPs should be obliged to hinder users from up-loading or downloading copyright protected material through file-sharing systems was controversially discussed during the debate about the EU Telecoms reform.24 After criticism of such obligations by the European Parliament25 the Commission decided not to include such obligations in the legislative text presented in November 2008.26 The debate was recently reopened in the debate about new legislative initiatives on e-commerce. In addition the proposal27 for an EU Council Framework Decision on combating child pornography repealing Framework Decision 2004/68/JHA, that was presented in March 2009 by the Commission for example contains an obligation of member states to take the necessary measures to enable the competent judicial or police authorities to order or similarly obtain the blocking of access by internet users to internet pages containing or disseminating child pornography.28

---

[22] *Deibert/Palfrey/Rohozinski/Zittrain,* Access Denied, The Practice and Policy of Global Internet Filtering, 2008; Lonardo, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 et seq.; Sieber/Nolde, Sperrverfuegungen im Internet, 2008; Gercke, The Role of Internet Service Providers in the Fight Against Child Pornography, Computer Law Review International, 2009, page 65 et seq; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide – available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq – available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007 – available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7 – available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch – available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17 – available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement – available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002 – available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf. *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

[23] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 50 et seq.; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 10 et seq.; Pfitzmann/Koepsell/Kriegelstein, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Pursch/Baer*, Sperrverfuegungen gegen Internet-Provider, Deutscher Bundestag, Wissenschaftlicher Dienst, 2009, available at: http://www.ccc.de/press/releases/2009/20090212/bundestag_filter-gutachten.pdf; *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Ayre*, Internet Filtering Options Analysis: An Interim Report, 2006.

[24] *Horten*, The Telcoms Package and „3 strikes" – voluntary cooperation to restrict downloads, 2008.

[25] Vote of the European Parliament on 24th of September 2008.

[26] See the Commissions press release, Telecoms Reform: Commission presents new legislative texts to pave the way for compromise between Parliament and Council, 07.11.2008.

[27] Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2009) 135.

[28] Art. 18 – Blocking access to websites containing child pornography "Each Member State shall take the necessary measures to enable the competent judicial or police authorities to order or similarly obtain the blocking of access by internet users to internet pages containing or disseminating child pornography, subject to adequate safeguards, in particular to ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers are informed of the possibility of challenging it.

4.1.3 Council of Europe

Blocking was intensively discussed within the development of the Council of Europe "Human Rights Guidelines for Internet Service Providers"29 as well as the development of "Recommendations on measures to promote the respect of freedom of expression and information with regard to Internet Filters"30 and remains on the agenda of the Council of Europe.

European Dialogue on Internet Governance 2009 / Internet Governance Forum 2009

Blocking of illegal content was discussed within workshop 4 during the 2009 European Dialogue Internet Governance31 and will be a topic at the 2009 IGF.

[29] Human Rights Guidelines for Internet Service Providers, Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA), 2008.

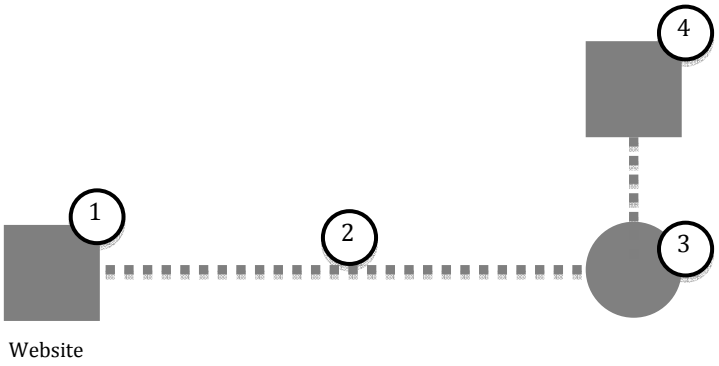
[30] Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, Adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies.

[31] The EuroDIG took place in Geneva from 14th – 15th September 2009.

4.2 Where Internet Blocking can be attempted

A 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
- Content-based approach
- User-based approach
- Search Engine based approach



4.2.1 Service-base approach

Firstly, one of the most popular approaches is the blocking of websites that is especially discussed within the context of blocking of child pornography[32] and is based on targeting Internet services. Since the Internet Access Provider is responsible for forwarding requests from the user to access a website, he is from a technical point of view technically able to check (legal issues are a separate consideration) if the website requested is on a block list. Different technical solutions to ensure that known websites are blocked are currently discussed. They range from a manipulation of the Domain Name Server (DNS) and the use of

[32] Regarding filter obligations/approaches see*:* Lonardo, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 et seq.; Sieber/Nolde, Sperrverfuegungen im Internet, 2008; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide – available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq – available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007 – available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7 – available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch – available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17 – available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement – available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002 – available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf. *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

proxy servers to hybrid solutions that combine various approaches.[33] The detailed technical aspects of these approaches are described in the chapter 5.

4.2.2 Content-based approaches

A second approach is the blocking of certain content during the transfer process. Provided that the user does not send or receive encrypted material, the Internet Access Provider has at least in some cases the technical possibility (legal issues are a separate consideration) to analyse the content transmitted. This approach is unlike service-based approaches mentioned above which are limited to known services that are included on a block-list. Like the Hosting Provider (with regard to uploaded material) the Access Provider could use hash-value based search techniques to search for known child pornography images[34] or a keyword search.[35]

4.2.3 User-based approaches

Thirdly, Internet Access Providers have, to a certain limit, the technical possibility to block customers from using their services. If they add a customer to a block list (legal issues are a separate consideration) he would not be able to use the Internet Access Providers service in the future to commit crimes.

One example for such approach concerning a hosting provider is a case involving the service provider Yahoo! in 2001, when a French court ordered Yahoo! (based in the US) to block the access of French users to Nazi-related material.[36] The user-based approach was controversially discussed (and rejected by both the European Parliament and European Commission during the debate on the EU Telecoms reform.[37] In 2008 France introduced a draft law that would oblige ISP to block users who have been considered of continuing to violate copyrights after repeated written warnings, from using their service.[38] This approach was reportedly criticised by the EU Commission.[39]

4.2.4 Search-engine based approach

A fourth approach discussed within the context of blocking is the establishment of obligations for search engines to not respond to requests related to child pornography (legal issues are a

---

[33] For an overview about the technical aspects see: *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 50 et seq.; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 10 et seq.; Pfitzmann/Koepsell/Kriegelstein, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Pursch/Baer*, Sperrverfuegungen gegen Internet-Provider, Deutscher Bundestag, Wissenschaftlicher Dienst, 2009, available at: http://www.ccc.de/press/releases/2009/20090212/bundestag_filter-gutachten.pdf; *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Ayre*, Internet Filtering Options Analysis: An Interim Report, 2006.

[34] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57; Forsyth/Malik/Fleck/Greenspan/Leung/Belongie/Carson/Bregler, Finding Pictures of Objects in Large Collections of Images, Proceedings of the International Workshop on Object Representation in Computer Vision II, 1996, page 335 et seq.; Pornography Image – Filter Effectiveness, Pinkblock Whitepaper, 2007, available at: http://www.pinkblock.com/downloads/Filter%20Effectiveness%5B1%5D.pdf.

[35] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[36] See *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 et seq.; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 et. seq. Development in the Law, The Law of Media, Harvard Law Review, Vol 120, page1041.

[37] *Horten*, The Telcoms Package and „3 strikes" – voluntary cooperation to restrict downloads, 2008.

[38] See: *Ozimek*, France gets closer to „three strike" downloader web ban, The Register, 12.06.2008, available at: http://www.theregister.co.uk/2008/06/12/france_music_law/.

[39] See: Loi anipiratage sur Internet: les observations de Bruxelles, La Tribune, 27.11.2008, available at: http://www.latribune.fr/entreprises/communication/telecom-internet/20081127trib000314818/loi-antipiratage-sur-internet-les-observations-de-bruxelles-.html.

separate consideration). Search engine providers offer search services to identify documents of interest by specifying certain criteria. The search engine will search for relevant documents that match the criteria entered by the user. Search engines play an import role in the successful development of the Internet. Content that is made available on a website but is not listed in the search engine's index can only be accessed if the person wishing to access it knows the complete URL. *Introna/Nissenbaum* points out that "without much exaggeration one could say that to exist is to be indexed by a search engine".[40]

The obligation not to process requests related to child pornography is therefore at least with regard to the result comparable to technical approaches.

However, if a child pornography website chooses to hide from search engines but is known by those seeking such content the content is still easily accessible.

[40] *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, Page 5. Available at: http://www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf

4.3 Who chooses what needs to blocked?

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. The decision-maker is the person or institution which makes the decision about what should be blocked.

4.3.1 Individual-driven

Individuals can choose to protect themselves or their dependents from self-selected types of content. There are several software-based products available that enable users to restrict access to certain websites and services. Those tools that are often named "parental control instruments" can for example be used to restrict available services on computers used by minors.

The constitutional aspect of approaches characterised as "individual-driven" approach is that the decision about implementing such blocking is undertaken by an individual decision of the affected user or his/her representative. Provided this blocking is voluntary in nature with no external legal pressure applied, such approaches provide the most open, accountable, balanced and effective system. Of course there are concerns about user competency in installing and configuring such software systems.

The conundrum with user managed blocking is that it does not solve the problem of users deliberately seeking illegal content. This document identifies this latter issue as a major concern of any Internet blocking system.

4.3.2 Institution-driven

Within approaches to protect minors, institution-driven approaches are widely implemented. Schools are, for example, using such technology to ensure that students are not able to access certain services that are considered harmful.

Many public libraries also install blocking solutions to protect their customers from all types of illegal or harmful content. In the USA public libraries must use filtering technologies in order to gain US government funding.

Internet-cafes that are often making services available to minors run similar technology. Even outside the child-protection focus such technology is used.

One example is the blocking of non-work-related websites such as popular gambling websites by businesses that want to prevent the use of such services by their employees.[41]

The solutions are not limited to end-user technology. Even ISPs have started to advertise Internet connections that include filter restrictions.[42]

4.3.3 Legislator / Court

A significant number of the recent debates about blocking of child pornography websites are not based on individual or institutional approaches but on mandatory blocking requirements that are either directly established by the law-maker or followed by decisions from courts or other competent state authorities.

---

[41] See in this context for example: Websense Survey on Employees addiction to web, 2008, available at: http://files.shareholder.com/downloads/WBSN/0x0x156252/cdc85544-7f16-410b-90b8-7711faefbc36/WBSN_News_2002_8_21_General.pdf.

[42] See for example: COLT Case Study, COLT Prevents Access to Illegal Web Sites, 2009. See http://www.nominum.com/pdf/case-studies/Colt_CaseStudy_7_30_09.pdf (last visited 1 September, 2009)

As the ability of the law-maker as well a courts and state authorities is limited by constitutional obligations, there were extensive discussions and political momentum about shifting responsibility to institution-driven approaches implemented by organisations which are usually for-profit commercial entities. One such example is the voluntary blocking agreement of several German ISPs that was proposed and promoted by the German Government. As this shifting of responsibility is going along with a circumvention of constitutional limitations such approach creates serious concerns for society.

The voluntary nature of these Internet blocking activities needs to be challenged and discussed due to the level of political pressure as observed in some countries such as the United Kingdom. This political pressure is unexpected and surprising considering the legal problems any government has to mandate such initiatives through law. This is further explained in Chapter 6 . It seems extraordinary that such commercial entities can perform Internet blocking measures when most constitutions prevent the state from mandating such public measures in the first place. When a society believed it necessary, in the past, to implement constitutional limitations on government powers, it is surprising that the state permits and sometimes encourages non-state actors to circumvent such government limitations.

The moral and legal right of Internet access Providers to choose to block selected content without exhibiting bias and prejudice in these decisions needs to be fundamentally questioned. The potential business motivations behind such choices by ISPs should also be considered.

This is particularly true for those profit making organisations which have been awarded the status of "common carrier" in law (no liability for illegal content travelling across their networks without actual knowledge of illegal content).

4.4 What to block?

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. Child pornography is among those categories of content where the content blocked is covered by criminal law provisions. This section provides an overview about some of the most common illegal activities discussed in the context of Internet blocking:

4.4.1 SPAM

Phenomenon

Anti-SPAM is one of the oldest known approaches of blocking Internet traffic. The term "spam" describes the emission of unsolicited messages – sometimes bulk, sometimes commercial.[43] Despite the fact that various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services. In addition spam is frequently used to disseminate malicious software. Since the first spam e-mail was sent in 1978,[44] the tide of spam e-mails has increased dramatically.[45] E-mail provider organisations report that currently as many as 85 to 90 per cent of all e-mails sent are spam.[46] In 2007 the main sources of spam e-mails were: the United States (19.6 per cent of the recorded total); People's Republic of China (8.4 per cent); and the Republic of Korea (6.5 per cent).[47]

Internet Blocking Considerations

Most e-mail providers have responded to rising levels of spam e-mails by installing anti-spam filter technology. This technology identifies spam using keyword filters or black-lists of spammers' IP addresses.[48] Although filter technology continues to develop, spammers in the past have developed approaches to circumvent technical protection systems - for example, by avoiding keywords. Spammers have found many ways to describe "Viagra", one of the most popular products offered in spam, without using the brand-name.[49] With regard to the debate about blocking, the differentiation between two different technical approaches to filter e-mails is of great importance. Filtering can be undertaken on the basis of traffic data analysis as well as on the basis of analysing the content of a message. The differentiation is important since there is a different degree of protection for content and traffic data by national law as well as international legal instruments. Most spam filtering is performed with full customer consent.[50]

---

[43] For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[44] Tempelton, "Reaction to the DEC Spam of 1978", available at: http://www.templetons.com/brad/spamreact.html.

[45] Regarding the development of spam e-mails, see: *Sunner*, "Security Landscape Update 2007", page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[46] The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see http://www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mail, see http://spam-filter-review.toptenreviews.com/spam-statistics.html.
Article in The Sydney Morning Herald, "2006: The year we were spammed a lot", 16 December 2006; http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html, available April 2007.

[47] "2007 Sophos Report on Spam-relaying countries", available at: http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

[48] For more information about the technology used to identify spam e-mails see *Hernan/Cutler/Harris*, Email Spamming Countermeasures: Detection and Prevention of Email Spamming, available at: http://www.ciac.org/ciac/bulletins/i-005c.shtml; For an overview on different approaches see: BIAC ICC Discussion Paper on SPAM, 2004, available at: http://www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf

[49] Lui/Stamm, "Fighting Unicode-Obfuscated Spam", 2007, page 1, available at: http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

[50] Spam blocking based on sending IP address is sometimes performed without direct customer consent. The sending email server receives a rejection notification.

4.4.2 Erotic and Pornographic Material

Phenomenon

Attempted blocking of sex-related material is often considered by policy makers especially within the context of preventing minors from getting access to content that is considered to be harmful. Such blocking attempts can be implemented by software solutions[51] installed on the minor's computer as well as by using Internet access services from a provider that is limiting the access to such material

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;[52]
- Worldwide[53] access, reaching a significantly larger number of customers than retail shops;
- The Internet is often viewed as an anonymous medium (often erroneously[54]) – an aspect that consumers of pornography appreciate, in view of prevailing social opinions. Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time.[55] Besides websites, pornographic material can be distributed through:
    - Exchange using file-sharing systems;[56]
    - Exchange in closed chat-rooms.

Different countries criminalise erotic and pornographic material to different extents.[57] Some countries permit the exchange of pornographic material among adults and limit criminalisation

[51] China was recently reported to implement a mandatory installation of filtering software on any personal computer sold in China. See Heise-News, 08.06.2009, "Bericht: Computer sollen in China nur noch mit Filtersoftware verkauft werden" with reference to a report published by Wall Street Journal.

[52] Depending on the availability of broadband access.

[53] Access is in some countries is limited by filter technology. Regarding filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq ., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement , available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

[54] With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: Chapter 6.2.

[55] *Ropelato*, "Internet Pornography Statistics", available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

[56] About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, "Internet Pornography Statistics", available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

[57] See *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 132 et seq.

to cases where minors access this kind of material[58], seeking to protect minors.[59] Studies indicate that child access to pornographic material might negatively influence their emotional development and well-being.[60] To comply with these laws, "adult verification systems" have been developed.[61] Other countries criminalise any exchange of pornographic material even among adults[62], without focussing on specific groups.

Internet Blocking Considerations

For countries that criminalise access to pornographic material, preventing access is a challenge. Outside the Internet, authorities can refer to existing structures to detect and prosecute violations of the prohibition of pornographic material. On the Internet, however, as pornographic material is often legally made available on servers outside the country, enforcement is difficult. Even where authorities are able to identify websites containing pornographic material, they may have no powers to enforce removal of offensive content by providers.[63] This challenge is a direct consequence of different national standards implemented with regard to the publication of such 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.

[58] One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch): Section 184 Dissemination of Pornographic Writings (1) Whoever, in relation to pornographic writings (Section 11 subsection (3)): 1. offers, gives or makes them accessible to a person under eighteen years of age; […]

[59] Regarding this aspect see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[60] See: *Nowara/Pierschke*, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008.

[61] See *Siebert*, "Protecting Minors on the Internet: An Example from Germany", in "Governing the Internet Freedom and Regulation in the OSCE Region", page 150, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[62] One example is the 2006 Draft Law, "Regulating the protection of Electronic Data and Information and Combating Crimes of Information" (Egypt):

Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

[63] See in this context as well Chapter 6

4.4.3 Child Pornography

Phenomenon

In contrast to differing views on adult pornography, child pornography is universally condemned and offences related to child pornography are widely recognised as criminal acts.[64] Various international organisations are engaged in the fight against online child pornography,[65] with several international legal initiatives including: the 1989 United Nations Convention on the Rights of the Child[66]; the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography[67]; and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, among others.[68]

Despite substantial efforts and costs, those initiatives seeking to control the network distribution of child pornography, have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography. US Research into the behaviour of child pornography offenders shows that 15 per cent of arrested people with Internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80 per cent had pictures of children between 6-12 years on their computer[69]; 19 per cent had pictures of children younger than the age of 3[70]; and 21 per cent had pictures depicting violence.[71]

There is a significant difference in motivations between those who operate commercial child pornography websites and those who operate non-commercial sites. The sale of child pornography can be highly profitable,[72] with collectors willing to pay significant amounts for movies and pictures depicting children in a sexual context.[73] In previous years, search engines could find such material quickly.[74] Often material is exchanged in password-protected closed forums, which normal internet users and law enforcement agencies can rarely access. This creates major problems for investigations and controlled undercover operations that are sometimes vital in the fight against online child pornography.[75]

---

[64] *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 134 et seq.; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[65] See for example the "G8 Communique", Genoa Summit, 2001, available at: http://www.g8.gc.ca/genoa/july-22-01-1-e.asp.

[66] United Nations Convention on the Right of the Child, A/RES/44/25, available at: http://www.hrweb.org/legal/child.html. Regarding the importance for Cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[67] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[68] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

[69] See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[70] See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[71] For more information, see "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[72] See *Walden*, "Computer Crimes and Digital Investigations", page 66.

[73] It is possible to make big profits in a rather short period of time by offering child pornography - this is one way how terrorist cells can finance their activities, without depending on donations.

[74] "Police authorities and search engines forms alliance to beat child pornography", available at: http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/; "Google accused of profiting from child porn", available at: http://www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

[75] See ABA "International Guide to Combating Cybercrime", page 73.

Internet Blocking Considerations

As the national regulation and investigatory processes on the publication of child pornography differed sufficiently it was one of first areas where blocking was intensively discussed as a solution.

Currently the debate about blocking illegal content is very much focusing on child protection.[76]

[76] Regarding the debate see: *Gercke*, Obligations of Internet Service Provider in the Fight Against Child Pornography, Computer Law Review International, 2009, page 65.

4.4.4 Controversial political topics / Hate Speech / Xenophobia

Phenomenon

The discussion about blocking is not limited to content that is widely recognised as criminal in nature. Therefore the debate exclusively about blocking child-pornography is potentially misleading. Blocking attempts are also discussed with regard to content that is less obviously criminal or even widely considered illegal. One example is the debate about blocking of controversial political topics. Some countries such as Germany and Austria 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. Other countries were reported to even going beyond this by trying to block critical comments in the context of political topics.[77]

As the distinction between a (at least in some countries legitimate) criminalisation of illegal politically-related content and suppressing political opinions is difficult, blocking of websites operated by radical (political) organisations is among the most controversially discussed aspects of blocking. Radical groups use mass communication systems such as the Internet to spread propaganda.[78] Recently, the number of websites offering racist content and hate speech has risen[79] - a study in 2005 suggested a rise of 25 per cent in the number of web-pages promoting racial hatred, violence and xenophobia between 2004 and 2005.[80] In 2006, over 6,000 such websites existed on the Internet.[81]

Internet distribution offers several advantages to those who wish to publish such material, including lower distribution costs, non-specialist equipment and a global audience. Examples of incitement to hatred websites include websites presenting instructions on how to build bombs.[82] Besides propaganda, the Internet is used to sell certain goods e.g. Nazi-related items such as flags with symbols, uniforms and books, readily available on auction platforms and specialised web-shops.[83] The Internet is also used to send e-mails and newsletters and distribute video clips and television shows through popular archives such as YouTube.

Not all countries criminalise these offences.[84] In some countries, such content may be protected by principles of freedom of speech.[85] Opinions differ as to how far the principle of freedom of expression applies with regard to certain topics, often hindering international investigations. One example of conflict of laws is the case involving the service provider

---

[77] Heise-News, 02.10.2008, Skype in China filtert und speichert politische Mitteilungen.
[78] Radical groups in the United States recognised the advantages of the Internet for furthering their agenda at an early stage. See *Markoff*, "Some computer conversation is changing human contact", NY-Times, 13.05.1990.
[79] *Sieber*, "Council of Europe Organised Crime Report 2004", page 138.
[80] *Akdeniz*, "Governance of Hate Speech on the Internet in Europe", in "Governing the Internet Freedom and Regulation in the OSCE Region", page 91, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.
[81] See "Digital Terrorism & Hate 2006", available at: http://www.wiesenthal.com.
[82] *Whine*, "Online Propaganda and the Commission of Hate Crime", available at: http://www.osce.org/documents/cio/2004/06/3162_en.pdf
[83] See "ABA International Guide to Combating Cybercrime", page 53.
[84] Regarding the criminalisation in the United States see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: http://www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.
[85] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

Yahoo! in 2001, when a French court ordered Yahoo! (based in the US) to block the access of French users to Nazi-related material.[86] Based on the First Amendment of the United States Constitution, the sale of such material is legal under United States law. Following the First Amendment, a US court decided that the French order was unenforceable against Yahoo! in the United States.[87]

The disparities between countries on these issues were evident during the drafting of the Council of Europe Convention on Cybercrime. The Convention seeks to harmonise cybercrime-related laws to ensure that international investigations are not hindered by conflicts of laws.[88] Not all parties engaged in negotiations could agree on a common position on the criminalisation of the dissemination of xenophobic material, so this entire topic was excluded from the Convention and instead addressed in a separate First Protocol.[89] Otherwise, some countries (including the United States) might have been unable to sign the Convention.

Internet Blocking Considerations

In Europe the context for this debate was opened by the 2000 EU E-Commerce Directive.[90] Faced with the challenges relating to the international dimension of the Internet, the drafters of the Directive decided to develop standards that provide a legal framework for the overall development of the Information Society, and thereby support overall economic development as well as the work of law enforcement agencies. [91] The regulation regarding the liability is based on the principle of graduated responsibility.

The Directive contains a number of provisions that limit the liability of certain providers.[92] . Based on Art. 12, the liability of access providers and router operators is completely excluded as long as they comply with the three conditions defined in that article. In this context Art. 12 paragraph 3 highlights, that the limitation of liability *"shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement."* This clause was for example used by German authorities to order ISP to block access to website containing xenophobic material.[93]

[86] See *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 et seq.; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 et. seq. Development in the Law, The Law of Media, Harvard Law Review, Vol 120, page1041.

[87] See"Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme", 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: http://www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938937961519199 1.

[88] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, 144.

[89] See "Explanatory Report to the First Additional Protocol", No. 4.

[90] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive) see: Pappas, Comparative U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol 31, 2003, pae 325 et seqq., available at: http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf

[91] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[92] Art. 12 – Art. 15 EU E-Commerce Directive.

[93] See in this context. *Mankowski*, Multimedia und Recht, 2002, page 277 ff..; *Stadler*, MMR 2002, 343 ff.

4.4.5 Illegal Gambling

Phenomenon

Although affected by the global financial crisis gambling remains an emerging market, Internet games and gambling are one of the fastest-growing areas in the Internet.[94] Linden Labs, the developer of the online game Second Life[95], reports that some ten million accounts have been registered.[96] Reports show that some such games have been used to commit crimes including[97]:

- Exchange and presentation of child pornography;[98]
- Fraud;[99]
- Gambling in online casinos[100]; and
- Libel (e.g. leaving slanderous or libellous messages).

Some estimates project growth in online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010.[101] (although compared with revenues from traditional gambling, these estimates are still relatively small[102]).

The regulation of gambling over and outside the Internet varies between countries[103] - a loophole that has been exploited by offenders, as well as legal businesses and casinos. The effect of different regulations is evident in Macau. After being returned by Portugal to China in 1999, Macau has become one of the world's biggest gambling destinations. With estimated annual revenues of USD 6.8 billion in 2006, it took the lead from Las Vegas (USD 6.6 billion).[104] Macau's success derives from the fact that gambling is illegal in China[105] and thousands of gamblers travel from Mainland China to Macau to play.

---

[94] Regarding the growing importance of internet gambling see: *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation", available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 et seq, available at: http://www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

[95] http://www.secondlife.com.

[96] The number of accounts published by Linden Lab. See: http://www.secondlife.com/whatis/. Regarding Second Life in general, see *Harkin*, "Get a (second) life", Financial Times, available at: http://www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

[97] Heise News, 15.11.2006, available at: http://www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

[98] BBC News, 09.05.2007 Second Life 'child abuse' claim,, available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm.

[99] *Leapman*, "Second Life world may be haven for terrorists", Sunday Telegraph, 14.05.2007, available at: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml; *Reuters*, "UK panel urges real-life treatment for virtual cash", 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

[100] See *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[101] Christiansen Capital Advisor. See http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

[102] The revenue of United States casinos in 2005 (without Internet gambling) was more than USD 84 billion, from: *Landes*, Layovers And Cargo Ships: "The Prohibition Of Internet Gambling And A Proposed System Of Regulation", page 915, available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

[103] See, for example, GAO, "Internet Gambling - An Overview of the Issues", available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the WTO Proceedings, "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; Article 21.5 panel concluded that the United States had failed to comply with the recommendations and rulings of the DSB.

[104] For more information, see: BBC News, "Tiny Macau overtakes Las Vegas", at: http://news.bbc.co.uk/2/hi/business/6083624.stm.

[105] See Art. 300 China Criminal Code: "Whoever, for the purpose of reaping profits, assembles a crew to engage in gambling, opens a gambling house, or makes an occupation of gambling, is to be sentenced to not more than three years of fixed-term imprisonment, criminal detention, or control, in addition to a fine.

The Internet allows people to circumvent gambling restrictions.[106] Online casinos are widely available, most of which are hosted in countries with liberal laws or no regulations on Internet gambling. Users can open accounts online, transfer money and play games of chance.[107] Online casinos can also be used in money-laundering and activities financing terrorism.[108] If offenders use online casinos within the laying-phase (when bets are placed on the table) that do not keep records or are located in countries without money-laundering legislation, it is difficult for law enforcement agencies to determine the origin of funds.

Internet Blocking Considerations

It is difficult for countries with gambling restrictions to control the use or activities of online casinos. The Internet is undermining some countries' legal restrictions on access by citizens to online gambling.[109] There have been several legislative attempts to prevent participation in online gambling[110]: notably, the US Internet Gambling Prohibition Enforcement Act of 2006 seeks to limit illegal online gambling by prosecuting financial services providers if they carry out settlement of transactions associated with illegal gambling.[111] Attempts to technically block access to such websites are discussed as an additional instrument.[112]

[106] Besides gambling in Macau, Chinese have started to use Internet gambling intensively. See: "Online Gambling challenges China's gambling ban", available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[107] For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

[108] See OSCE Report on Money Laundering Typologies 2000 – 2001, page 3, available at: http://www.oecd.org/dataoecd/29/36/34038090.pdf; *Coates*, Online casinos used to launder cash, available at: http://www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681.

[109] See, for example, "Online Gambling challenges China's gambling ban", available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[110] For an overview of the early United States legislation see: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[111] See § 5367 Internet Gambling Prohibition Enforcement Act.

[112] Italy has introduced obligations to block illegal as well as unlicensed gambling websites. Regarding the industry response see for example: COLT Case Study, COLT Prevents Access to Illegal Web Sites, 2009, available at: http://www.nominum.com/pdf/case-studies/Colt_CaseStudy_2_19_09.pdf; Regarding the gambling legislation in Italy see: Sbordoni/Celesti/Dionisi, Sanctions for Infringements of Gambling Laws in Italy, ERA Forum 2007, 413.

4.4.6 Libel and publication of false information

Phenomenon

The Internet can easily be used to spread misinformation.[113] Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.[114] Minors are increasingly using web forums and social networking sites where such information can be posted as well.[115] Criminal behaviour[116] can include (for example) the publication of intimate photographs or false information about sexual behaviour.[117]

In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID.[118] This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators. These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia,[119] where strict procedures exist for the regulation of content. However, the same technology can also be used by offenders to:

- Publish false information (e.g. about competitors);[120]
- Libel (e.g. leaving slanderous or libellous messages);[121]
- Disclose secret information (e.g. the publication of State secrets or sensitive business information).

It is vital to highlight the increased danger presented by false or misleading information. Defamation can injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience. The moment information is published on the Internet the author(s) often lose control of this information. Even if the information is corrected or deleted shortly after publication, it may already have been duplicated ("mirroring") and made available by people that are unwilling to rescind or remove it. In this case, information may still be available in the Internet, even if it has been removed

---

[113] See *Reder/O'Brien*, Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters, Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, available at http://www.mttlr.org/voleight/Reder.pdf.

[114] Regarding the situation in blogs see*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 et. seq., available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 et seq., available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol 84, 2006, page 1187 et. seq., available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[115] Regarding the privacy concerns related to those social networks see: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available at: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[116] Regarding the controversial discussion about the criminalisation of defamation see: Freedom of Expression, Free Media and Information, Statement of Mr. *McNamara*, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf; Regarding the development of the offence see: Walker, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://www.article19.org/pdfs/standards/definingdefamation.pdf.

[117] See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

[118] With regard to the challenges of investigating offences linked to anonymous services see below: Chapter 3.2.l2.

[119] See: http://www.wikipedia.org

[120] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[121] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

or corrected by the original source.[122] Examples include cases of 'runaway e-mails', where millions of people can receive salacious, misleading or false e-mails about people or organisations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail. Therefore the freedom of speech[123] and protection of the potential victims of libel needs to be well balanced.[124]

Internet Blocking Considerations

Attempting to block such content is often rashly considered as a technical approach to address this issue. However there are substantial legal and technical concerns which need to be addressed which are described in Chapter 5 Chapter 4 , Chapter 6 and Chapter 7 .

[122] Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as http://www.archive.org

[123] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[124] See in this context*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 et. seq., available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 et seq., available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol 84, 2006, page 1187 et. seq., available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

4.4.7 Content published by terrorist organisations

Phenomenon

In the 1990s the discussion about the use of the Internet by terrorist organisations was focusing on network-based attacks against critical infrastructure such as transportation and energy supply ("cyber terrorism") and the use of information technology in armed conflicts ("cyberwarfare").[125] The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorist are possible,[126] but it is difficult to assess the significance of threats[127] and at least up until this decade, the degree of interconnection was small compared to the current status and it is very likely that this – apart from the interest of the states to keep successful attacks confidential – is one of the main reasons why very few such incidents were reported. At least in the past, falling trees therefore posted a greater risk for energy supply than successful hacking attacks.[128]

This situation changed after the 9/11 attacks. An intensive discussion about the use of ICT by terrorists started.[129] This discussion was facilitated by reports[130] that the offenders used the Internet within the preparation of the attack.[131] Although the attacks were not cyber-attacks, as the group that carried out the 9/11 attack did not carry out an Internet-based attack, the Internet played a role within the preparation of the offence.[132] Within this context, different ways in which terrorist organisations use the Internet were discovered.[133] Today it is known that terrorists use ICT and the Internet for various purposes. With regard to the debate about

---

[125] *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.

[126] *Rollins/ Wilson*, "Terrorist Capabilities for Cyberattack", 2007, page 10, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf.

[127] *The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: Rollins/Wilson, "Terrorist Capabilities for Cyberattack, 2007", page 13, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf. However, the FBI has stated that there is presently a lack of capability to mount a significant cyber-terrorism campaign. Regarding the FBI position, see: Nordeste/Carment, "A Framework for Understanding Terrorist Use of the Internet, 2006", available at: http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp*

[128] See: Report of the National Security Telecommunications Advisory Committee - ☐Information Assurance Task Force - ☐Electric Power Risk Assessment, available at: http://www.aci.net/kalliste/electric.htm.

[129] See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Denning*, "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 et seqq., available at: http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, "Cyberterrorism, Are We Under Siege?", American Behavioral Scientist, Vol. 45 page 1033 et seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

[130] See: *Rötzer*, Telepolis News, 4.11.2001, available at: http://www.heise.de/tp/r4/artikel/9/9717/1.html.

[131] The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail see *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

[132] CNN, News, 04.08.2004, available at: http://www.cnn.com/2004/US/08/03/terror.threat/index.html.

[133] For an overview see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.;

blocking, two aspects are from particular interest: The publication of propaganda and the publication of information related to the commission of crimes.

In 1998 only 12 out of the 30 foreign terrorist organisations that are listed by the United States State Department, maintained websites to inform the public about their activities.[134] In 2004 the United States Institute of Peace reported that nearly all terrorist organisations maintained websites – among them Hamas, Hezbollah, PKK and Al Qaida.[135] Terrorists have also started to use video communities (such as YouTube) to distribute video messages and propaganda.[136] The use of websites and other forums are signs of a more professional public relations focus of subversive groups.[137] Websites and other media are used to disseminate propaganda,[138] describe and publish justifications[139] of their activities and to recruit[140] new and contact existing members and donors.[141] Websites have been used to distribute videos of executions.[142]

In addition, the Internet can be used to spread training material such as instructions on how to use weapons and how to select targets. Such material is available on a large scale from online sources.[143] In 2008, Western secret services discovered an Internet server that provided a basis for the exchange of training material as well as communication.[144] Different websites were reported to be operated by terrorist organisations to coordinate activities.[145]

Internet Blocking Considerations

Currently the possibilities to address those challenges are intensively discussed. Criminalising the publication of such material has become an issue. In 2008 the European Union started a discussion about a Draft Amendment of the Framework Decision on Combating Terrorism.[146] In the introduction to the draft amendment, the European Union highlights that the existing legal framework criminalises aiding or abetting and inciting but does not criminalise the dissemination of terrorist expertise through the Internet.[147] With the amendment the European Union is aiming to take measures to close the gap and bring the legislation throughout the European Union closer to the Council of Europe Convention on the Prevention

---

[134] ADL, Terrorism Update 1998, available at: http://www.adl.org/terror/focus/16_focus_a.asp.

[135] *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes see as well: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

[136] Regarding the use of YouTube by terrorist organisations, see Heise News, news from 11.10.2006, available at: http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

[137] *Zanini/Edwards*, "The Networking of Terror in the Information Age", in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

[138] United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

[139] Regarding the justification see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

[140] *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 et. seqq.

[141] See: *Conway*, "Terrorist Use of the Internet and Fighting Back", "Information and Security", 2006, page 16.

[142] Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report, "How Terrorists use the Internet", 2004, page 5.

[143] *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp? In Terrorism and Political Violence, 2008, page 215 et seq.

[144] *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

[145] *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

[146] Draft Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, COM(2007) 650.

[147] "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

of Terrorism. Based on Article 3, paragraph 1 (c)[148] of the Framework, the Member States are for example obliged to criminalise the publication of instructions on how to use explosives, knowing that this information is intended to be used for terrorist-related purposes. Such approach opens the floor for debates about the potential need to block such content in addition to criminalising the publication.[149]

[148] "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

[149] Regarding the blocking issue see: Conway, Terrorism and Internet Governance: Core Issues, ICTs and International Security, Disarmament Forum, 2007, Issue 3, page 26; Franco Frattini, Press release 14.09.2007, "The right to privacy of internet users: let's find a balanced way to ensure both the right to exchange information and public security" says Franco Frattini", available at: http://ec.europa.eu/commission_barroso/frattini/news/archives_2007_en.htm#september.

4.4.8 Copyright Violations

Phenomenon

With the switch from analogue to digital,[150] digitalisation[151] has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and video-tapes.[152]

Digitalisation has also opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalisation, copying a record or a video-tape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy. The most common copyright violations include:

- Upload or exchange[153] of copyright-protected songs, files and software in file-sharing systems;[154]
- The circumvention of Digital Rights Management systems;[155]

File-sharing systems are peer-to-peer[156]-based network services that enable users to share files,[157] often with millions of other users.[158] After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users.

---

[150] Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006", Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

[151] See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

[152] Besides these improvements, digitalisation has speeded up the production of the copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.

[153] In some countries there are exceptions to the prohibition of reproducing protected files, which can make the download not illegal. In France, for instance, copying is not illegal when done for private purposes, and courts of law did not yet really stated if downloading from an illegal matrix was illegal: on this issue see Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux", 4 June 2009, Juriscom.net, page 6, available at: http://www.juriscom.net/uni/visu.php?ID=1133.

[154] *Sieber*, Council of Europe "Organised Crime Report 2004", page 148.

[155] Digital Rights Management describes access control technology used to limit the usage of digital media. For further information, see: *Cunard/Hill/Barlas*, "Current developments in the field of digital rights management", available at: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf. Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

[156] Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking, 2005", available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, "A Survey of Peer-to-Peer Content Distribution Technologies, 2004", available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[157] GAO, File Sharing, "Selected Universities Report Taking Action to Reduce Copyright Infringement", available at: http://www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. United States Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3, available at: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

[158] In 2005, 1.8 million users used Gnutella. See *Mennecke*, "eDonkey2000 Nearly Double the Size of FastTrack", available at: http://www.slyck.com/news.php?story=814.

Peer-to-Peer (P2P) technology plays a vital role in the Internet. Currently, over 50 per cent of consumer Internet traffic is generated by peer-to-peer networks.[159] The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in file-sharing systems,[160] with other OECD countries showing similar trends.[161] Of course, some music or protected files exchanged on P2P protocols are (i) offered by the artist himself (emerging or not) or (ii) sold by the producer on this protocol. In consequence some such downloads/uploads are compliant with the law. File-sharing systems can be used to exchange any kind of computer data, including music, movies and software.[162] Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.[163]

The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time.[164] First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network.[165] Unlike first-generation systems (especially the famous service Napster), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users.[166] The decentralised concept of second-generation file-sharing networks makes it more difficult to prevent them from operating. However, due to direct communications, it is possible to trace users of a network by their IP-address.[167] Law enforcement agencies have had some success investigating copyright violations in file-sharing systems. More recent versions of file-sharing systems enable forms of anonymous communication and easy encryption and will make investigations more difficult.[168]

---

[159] See Cisco "Global IP Traffic Forecast and Methodology", 2006-2011, 2007, page 4, available at: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

[160] See: "OECD Information Technology Outlook 2004", page 192, available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf.

[161] One example is Germany, where a regularly updated report of the Federation of the phonographic businesses pointed out that, in 2006, 5.1 million users in Germany downloaded music in file-sharing systems. The report is available at: http://www.ifpi.de/wirtschaft/brennerstudie2007.pdf. Regarding the United States see: *Johnson/McGuire/Willey*, "Why File-Sharing Networks Are Dangerous", 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[162] Apart from music, videos and software, even sensitive personal documents are often found in file-sharing systems. See: *Johnson/McGuire/Willey*, "Why File-Sharing Networks Are Dangerous", 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[163] While in 2002, music files made up more than 60% of all files exchanged in file-sharing systems in OECD countries, this proportion dropped in 2003 to less than 50%. See: "OECD Information Technology Outlook 2004", page 192, available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf.

[164] *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking", 2005, page 11, available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Cope, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: http://www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[165] Regarding Napster and the legal response see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html. *Penn*, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

[166] Regarding the underlying technology see: *Fischer*, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: http://www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf; *Sifferd*, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; Herndon, Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children, Oklahoma Journal of Law and Technology, Vol. 12, 2004, available at: http://www.okjolt.org/pdf/2004okjoltrev12.pdf; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[167] For more information on investigations in peer-to-peer networks, see: "Investigations Involving the Internet and Computer Networks", NIJ Special Report, 2007, page 49 et seqq., available at: http://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

[168] Clarke/Sandberg/Wiley/Hong, "Freenet: a distributed anonymous information storage and retrieval system", 2001; Chothia/Chatzikokolakis, "A Survey of Anonymous Peer-to-Peer File-Sharing", available at:

File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses.[169] Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorised copies or artwork within the public domain.[170]

Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry.[171] It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems. Research has identified millions of file-sharing users[172] and billions of downloaded files.[173] Any revenue decrease could come from other factors like the diversification of medias and supports, while file sharing could generate other revenues such as concert ticket purchase or additional products (T shirt, games, videos etc..) Copies of movies have appeared in file-sharing systems before they were officially released in cinemas[174] at the cost of copyright-holders. The recent development of anonymous/encrypted file-sharing systems will make the work of copyright-holders more difficult, as well as law enforcement agencies.[175]

Internet Blocking Considerations

While international legal approaches are focusing on the criminalisation of copyright violations on a "commercial scale", the discussion concerning national approaches is broader and includes hindering users that are involved in online copyright violations from accessing the Internet. This approach was controversially discussed during the debate on the EU Telecoms reform[176] and rejected by the European Parliament[177] and European Commission in first reading.[178] In 2008, France introduced a draft law that would oblige ISP to block users that have been repeatedly accused of breaching copyrights from using their service.[179] This approach was reported to be criticised by the EU Commission.[180]

---

http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Han/Liu/Xiao;Xiao, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

[169] Regarding the motivation of users of peer-to-peer technology see: *Belzley*, Grokster and Efficiency in Music, Virginia Journal of Law and Technology, Vol. 10, Issue 10, 2005, available at: http://www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

[170] For more examples, see: Supreme Court of the United States, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, I. B., available at: http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

[171] Regarding the economic impact, see: *Liebowitz*, "File-Sharing: Creative Destruction or Just Plain Destruction", Journal of Law and Economics, 2006, Volume 49, page 1 et seqq.

[172] The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

[173] "The Recording Industry 2006 Privacy Report", page 4, available at: http://www.ifpi.org/content/library/piracy-report2006.pdf.

[174] One example is the movie, "Star Wars – Episode 3", that appeared in file-sharing systems hours before the official premiere. See: http://www.heise.de/newsticker/meldung/59762 that is taking regard to a MPAA press release.

[175] Regarding anonymous file-sharing systems, see: *Wiley/ Hong*, "Freenet: A distributed anonymous information storage and retrieval system", in Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability, 2000.

[176] *Horten*, The Telcoms Package and „3 strikes" – voluntary cooperation to restrict downloads, 2008.

[177] Vote of the European Parliament on 24th of September 2008.

[178] See the Commissions press release, Telecoms Reform: Commission presents new legislative texts to pave the way for compromise between Parliament and Council, 07.11.2008.

[179] See: *Ozimek*, France gets closer to „three strike" downloader web ban, The Register, 12.06.2008, available at: http://www.theregister.co.uk/2008/06/12/france_music_law/.

[180] See: Loi anipiratage sur Internet: les observations de Bruxelles, La Tribune, 27.11.2008, available at: http://www.latribune.fr/entreprises/communication/telecom-internet/20081127trib000314818/loi-antipiratage-sur-internet-les-observations-de-bruxelles-.html.

4.5 Why consider Internet Blocking?

The motivations for Internet blocking emphasise that Internet blocking is often used to respond to technical and legal challenges. This section gives an overview about some of the global motivations discussed in the context of blocking.

4.5.1 Missing Control Instruments

Most mass communication networks - from phone networks used for voice phone calls to the Internet - need central administration and technical standards to ensure operability. The ongoing discussions about Internet governance might suggest to the beginner that the Internet is no different compared with national and even transnational communication infrastructure.[181] The Internet also needs to be governed by laws and law-makers and law enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

The Internet was originally designed as a defence-funded network[182] based on a decentralised network architecture that sought to preserve the main functionality intact and in power, even when components of the network were attacked. As a result, the Internet's network infrastructure is resistant to external attempts at control. It was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network.

Today, the Internet is increasingly used for civil services. With the shift from defence to civil services, the nature of demand for control instruments has changed. Since the network is based on protocols designed for defence purposes, these central control instruments are limited or do not exist and it is difficult to implement them retrospectively, without significant redesign of the network. The absence of control instruments makes cybercrime investigations very difficult.[183]

Blocking attempts could be considered as an approach to implement such control instrument that was not foreseen when the network was developed

4.5.2 International Dimension

Many data transfer processes affect more than one country.[184] The protocols used for Internet data transfers are based on routing policies unique for each service provider and dynamically overcome obstacles if direct links are temporarily blocked.[185] Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to its final destination.[186] Further, many Internet services are based on services from abroad[187] e.g.,

---

[181] See for example, *Sadowsky/Zambrano/Dandjinou*, "Internet Governance: A Discussion Document", 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf;

[182] For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; lynch, Postel, Roberts, Wolff*, "A Brief History of the Internet", available at: http://www.isoc.org/internet/history/brief.shtml.

[183] *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[184] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[185] The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: *Tanebaum*, Computer Networks; *Comer*, "Internetworking with TCP/IP – Principles, Protocols and Architecture".

[186] See *Kahn/Lukasik*, "Fighting Cyber Crime and Terrorism: The Role of Technology," presentation at the Stanford Conference, December 1999, page 6 et seqq.; *Sofaer/Goodman*," Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[187] One example of the international cooperation of companies and the delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system

host providers may offer webspace for rent in one country based on hardware in another.[188] To make content available does not require the use of hosting services in the country an offender is acting from.

If offenders store information on servers outside the home country, cybercrime investigations need the cooperation of law enforcement agencies in all countries affected.[189] National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities.[190] International cooperation based on principles of traditional mutual legal assistance is very time consuming. The formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations.[191] Investigations often occur in very short timeframes.[192] Data that is vital for tracing offences is often deleted after only a short time. This short investigation period is problematic, because traditional mutual legal assistance regime often takes time to organise.[193]

Blocking attempts might therefore be considered as an approach to act even in those cases where the limitations of international cooperation prevent measures to be taken in a timely manner. However, blocking does not facilitate obtaining data on crime nor to find the criminal either.

4.5.3 Decreasing importance of national hosting infrastructure

It is not only the time element that leads to difficulties when it comes to illegal content. The principle of dual criminality[194] also poses difficulties if the offence is not criminalised in one of the countries involved in the investigation.[195] Offenders may be deliberately including multiple countries in their attacks to make investigation more difficult.[196] For example, if they store illegal content on servers based in a country that does not criminalise such publication, legal attempts to remove information at its source might turn out to be unsuccessful.

---

mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, Page 429 et seq. (with notes *Sieber)*.

[188] See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplyfing Data Storage and Management.

[189] Regarding the need for international cooperation in the fight against Cybercrime, see: *Putnam/Elliott,* "International Responses to Cyber Crime", in Sofaer/Goodman, " Transnational Dimension of Cyber Crime and Terrorism", 2001, page 35 et seqq., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 1 et seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

[190] National Sovereignty is a fundamental principle in International Law. See *Roth*, "State Sovereignty, International Legality, and Moral Disagreement", 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[191] See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf;

[192] See below: Chapter 3.2.10.

[193] See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142.

[194] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

[195] Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

[196] See: *Lewis*, "Computer Espionage, Titan Rain and China", page 1, available at: http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

As pointed out previously, the publication of illegal content does not require the use of hosting services in the country an offender is acting from.

Especially with regard to illegal content the extent of criminalisation differs. 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.

4.5.4 Evaluation of the challenges in the context of blocking

The fact, that it is possible to store content outside a country that criminalises the publication of such material without affecting the ability of people inside that country to get access to such information is possibly one of the main reasons why blocking is taken into consideration.

4.6 Who to block?

The intention of Internet blocking attempts varies significantly. The variety of purposes is mainly a result of the great variety of types of content discussed within the debate about blocking.[197] This section focuses on the intention of blocking child pornography.

In this context it is in general possible to divide between two different focus of approaches – the content provider (producer) and the user (consumer).

4.6.1 The Producer of Illegal content – the illegal content provider

Background

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. [198] In a analogous way, the modern digital camera and digital camcorder have become the major tool for the ***production*** of child pornography.

- Creating a website with child pornography images enables the content to be available to anyone who has access to the global Internet. This increases the potential number of consumers compared to approaches based on the traditional physical exchange of child pornography.[199]

- The publication of illegal content does not require the use of hosting services in the country an offender is acting from. This is a substantial challenge for law enforcement agencies with regard to the removal of the content.

Debate about solutions

Attempting to block Internet services that are used to exchange child pornography is therefore discussed as a solution to prevent the use of such services in the exchange of child pornography.[200] The objective to implement blocking technology is therefore similar to the

---

[197] Regarding the different types of content see above: Section 4.4

[198] *Krone*, "A Typology of Online Child Pornography Offending", Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB; *Eneman*, A Critical Study of ISP Filtering of Child Pornography, 2006, available at: http://is2.lse.ac.uk/asp/aspecis/20060154.pdf; *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 32 et seq.

[199] Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, ref. 259.

[200] Regarding the overall debate see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 et seq.; Sieber/Nolde, Sperrverfuegungen im Internet, 2008; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide – available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq – available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007 – available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7 – available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch – available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17 – available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement – available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002 – available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf. *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

objective to criminalise the exchange of child pornography i.e. to reduce the volume of crime and to protect children. Within the current debate about blocking, the discussion is very much focusing on blocking of access to websites. Several technical solutions are taken into consideration to prevent users from accessing a website that contains child pornography.[201] Many of these approaches are based on block-lists that contain known child pornography websites.[202]

Child pornography is one of the very few categories of content that is widely considered as illegal and is criminalised in most countries.[203] On first sight the existence of websites containing child pornography is therefore surprising – especially because the existence of block-lists highlights that such websites have already come to the attention of law enforcement agencies.

There are four main reasons for the difficulties in removing the content.

No Central Authority
The Internet is based on a decentralised concept.[204] Unlike in centralised networks the Internet knows very few central control institutions.[205] Those institutions that exist such as the Internet Corporation for Assigned Names and Numbers (ICANN, the central internet addressing body) have very limited power when it comes to taking measures against illegal content including the exchange of child pornography via Internet-services.

National Sovereignty
The principle of national sovereignty[206] limits the ability of law enforcement agencies to directly react and order the removal of websites containing child pornography if the website is physically stored outside the territory.[207] In this case the law enforcement authorities need to start an investigation and make use of instruments of international cooperation to be able to initiate the process of removing such content. Due to formal requirements international cooperation can be a very time consuming process.[208] Attempting to block users from accessing child pornography websites that can not be removed in a timely manner is therefore a **response to the difficulties with regard to international cooperation**.

---

[201] See above: Section 5.3.2
[202] See above: 5.2.1
[203] *Akdeniz* in *Edwards / Waelde*, "Law and the Internet: Regulating Cyberspace"; *Williams* in *Miller*, "Encyclopaedia of Criminology", Page 7. Regarding the extend of criminalisation, see: "Child Pornography: Model Legislation & Global Review", 2006, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalisation of child pornography and Freedom of Speech in the United States see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.
[204] For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; lynch, Postel, Roberts, Wolff*, "A Brief History of the Internet", available at: http://www.isoc.org/internet/history/brief.shtml.
[205] Regarding the related challenges for Cybercrime investigations in general see: *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 38 et seq.
[206] National Sovereignty is a fundamental principle in International Law. See *Martinez*, National Sovereignty and International Organizations, 1996; *Sieghart*, The International Law of Human Rights, 1984, page 11 et seq. *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.
[207] *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 38 et seq.
[208] The need to speed up the process of international cooperation is pointed out in the Explanatory Report to the Convention on Cybercrime. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

Within the debate about blocking there were tests undertaken to prove that, since the content could be rather easily removed, Internet blocking is not required. After block-lists leaked there were different tests undertaken to contact those hosting providers whose services were used to store child pornography websites seeking for the removal of the illegal content. In a high number of cases the content was immediately removed.

While this example highlights the potential for improvement of the timeliness of removal procedures (e.g. faster processing of notifications from trusted countries would help) **it does not prove on its own that there are faster means** to remove the content that would make blocking attempts unnecessary. Unlike private expert and civil liberty groups, law enforcement agencies are generally not permitted to directly contact businesses based outside their territory to seek the removal of illegal content. The principle of national sovereignty[209] hinders them for undertaking such direct approach. In addition such uncoordinated interventions could interfere with ongoing investigations.

Degrees of Criminalisation
Despite the fact that there is a global consensus that child pornography is illegal, there are significant differences in the degree of criminalisation. While some countries criminalise real child pornography as well as virtual child pornography[210] other limit the criminalisation to material that show the real abuse of children. Some countries consider an actor to be a child if the actor meets certain criteria used to identify a minor while other countries require the identification of the victim to prosecute a perpetrator. These national differences can seriously hinder approaches to remove content within international investigations.

Legal Entrapment
Law enforcement agencies are reported to have maintained websites with child pornography online to use them as what is called a "honey-pot" attracting suspects that are trying to download child pornography. (Usually the images are corrupted or not actually illegal which is only discovered once a user has registered for a website advertising child pornography.)

The difficulties in enforcing the removal of illegal content stored outside the country highlights the increasing demand for technical solutions attempting to prevent access to such material during the time-consuming and not always successful process of removing the content at its source. Trends towards decentralised storage ("cloud storage") will very likely increase the challenges of removing the content in time as the importance of the physical location where the content is stored decreases.[211]

[209] National Sovereignty is a fundamental principle in International Law. See *Martinez*, National Sovereignty and International Organizations, 1996; *Sieghart*, The International Law of Human Rights, 1984, page 11 et seq. *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[210] Regarding the criminalisation of virtual child pornography see: *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 134 et seq.

[211] Regarding the aspect of jurisdiction in cloud computing cases see: *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009, abrufbar unter: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf.

4.6.2 The consumer - the Internet user

Background

In addition to the production, publication and making available of child pornography a significant number of countries criminalise the possession of child pornography.[212] The demand for such material could promote their production on an ongoing basis.[213] In addition the possession of such material could encourage the sexual abuse of children, so policy makers suggest that one effective way to curtail the production of child pornography is to make ***possession*** illegal.[214] An example is Art. 10 of the Convention on Cybercrime. However, the Convention enables the parties in Paragraph 4 to exclude the criminalisation of mere possession, by restricting criminal liability to the production, offer and distribution of child pornography only.[215]

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. One example is Art. 20, paragraph 1f, of the Council of Europe Convention on the Protection of Children. It criminalises the act of obtaining access to child pornography through a computer. This enables law enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography but they are unable to prove that the offender downloaded material. Such difficulties in collecting evidence do for example arise if the offender is using encryption technology to protected downloaded files on his storage media.[216] The Explanatory Report to the Convention on the Protection of children points out that the provision should also be applicable in cases, where the offender does only watch child pornography pictures online without downloading them.[217] In general opening a website does automatically initiate a download process – often without the knowledge of the user.[218] The case mentioned in the Explanatory Report is therefore only relevant in those cases where a download in the background is not taking place.

Investigating in those cases goes along with several challenges.

- Very often data that is necessary to identify a connection which has been used to download child pornography is shortly deleted after use. This is especially relevant with regard to IP addresses. The implementation of data retention obligations (for example by the EU Directive on Data Retention[219]) only partly solved this problem.[220]

---

[212] Regarding the criminalisation of the possession of child pornography in Australia, see: *Krone*, "Does thinking make it so? Defining online child pornography possession offences" in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

[213] See: "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[214] Explanatory Report to the Council of Europe Convention on Cybercrime No. 98.

[215] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[216] Regarding the challenges related to the use of encryption technology see above: Chapter 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[217] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[218] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser the information can be downloaded to cache and temp files or are just stored in the RAM memory of the computer. Regarding the forensic aspects of this download see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[219] 2005/0182/COD.

[220] The fact that key information about any communication on the Internet will be covered by the Directive has lead to intensive criticism from human rights organisations ([220] See for example: Briefing for the Members of the European Parliament on Data Retention, available at: http://www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to

- The availability of anonymous communication services enables offenders to hide their identity and make investigations more challenging for law enforcement agencies.

data retention continues to grow, available at: http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf; Regarding the concerns related to a violation of the European Convention on Human Rights see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et seq.)

4.6.3 Summary

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).

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 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.

With regard to the intention to make content unavailable to users the main arguments against blocking is the missing removal of the content at its source and the possibility to circumvent the technology. These aspects have several implications:

- The content can still be accessed by using connections that do not block access. This enables users from countries without blocking obligations to access the services used to distribute child pornography. The availability of such services might even still be possible from countries that do generally require the blocking of content as obligations to implement blocking technology are often limited to service providers with a certain number of clients. An example is Sec. 2 of the German Law that implemented blocking obligations for Internet Service Provider with a minimum of 10.000 clients.[221] In addition, different technologies have different levels of effectiveness so some users might unknowingly bypass simpler blocking systems.

- 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 those blocking approaches that are recently discussed can be circumvented. Using anonymous communication service or secure encrypted links using https connections can already circumvent some of the control instruments currently discussed. Within the national debates about blocking instructions were frequently published detailing how to circumvent blocking approaches.

- 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.

- Internet websites are just one service used to exchange child pornography. The recent technical approaches are very much focusing on web services. Exchange of child pornography via file-sharing systems or encrypted e-mail exchange are not covered by the approach.

[221] Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz – ZugErschwG) - § 2 (1) (1)Diensteanbieter nach § 8 des Telemediengesetzes, die den Zugang zur Nutzung von Informationen über ein Kommunikationsnetz fur mindestens 10 000 Teilnehmer oder sonstige Nutzungsberechtigte ermöglichen, haben geeignete und zumutbare technische Maßnahmen zu ergreifen, um den Zugang zu Telemedienangeboten, die in der Sperrliste aufgefu□hrt sind, zu erschweren.

4.7 Conclusions

- It is likely that in the current situation a time gap between the identification of illegal content and the removal will remain. If blocking attempts can be made to technically work efficiently and effectively, it is therefore a possible approach to address this particular issue – depending on its proportionality.

- With regard to the fact that blocking does not remove the content, **blocking can not be considered as an instrument to prevent the act of making illegal content available** online by the content provider but it is a possible technical solution to prevent users from (accidentally) committing an offence by accessing a website with child pornography.

- The **current blocking approaches are only addressing web-services**. Other services are not included. Difficulties could not result from current approaches but also from an increasing use of anonymous hosting through networks like The Onion Router (TOR). If the aim of the instrument is to block serious criminals the instrument is not sufficient and will in the future likely be even less effective.

- Blocking is not the only possible solution to reduce the time gap between identification and removal. Another approach could be to **improve the means of international cooperation** in order to narrow the time gap between the identification of illegal content stored abroad an the removal.

- Taking into account the ease in circumventing the currently discussed instruments highlights that the instruments are not a sufficient approach to prevent serious criminals from getting access to such material. This leads to one main conclusion which is that **Blocking content can not substitute the removal of such content** as only the removal of content can hinder serious offenders from getting access to it. As a consequence, the main target of such technology cannot be serious criminals but people that are less experienced in circumventing blocking technology. A likely aim of the technology is therefore to **prevent accidental access** to such material.

- One issue raised within this discussion about blocking content to prevent unintentional access is the fact, that the fact that such material is not **visible anymore might mislead the political debate** as it could lead to the impression that the problem of child pornography being available online was solved.

- Successfully blocking child pornography does not identify the victims in those images nor remove the victims from the abusive situation. Investigations must proceed with those images to insure that such steps are successfully achieved. Successfully blocking of those images which clearly show victims which have already been identified and are in care or recovery would prevent ongoing re-victimisation for those victims.

- In addition to the above mentioned systematic limitation of blocking approaches technical and legal concerns need to be taken into consideration.

4.8 Country Examples

Several European countries such as Finland, Norway[222], Sweden[223], Switzerland[224] United Kingdom[225] and Italy[226] as well as non European countries such as Australia[227], China[228], Iran[229] and Thailand[230] use such an approach. 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.[231] At the moment tests with some ISPs are running. Telstra, Australia's largest ISP, announced it will not join trials of filtering.[232]

In the UK the block-list is generated by IWF (Internet Watch Foundation).[233] The technology used is BT Cleanfeed.[234] In Denmark the block-list is generated by National High Tech Crime Centre of the Danish National Police and Save the Children Denmark.[235] The 3 largest ISPs participate. 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.[236]

---

[222] „Telenor Norge: TelAuenor and KRIPOS introduce Internet child pornography Filter." Telenor Press Release, 21 Sep 2004; Clayton, Failures in a Hybrid Content Blocking System in: Privacy Enhancing Technologies, 2006, page 79; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 46 et seq.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, page 3.

[223] Swedish Providers are using a tool called „Netclean". See Netclean Pro Active, available at: http://www.netclean.com/documents/NetClean_ProActive_Information_Sheet_EN.pdf; Telenor and Swedish National Criminal Investigation Department to introduce Internet child porn filter, Telenor Press Release, 17 May 2005, available at: http://press.telenor.com/PR/200505/994781_5.html; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 59 et seq.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, page 3; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, page 6.

[224] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55; Schwarzenegger, Sperrverfuegungen gegen Access-Provider in: Arter/Joerg, Internet-Recht und Electronic Commerce Law, page 250.

[225] *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, page 4; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 64 et seq.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, page 3; *Eneman*, A Critical Study of ISP Filtering of Child Pornography, 2006, available at: http://is2.lse.ac.uk/asp/aspecis/20060154.pdf.

[226] *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 et seq.; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, page 6 et seq.; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 54.

[227] Regarding the filtering approaches see: Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety, ACMA, 2008.

[228] *Clayton/Murdoch/*Watson, Ignoring the Great Firewall of China, available at: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73;

[229] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[230] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55

[231] Regarding the filtering approaches see: Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety, ACMA, 2008.

[232] http://www.itu.int/osg/blog/2008/12/12/NetFirmsRebuffFilteringPlan.aspx.

[233] *Stol/Kaspersen/Kerstens/Leukfeldt/Lobber*, Governmental filtering of websites: The Dutch case, Computer Law & Security Review 2009, page 251.

[234] *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, page 55, at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf;

[235] *Regarding* filtering in Denmark see: York, Secret Censorship in Denmark, 2008, available at: http://opennet.net/blog/2008/12/secret-censorship-denmark.

[236] Ricknäs, Europe *makes* moves towards Internet censorship, 2008, available at: http://www.infoworld.com/d/security-central/europe-makes-moves-toward-internet-censorship-622.

Chapter 5 TECHNICAL ASPECTS OF INTERNET BLOCKING

5.1 Introduction

The development and implementation of various types of Internet blocking technology on the internet is not a recent development. Spam, internet-based viruses and malware and many other content-types that are unwanted and unrequested by the end-user have become targets in 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.

Initially, pressure for Internet blocking came primarily from users and industry. State involvement was, at first, limited to the courts in cases of unjustified or excessive blocking. An excellent recent example of this is the Spamhaus vs. e360 case that was started by an American company apparently to harass their spam blocking counterparts in the ongoing filter wars in the spam domain, by involving Spamhaus in a US civil court case.[237]

In recent years, 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. These cases varied in topic from the availability of Nazi memorabilia via online marketplaces[238] to gambling websites hosted in countries with liberal regimes in relation to online gambling.[239] 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.

The latest step in this development was reached in recent years when various western, democratic states began efforts to limit the accessibility of child pornography online. Simultaneously many countries saw limitations on access to online information reach new heights in times of civil unrest (Moldova's "Twitter revolution") or revolution (Iran's Internet revolution).[240]

---

[237] See "Spamhaus [An internet block list for spam; HEDR] fined $11.7 million; won't pay a dime", Nate Anderson, Ars Technica, http://arstechnica.com/business/news/2006/09/7757.ars; The order issued by the court in default judgment can be found at: http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf; e360, the plaintiff, has later filed for Bankruptcy and cited huge legal bills as a contributing factor.

[238] Yahoo case (France), see "Yahoo hits back at Nazi ruling" http://news.bbc.co.uk/2/hi/europe/1032605.stm and "Yahoo! loses! Nazi! lawsuit!" http://www.theregister.co.uk/2006/01/13/nazi_yahoo_defeat/

[239] De Lotto (the only permit holder under Dutch law that is allowed to have an online gambling website) vs. LadBrokes (UK betting website). The Dutch High court rules that by offering the option to gamble at the UK based LadBrokes website, LadBrokes is trespassing against the Dutch law on games of chance, and is ordered to block access to Dutch citizens. See (in Dutch) the preliminary order issued by the High Court on: http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AR4841&u_ljn=AR4841

In the ongoing main case between the same parties the High Court has asked prejudicial questions to the Court of Justice of the European Communities (ECJ). See (in dutch) : http://www.rechtspraak.nl/Actualiteiten/Hoge+Raad+stelt+vragen+van+uitleg+aan+HvJEG+over+kansspelzaak+Ladbrokes.htm Other cases involve a similar case brought against Unibet, another UK based gambling website. In English see, on the preliminary case: "Dutch Supreme Court rules on Ladbrokes appeal" on http://www.droit-technologie.org/actuality/details.asp?id=836

[240] Cf. The Moldovan Twitter revolution: http://statismwatch.ca/2009/04/07/protests-in-moldova-explode-with-help-of-twitter/ and http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution.

All of these developments hinge on the availability of internet blocking technology. These are available for several internet related protocols/services (content distribution methods) and can be used in various locations of the Internet network as well as in consumer equipment (i.e. in the home/office). Depending on their technical characteristics, they differ in effectiveness and potential for circumvention. This chapter will describe the blocking technology behind most of these blocking efforts and discuss their implications from a democratic perspective.

This chapter will primarily concentrate on the available techniques for blocking child pornographic content, the main focus of this report, but it is important to note that many of these technologies can be deployed for other types of content or activity with limited additional investment. The chapter will conclude by exploring the (democratic) implications of each the available techniques before reaching a number of interim conclusions.

Regarding the events following the 2009 Iranian presidential election: http://english.aljazeera.net/programmes/rizkhan/2009/06/200962281940160238.html and http://cosmiclog.msnbc.msn.com/archive/2009/06/18/1970353.aspx

5.2 Technical Blocking Strategies

Several blocking strategies exist that provide different methods and levels of effectiveness to block Internet content. The focus will be on blocking child pornography and will give a moderately detailed overview of the technical possibilities and strategies for blocking this content at various network levels and through various technologies.

5.2.1 Specifying content

In order to attempt to block content, identifiers are needed whereby a blocking decision can be implemented. Since some of these identifiers are very common and will be discussed throughout this chapter they are individually explained here from a technical perspective.

The content this report focuses on is usually visual in nature, meaning that it contains either still pictures or video footage of child sexual abuse.

5.2.1.1 IP addresses

Internet Protocol, or IP, addresses are the most basic addresses used to identify machines connected to the internet. They identify all computers with a direct internet connection, such as end user PC's or residential gateways or web-servers that are used to display websites. Since IP addresses are allocated from a central location (under the overall responsibility of ICANN) every address is unique (except for certain addresses that are reserved for local usage).

An IP version 4 address consists of 4 positions of 4 bytes each, or in other words, an address that looks like this: "x.x.x.x" and where x is any number from 0 to 255.

IPv6 addresses are longer (128 instead of 32 bits) and are typically noted with colons separating eight hexadecimal numbers such as 3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344. Hexadecimal notation runs from '0'-'10' and on from 'a' to 'f', which explains the presence of letters in the address.

Since IPv6 is currently not yet widely deployed, this report will use IPv4 addresses in the examples. From a technical perspective there is not a lot of difference between blocking of IPv4 and IPv6 addresses.

The vast address space that comes with IPv6 will probably mean addresses become less scarce and sharing addresses will be a rare occurrence (unlike IP v4). Each IP address will therefore contain less content, which may, in turn, lead to more precision when it comes to blocking at the level of IP addresses.

5.2.1.2 Domain names and DNS

To make the internet more user-friendly and efficient, domain names are used to give meaningful names to content residing on the internet. They have the familiar format of "domainname.com" or "www.website.fr".

Domain-names are used to identify internet resources such as websites or other services (like mail-servers or servers used for instant messaging services). By way of the domain-name system (DNS) these names are resolved to numerical IP addresses that computers can use to communicate.

The top level of the domain-name structure consists of extensions like ".com" or ".ie". A domain-name (also: top level domain) can either be generic, meaning it's extension is not linked to a specific country or region, or geographical meaning, that the domain-name is used to identify a country by means of a two letter (ISO) code (such as .ie, .fr or .nl).

The second level of the domain is essentially selected and controlled by the administrator of that particular domain. A domain like aconite.ie, is, for instance, used by Aconite Internet Solutions to point web-surfers to the Aconite website and email services. More specific identifiers (URL's) then link to specific website content

5.2.1.3 URLs

URL's, or Uniform resource locators, are more specific identifiers for content on the internet. They consist of a domain-name (which identifies the machine where the content is available) and then contain further information pointing at a specific location.

A typical website URL contains both a path (section with directories that contain content) and a filename (final identifier of the content on the server), like so:
http://www.domainname.com/path/to/filename.html

Other services such as email and instant messaging may also make use of URLs and domain-names to identify parts of the services infrastructure.

5.2.1.4 File content and Filename

In many cases content is contained in a file. The file itself contains the picture or video content. It is labelled separately in order for the user to identify the content. Usually users choose self-explaining filenames (such as '`picture_of_me.jpg`'). However, where illegal content is concerned, the same content can easily be re-labelled in order to make it appear inconspicuous. In other words, the contents of the file are independent of the filename or file type.

5.2.1.5 Keywords

A method for identifying content is the use of keyword filtering. In a text based file format, such as a Microsoft Word document, or in the filename of a file, it is possible for machines to identify keywords. A block-list of allowed and disallowed keywords will then need to be kept in order to make a blocking decision. Since many words can be used in a perfectly legal context, and mere appearance of a word need not signify illegal content in every context ("preteen" and "sexuality" could be a perfectly sound description for a scientific paper on that topic, for example), it is still a challenging task for computers to effectively distinguish illegal content without very specific keywords (or filenames) and context analysis taking place.

5.2.1.6 Content Signatures (hash values)

Content can be identified using *signatures* that allow classification of content that was previously categorised as illegal. In this case a unique value can be created that identifies this content using a '*hash algorithm*' (such as SHA1, SHA256 or MD5).

For example, a child pornography image (within a filename of '`preteen.jpg`') has a calculated globally unique hash value of "`87e1a46d2529fe4f42a75789f0bae7a1`" (md5) – i.e the hash value is a short representation of the content of the file, from which the file itself cannot be reproduced, but can be used to identify that file. If an image (with a filename of '`unknown.jpg`') is discovered at a different location, and the hash value calculated for that image is an exact match for the hash value previously calculated for the image within the file '`preteen.jpg`', this is proof that both files contain the exact same image or file content. It can therefore be proven that the image is not innocent and it would be acceptable to block access to it.

5.2.2 Internet Blocking Effectiveness

In addition, the effectiveness of each blocking mechanism will be highlighted. This effectiveness will be assessed using two parameters: accuracy and the actual effect on the accessibility of the material.

To express effectiveness as the amount of content that is blocked correctly in comparison to the total amount of available illegal content (an ideal measure for accuracy) is extremely problematic as there are various unknown parameters. Since the total volume of available illegal content is unknown, the volume of hits on an existing blocking list can only provide a very limited insight into the effectiveness of the respective blocking methodologies.

Additionally, since it is often unclear where hits come from, figures quoting volume of hits on an existing list are a very crude indicator at best[241]. Hits can come from users attempting to access the blocked web-server, from other websites referencing content on the blocked web-server and from search engines and software tools called 'robots' which automatically search for content on the Internet without user intervention. Indeed some malware such as trojans can cause user computers to access these web-sites without the owner's actual knowledge or consent. These automatic software activities are often included in volume hit statistics since it is very difficult to remove them from the statistical population. This concern should cause further investigations especially when such statistics indicate remarkable consistency over a period of time which is unlikely with random user accesses.

In addition, analysis of over-blocking and under-blocking potential will be used as indicator. In other words: with no available insight into the total volume of child pornography being traded, only inaccurate estimates can be made regarding the effectiveness of currently used blocking systems, particularly with regard to attempts at deliberate access to illegal content.

A first indicator for this is the **ease of circumvention of a block**. If it is easy to circumvent or disable a blockade, the availability of the blocked material is likely to remain unaffected. Therefore, effectiveness can be measured by measuring the effect a blockade has on the accessibility of the target material by assessing the number of attempted accesses (accidental and deliberate).

In addition, **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. This means that where the blockade may well be effective, an easy alternative to publicising the same content on a different channel is a good indicator of the impact on the availability of the material and the success of the blockade in that respect. This, however, is not necessarily a property of a distribution technology and its relevant blocking strategies.

Lastly, **the availability of other enforcement options**, that offer other more effective methods of preventing access to the material, should also be assessed - especially if they are less costly, less intrusive or more effective towards the availability of the material.

[241] Cf. Kaspersen 2009 p.261; Numbers of hits publicized do not differentiate per type of visit (Google bot automated spider visit or consumer access provider visit) or type of hit measured (direct access to a warning page on display or amount of requests to a block-list for instance) obscuring possibilities for effective comparison. The quality, size and nature of the filters involved is obviously also related to positive "hits" on the filter too.

5.2.3 Characteristics of Blocking Strategies

The following paragraphs highlight the characteristics of several blocking. There are a few common aspects of blocking strategies which need to be explained.

5.2.3.1 Allow-list versus Block-list

A first characteristic of blocking strategies is the way the filter operates. 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*. The vast resources needed to scan and classify all available material alone seems reason enough to disqualify allow-listing for broad, even publicly mandated usage in an open, democratic society. Not surprisingly all recent western child pornography blocking initiatives have taken a "block-list" approach.

5.2.3.2 Human intervention (dynamic and non-dynamic blocking)

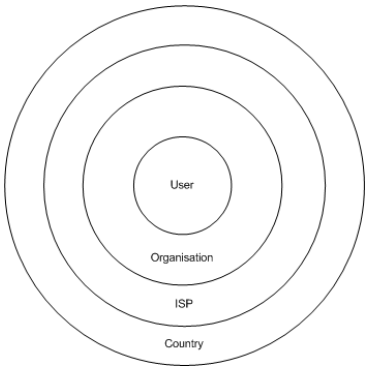
A second characteristic of any blocking strategy is the amount of human intervention required to achieve the blockade.

Typically, child pornography filters are based on consumer complaints and law enforcement investigations. In this case, the contents of the filter will usually be handpicked by the block-list administrator. The content is then reviewed and matched against the block-list criteria personally by the list administrator. This is considered as non-dynamic filtering.

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. In spam filtering, complex statistical calculations are used to tell spam messages apart from normal emails (Bayesian filtering). This type of filtering is often referred to as dynamic filtering.[242]

Unlike spam filtering, in the case of (child) pornography, research shows that dynamic filtering is highly ineffective. Surprisingly, increased accuracy in specifying content to block invariably leads to over-blocking of legal content.[243] Child pornography blocking therefore is usually restricted to the labour intensive variant of block-lists that require extensive human intervention and maintenance.

5.2.3.3 Blocking Point



Blocking strategies can be differentiated by the level at which they are executed.

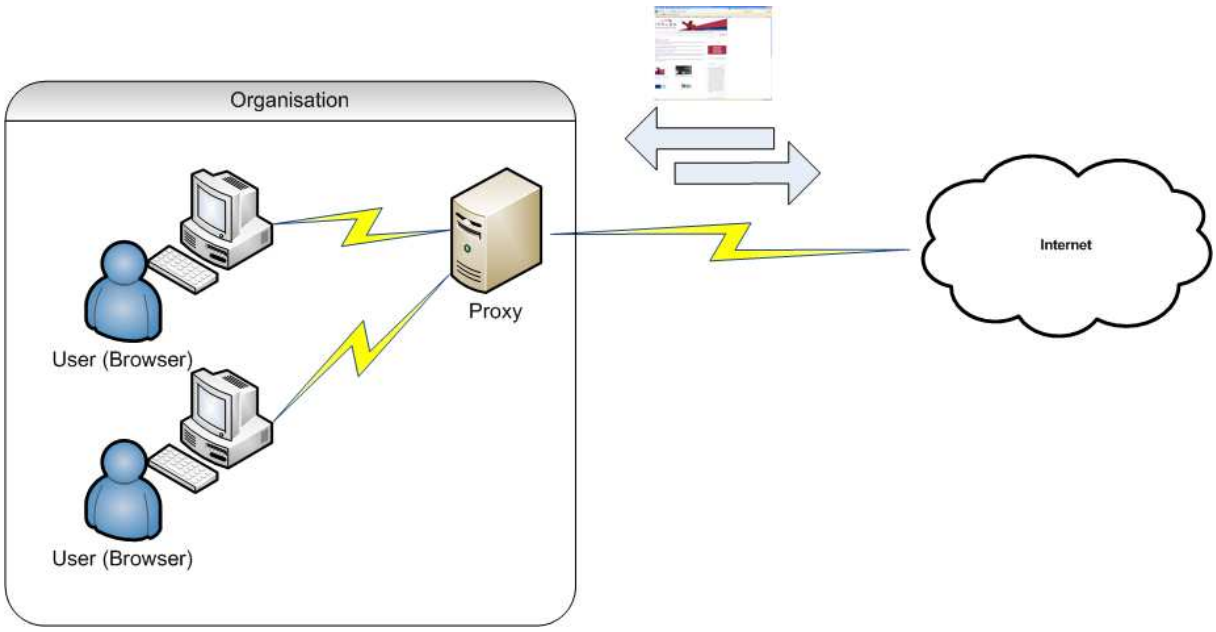
Firstly, user level filters allow parents and computer administrators to block content. Circumvention of these filters is usually easy for the administrator, others users cannot easily circumvent it as long as they can be kept within the boundaries of the machine and of the operating system the filter is installed

[242] Haselton B. Report on accuracy rate of FortiGuard Filter. Bellevue,WA: Peacefire.org; 2007. Kaspersen 2009, p. 252

[243] Kaspersen 2009 p. 253, Greenfield P, Rickwood R, Tran H. Effectiveness of Internet filtering software products. CSIRO Mathematical and Information Sciences; 2001; Kranich N. Why filters won't protect children or adults. Library Administartion and Management 2004;18(1):14–8.; Stark Ph.B. Expert report of Philip B. Stark Ph.D. Civil Action no. 98-5591 (E.D. Pa) ACLU vs. Gonzales; 8 May 2006. Haselton B. Report on accuracy rate of FortiGuard Filter. Bellevue, WA: Peacefire.org; 2007.

on.[244] Effectiveness of user filters has seen significant testing in the US and Australia in relation to (child) pornography in the beginning of the century. The results were mediocre at best.[245]

Secondly, 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. This machine is in contact with the internet and monitors the requests made by users. It usually checks the request for the title of the content requested and through dynamic or non-dynamic filtering will decide whether to block it or not.



It is also possible for blocking technologies to simply record and monitor Internet requests and responses *without* actually blocking. This can be very useful for monitoring potentially criminal or terrorist activities which utilise national public networks.

A state–level, fully centralised filtering infrastructure for all internet traffic is very costly. Investment into central infrastructure alone would need to be significant in order to cope with the traffic loads.

5.2.3.4 Level of Detail or Specificity

If content is checked manually before entering a block-list, there are several methods to actually block users accessing the content. The difference between these methods lies in the level of detail by which the content is identified. Several identifiers are often used to specify the content in varying levels of detail:

IP Addresses

Each of these has a different level of granularity or uniqueness in terms of the content they block. For example, blocking an *IP address* means that other Internet services and

[244] See also ACMA, Closed environment testing of ISP-level content filtering, june 2008, p.9 http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf

[245] A 2001 study commissioned in Australia: http://www.acma.gov.au/webwr/aba/newspubs/documents/filtereffectiveness.pdf
US GAO on P2P filtering effectiveness: http://www.freedom-to-tinker.com/doc/2005/gao_30jun.pdf
A Study on Internet Access in Educational Institutions by the EFF: http://w2.eff.org/Censorship/Censorware/net_block_report/net_block_report.pdf

users that use the same address will also be blocked. Remember, that it is possible for several websites, to be identified by distinct domain-names but still to share one single IP address. If access is blocked to that shared IP address, it will therefore mean that all the other websites and services located at that same IP address will also become unreachable, even if operated by different owners.[246] When some tier 1 (large scale) transit providers in Finland blocked wider Internet access to a range of known IP addresses being regularly used to host child pornography websites in Russia, the effect was to block a wide range of innocent users in Russia and disrupt the business of those Russian ISPs affected. This tactic was chosen in order to apply pressure on some Russian ISP's to take steps against those hosting websites with illegal content.

Domain-Names

Blocking by a domain-name will block ***all*** content residing under that domain. Although some websites can be focussed on a single subject and content type such as child pornography, there is still a possibility that part of the content residing under a domain may be unrelated to child pornography but would still be blocked. In some countries. the percentage of potentially illegal content to legal content is statistically calculated and at a pre-selected percentage point the domain name is added to the blocking list. This approach accepts the fact that there will be undesired blocking of legal/innocent content caused by this decision. For example, consider blocking a (first level) domain like "`xs4all.nl`" (a major ISP in the Netherlands, whose users may have homepages under the domain name with their username as identifier for their directory on the server). Blocking this domain will then not only block "`home.xs4all.nl/~perpetrator`" but also "`home.xs4all.nl/~innocent_user`" as well as XS4all's main website which is accessible via "`www.xs4all.nl`" (all, so called second level domain-names that contain various websites and services).

Uniform Resource Locators (URL's)

Best results in terms of specificity will therefore be obtained by filtering on a *URL basis*. This means that the block list can discriminate between URLs such as "`www.xs4all.nl/~perpetrator/illegalpage.htm`" and "`www.xs4all.nl/~innocent_user`" or "`www.xs4all.nl/~perpetrator/legalpage.htm`". This will require a blocking system which can also work at this same level of specificity. This level of detail requires significant effort and resources to analyse the extensive and varied content of websites to create a list of url's to be blocked. Also, for a website owner, changing a URL is a trivial exercise and can be automatically done by website software for every file which is served in order to confuse blocking filters. Due to the ability to evade blocking 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. See section 5.2.1.6

This type of filtering requires extensive access to the internet content being transferred between the user and the internet. It also implies ready knowledge of available illegal content since it requires the creation of signatures. New content, then, is easily missed by the filter. However, even a trivial or minor change to the relevant images can cause a different hash value to be calculated thereby causing this type of block filter to fail. This can only be overcome by extensive investment into analysis of new content by other means, typically by human content analysts. The costs for that are likely to be significant.

246 Cf. B. Edelman, Web Sites Sharing IP Addresses: Prevalence and Significance, http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/ whose analysis shows the majority (87.3 %) of websites identified by domainnames are hosted on a shared IP address

Encryption of the content concerned will also render this method useless since the encrypted file content cannot be easily analysed.

This system results in a significant risk for under-blocking. Since every piece of relevant content would require a hash value to find it in a database, it is extremely resource intensive.

Keywords

An Internet blocking decision can be made based on keywords found either in the filename or the URL or the text at the location of the content being accessed. For this to work effectively, complex analysis of the recognised keywords in the context of their use needs to be performed. A single mention of a conspicuous word may, given the context, be enough for any human to identify the content as "possibly legal". Making this type of decision, however, is not trivial for dynamic filters when asked to filter internet content.

For example if we decided to simplistically block any pages which contained the words "child pornography" then sites which contain "child pornography research" or "child pornography legislation" would also be blocked which is clearly not the intention of the blocking system. Indeed this very document would be completely blocked by simplistic systems which would find keywords many times in this document.

A system using keywords is subject to easy evasion by spelling important words in different ways such as "child pornography" being spelt as "chld pornography" or "ch1ld pornography". Even more complex (mis)spellings and acronyms are seen in widespread use with mobile phone short message texting e.g later is spelt as l8tr, etc.

5.3 Internet distribution methods for Child pornography

5.3.1 Internet penetration and Illegal content distribution

The last few years have seen a rapid growth in the availability of broadband services. Figure 1 clearly shows that many open, western and democratic societies lead the way.[247]

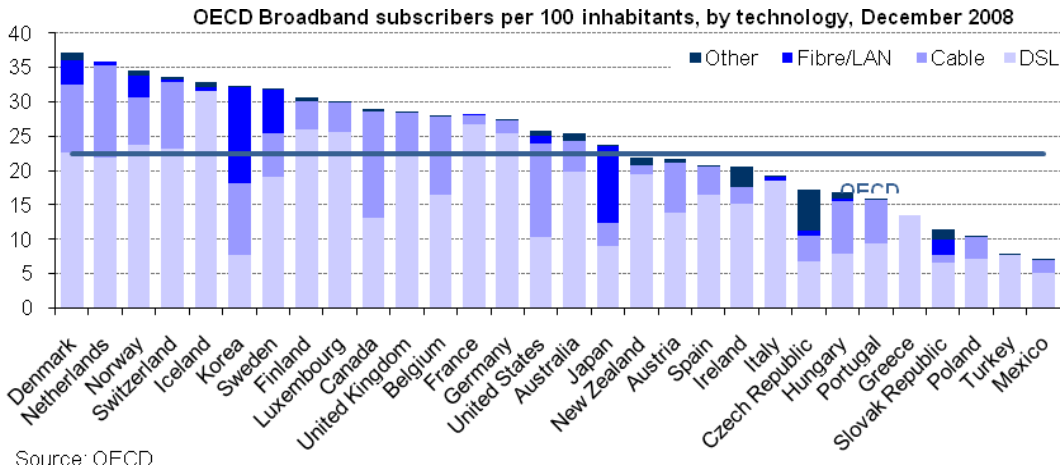


Figure 1 Broadband Subscribers per 100 citizens according to OECD Broadband Portal[248]

Child pornography can be distributed across the Internet using various methods via these high speed broadband Internet connections.[249] 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.[250]

INHOPE, the international network of Internet hotlines which process reports from the public of certain types of illegal content on the internet, provides an indication of the current primary methods detected by the public for spreading static content . [251] This figure includes complaints about racial hatred and other content, but since allegations of child pornography make up 50% of the potentially illegal content reported, it is still a good overview of the most relevant distribution mechanisms, as perceived by the general public.

[247] By comparison (not many developing countries are OECD member), figures taken from non-OECD members from Africa and eastern Europe suggest significantly lower penetration rates. Cf. EBRD, Comparative assessment of the telecommunications sector in the transition economies (Eastern Europe): http://www.ebrd.com/country/sector/law/telecoms/assess/report.pdf and for Africa (Including dial up access): http://www.internetworldstats.com/stats1.htm

[248] Figures taken from OECD Broadband portal at http://www.oecd.org/sti/ict/broadband (2009)

[249] Cf. http://is2.lse.ac.uk/asp/aspecis/20060154.pdf

[250] Cf. Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences, Kim-Kwang and Raymond Choo, Australian Institite for Criminology available at: http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf

[251] See the 2007 INHOPE Global Internet Trend Report, available at https://www.inhope.org/en/system/files/inhope_global_internet_trend_report_v1.0.pdf

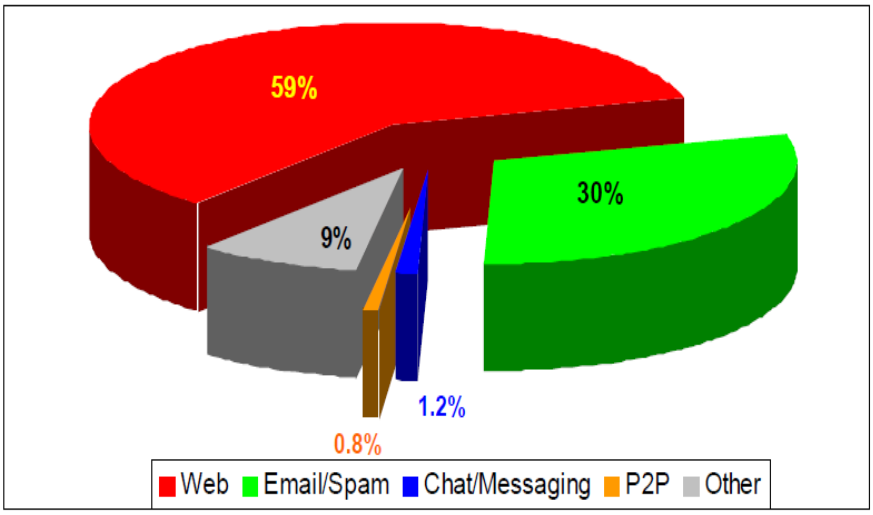


Chart of different **Internet Services**, and their contribution to the **Total number of Reports Received** (trend average for last quarter of 2006).

Figure 2

Distribution methods of alleged illegal content according to INHOPE

Recent figures from the Dutch child pornography hotline, which also publishes the distribution of their complaints across various services, support these results in citing websites as the predominant distribution platform perceived by the public, followed by email spam, usenet and peer to peer (filesharing) networks.[252]

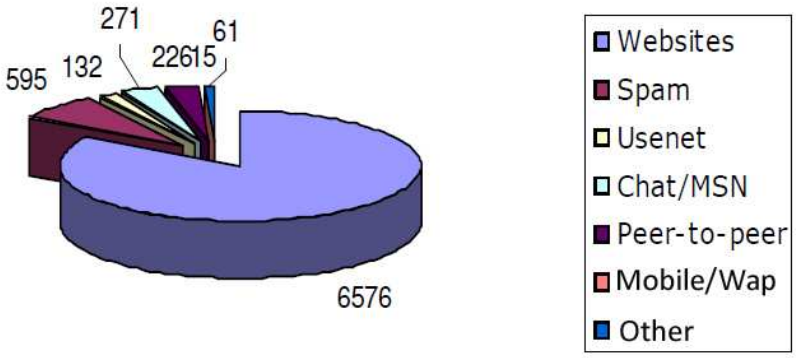


Figure 3

Distribution Methods according to Dutch Child

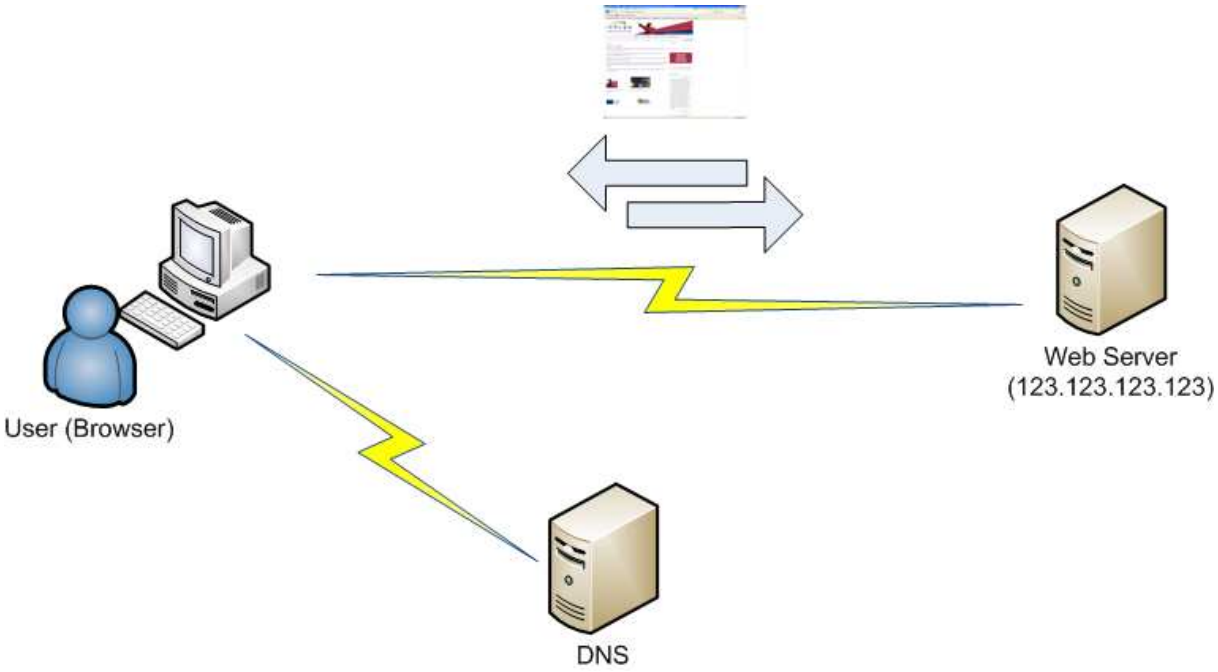
One should note that these figures relate to complaints. Therefore only allegations[253] of child pornographic content that are reported by the public are incorporated in these figures. It also important to note that that whereas websites are often publically accessible and spam is sent untargeted, some services (such as peer to peer networks) require that direct selections of the available content be made by the end user (e.g. online searches). This makes it less likely that end users will "innocently stumble" over this data, let alone report its objectionable content.

It is worth noting that despite the high penetration of internet in the Netherlands, the incidence of an end user accidentally discovering child pornographic content is quite low. In a nation of 16m inhabitants, most of whom have regular internet access, the above figure of around 7,500 complaints[254] results, approximately, in a 0.05% chance of this happening once to an inhabitant at any time in a given year.

[252] Also compare: Kaspersen et al 2008, p. 6, which lists similar, historic figures since 2002.
[253] 20% of reports contained illegal and harmful content and an overall 10% contained illegal content including child pornographic content and hate speech. (www.inhope.org global Internet Trend report)
[254] This calculation excludes users who discover illegal content but do not report it to a hotline

5.3.2 Websites

Websites are one of the foremost distribution methods of all types of content on the internet. They work through servers which are all identified by domain-names and Internet Protocol (IP) addresses.



The world wide Domain Name System (DNS) translates the domain name of a website to an IP address that is subsequently used to retrieve its contents.

The communication system or protocol used to access a website s is called HTTP (HyperText Transport Protocol).

To make content available to end users, many different software and hardware systems work together. First, there is the server which is programmed to collate the requested web content to send to the user and to maintain a connection with the the internet browser making the request. This machine is usually referred to as the *web server*. Usually only one machine contains the software used to serve the content, in larger websites it is not uncommon to spread the work over several machines.

Sometimes there is an intermediary server called a 'proxy server' which provides content that it has previously retrieved from web-servers around the world. A proxy-server is often used by organisations to speed up access to regularly access web-sites for its users.

The software used to serve web-pages is called web hosting software. It is often open source such as Apache although many alternatives are available. Microsoft and many other software vendors have developed web servers for all sorts of usage scenario's.

Usually, web content resides on the hard-drive contained in the server, but such content can also be retrieved dynamically or created dynamically, whereby a database is often used to hold relevant data. Where the content is produced dynamically using database queries or programs residing on the web-server, the term "*generated content*" is used. This means the content is the product of a programmed operation and is not present as a static copy on the web-server. In this scenario the web-content returned can depend on the IP Address of the machine requesting the content, the time of day, or hundreds of other criteria programmed into the web-server.

Many programming and scripting languages can be employed to display relevant content based on user input. Typical scripting (or web programming) languages are PHP (open source) and ASP (Microsoft), although many others are in use throughout the web.

In a multi-server setup, content may reside on several machines all performing different tasks. Where one machine connects with end users, others may contain the files they will view, and a third may hold the database that produces search results for users to explore. Such a multi-server environment has the added capability of choosing to place the machines involved in geographically different networks, using the internet to combine them to a working environment.

The content displayed from a web-server is usually formatted in the Hypertext Markup Language (HTML). This language allows for images, video and other content types to be visible to end users in a web-browser (like Chrome, Firefox, Internet Explorer, Opera or Safari).

When users visit any website identified by a domain name, their internet browser will usually first query the DNS of the users' internet access provider for the appropriate IP address to contact the web-server for that domain. The ISP will then use the DNS system to find the server that hosts the answer to the query, using the hierarchical structure of domain-names to find relevant answers.

For example,

- It will first query the top level domain-name service for the **`.com`** zone (operated under the authority of ICANN), which resides with a company called Verisign.
- There the whereabouts of the authoritative server for a specific .com domain-name (like domainname.com) are available (for instance in a record that refers the user to **`nameserver.registrar.com`**)
- at this name-server the answer is then finally retrieved and sent back to the end user.

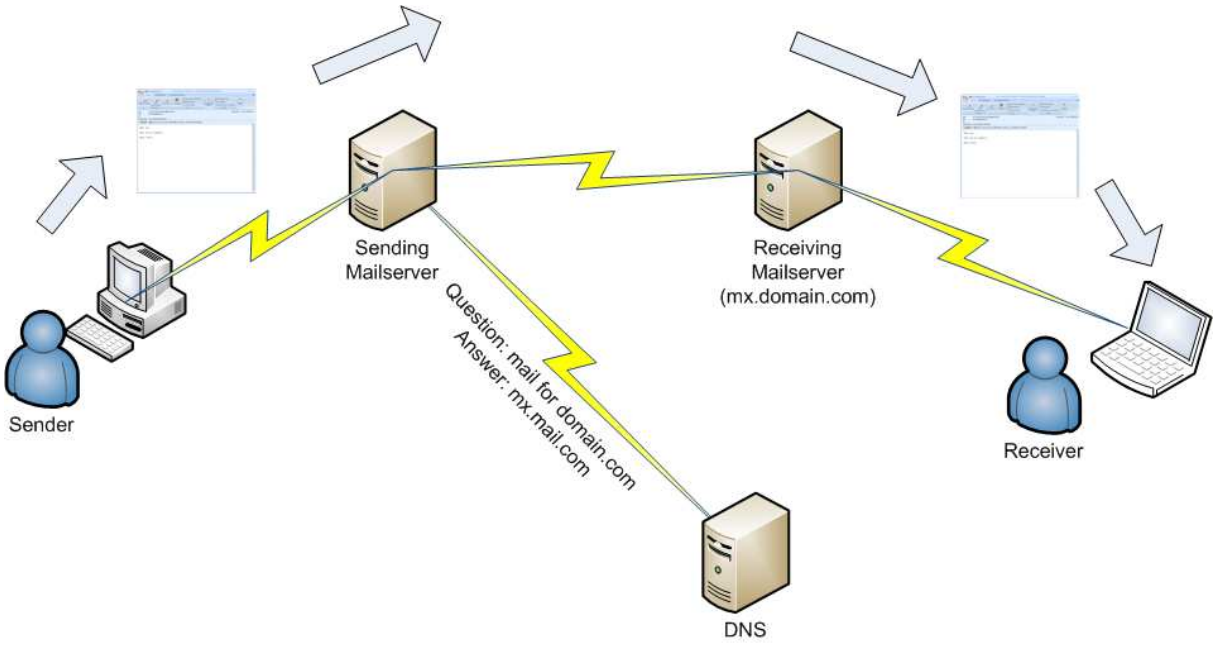
Once the answer arrives, a connection is set up between the end users PC and a web server that contains or generates the content of the website. Although many websites will operate on their own IP address, many different domain names can point to the same IP address. This is not at all uncommon.[255]It is also possible to visit a web-server without a host name by directly typing an IP address.

It is common for many different web-servers operated by different owners to be attached to one IP address. To serve the right content the web-server needs to know the requested domain name (i.e. which URL or domain name at a shared IP address the user is trying to access).

[255] B. Edelman, Web Sites Sharing IP Addresses: Prevalence and Significance, http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/

5.3.3 Email and Spam (unsolicited email)

Email is still the most widely used service on the Internet, even more than web or social networking websites. However, email also attracts most complaints relating to the distribution of abusive material relating to website content.



Outbound messages are delivered by a client (such as Microsoft Outlook or a webmail system such as MSN Live and Gmail) to a predefined mail-server that handles outbound mail for the sender.

Outbound mail-servers are usually operated by an Internet Access Provider or Internet Hosting Provider who will only allow their own users to send email. Inbound mail servers, which are sometimes the same machines as the outbound mail-servers, are used to receive email and store it until the end-user retrieves it using a PC or mobile device.

The domain name system again plays an important role in email usage. The DNS is used to look up the destination of a message. The destination of the message is selected using a DNS query to find the destination MTA (Mail Transfer Agent: an email server). For example, a query for a Google Gmail subscriber will return the DNS name of the inbound mail-server at "`gmail-smtp-in.l.google.com`" and four others that could be used as an alternative if the primary MTA is not working or can't be reached.

The actual transport of messages takes place between MTAs, using the Simple Mail Transfer Protocol (SMTP). SMTP is a very old[256] and ubiquitous protocol that defines how messages are passed between servers. The protocol is stateless and open-by-design which means that the sending MTA does not keep track of the delivery state (successful or not) and that, by default, any machine can deliver mail to a receiving server.

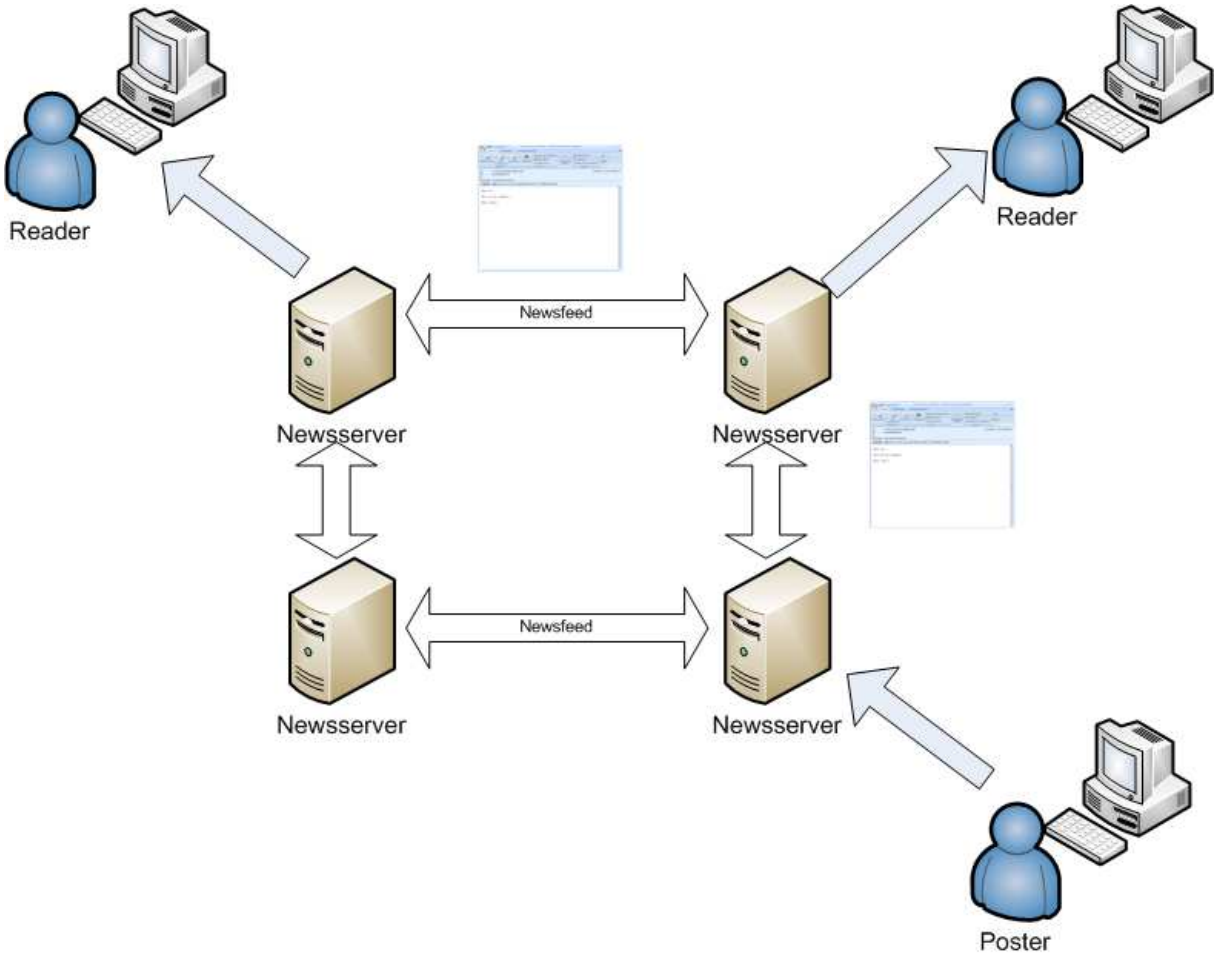
In order to transport data (such as pictures and video) inside the text messages passed between MTAs, encoding and decoding of messages (into and out of simple text format) takes place in the e-mail software of the end-user. This allows the text only email protocols to pass data files (binary data) as attachments inside the body of the text message.

[256] It was first designed in 1982, see the design documentation, RFC 822 http://tools.ietf.org/html/rfc822 later (2001) replaced by RFC 2822 http://tools.ietf.org/html/rfc2822

5.3.4 Usenet Newsgroups

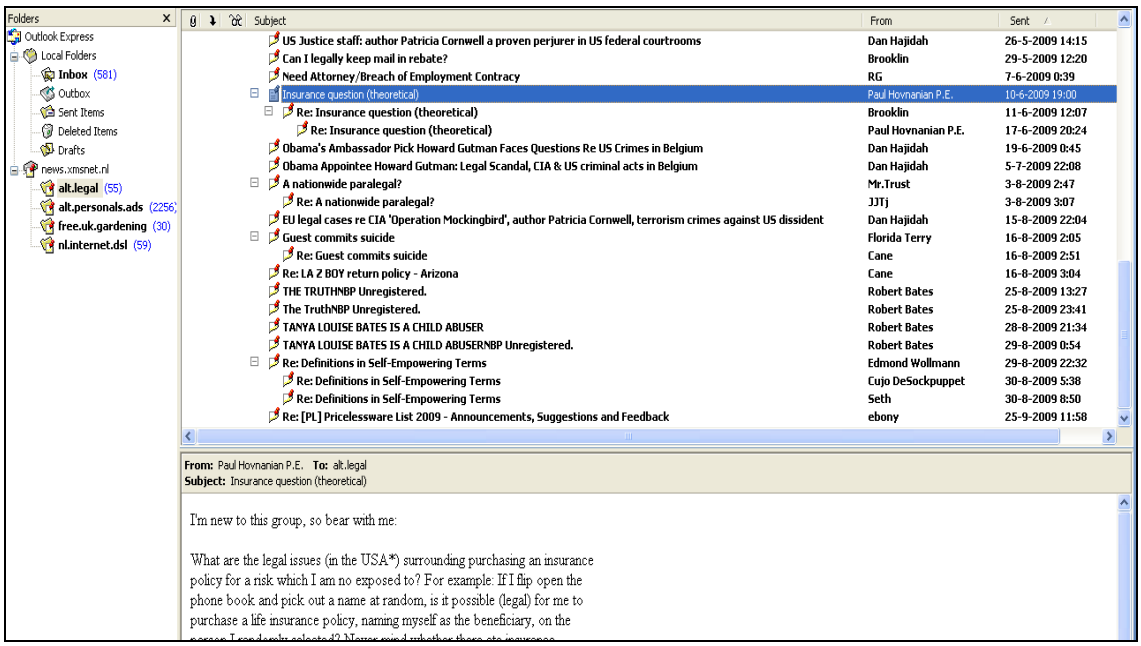
Usenet has been in operation for decades[257], and has served to distribute text content between public Usenet servers. Since the commercial use of the internet, it has become a popular platform for distributing all sorts of illegal content varying from copyrighted material to child pornography.

Usenet servers, usually operated by ISPs, act like mail servers in that they receive text messages from end users and forward them onwards to other Usenet servers (or news) servers. Users will be using newsreader programs such as Outlook Express or specialised Usenet software (such as Grabit or Newzleecher) to display the servers' content.



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 (for example "`alt.binaries.windows`"). Like a web forum page or a discussion board, these servers display the messages to the general user public. The servers maintain lists of messages per group, which can be retrieved using the Usenet (or NNTP) protocol. Group content is then usually displayed in threads of messages pertaining to similar sub-topics displayed in hierarchical order by modern newsreader programs (see screenshot).

[257] Usenet was conceived by two students of Duke University, Tom Truscott and Jim Ellis, in 1979. They based the idea of the then popular Bulletin Board Services where users could dial in and see text content on their computer.



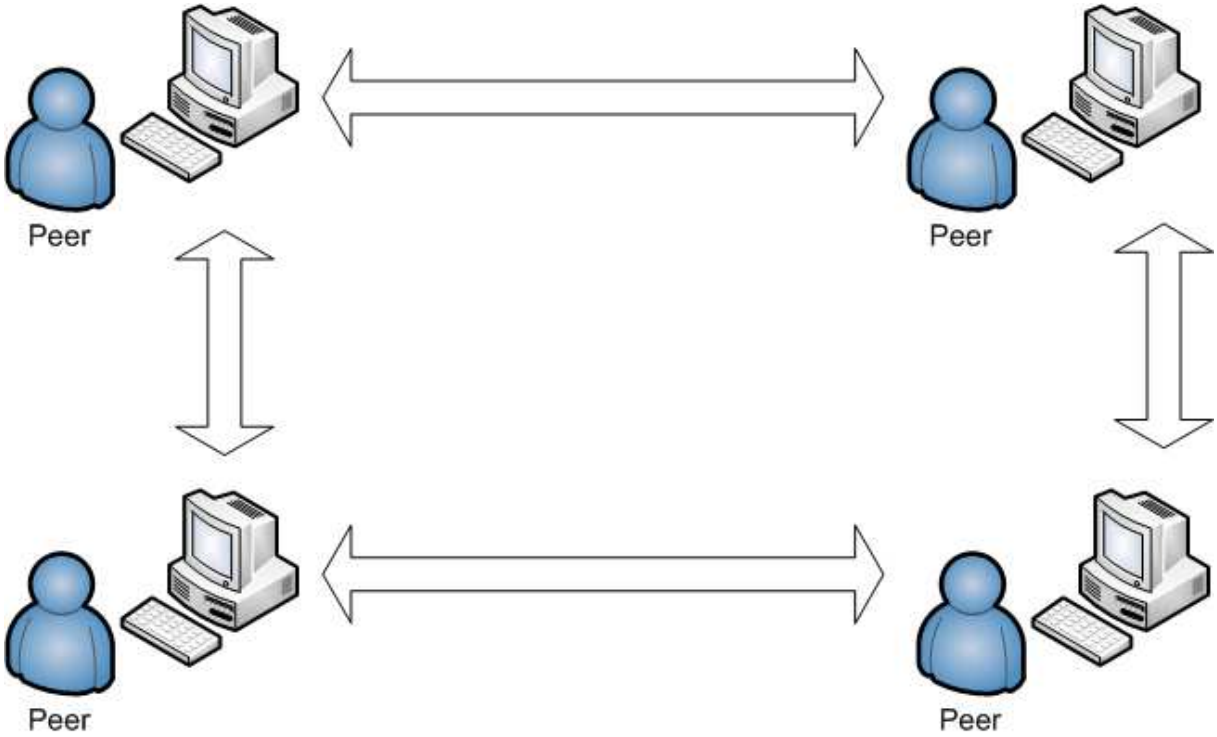
As Usenet can only handle plain text, encoding is needed in order to permit the sharing of data files, such as pictures or video files. Since messages are usually limited in size, intricate encoding techniques are used to encode and compress data files, and to spread them out over several hundreds or thousands of text messages, and making these available in sequential order for decoding.[258] Separate channels such as FTD or "nzb" file search engines are then often used to identify these messages and to allow specialised software to download, repair and decode the content (often messages get lost, so file recovery data and redundant data blocks are used to securely post larger files on Usenet).

Removing content from Usenet is difficult, since '`cancel`' requests between servers are often ignored for security reasons. The protocol, although fitted with a cancel option, does not have a secure system to verify cancel messages. All binary (file) content usually disappears after a while, usually not longer than 200 days to 1 year. After this retention time, the messages are replaced by new ones arriving from the posting user community. For this reason material is often re-posted after the initial retention period.

[258] For a full description of this process please refer to http://en.wikipedia.org/wiki/Usenet#Binary_content

5.3.5 Peer to Peer networks (P2P)

Since the advent of the Napster file-sharing system in 1999, peer-to-peer file-sharing technology has developed at a rapid pace. Although the technology has legitimate uses, particularly for businesses that need to transfer very large files, it lends itself to the sharing of music and movie files, without right causing major problems for copyright holders.



Peer-to-peer file-sharing is based around the exchange of files directly between end users' computers, bypassing intermediate servers which can cause delays or even communications failures. For this purpose, specialised software was developed that enables rapid index searching through the available content and retrieving files from the p2p network that may consist of tens of thousands, if not millions of end users at the same time.

Whereas centralised servers were used to locate and index content in the beginning, in recent years (mostly due to legal pressure exerted on these centralised infrastructures by copyright holders[259]) technological advances have allowed for decentralised, distributed and highly anonymous network topologies that defeat the perceived weaknesses of a centralised database in the network. The term distributed means that content and network (search) functions are all dispersed across many users PC's – called 'peers'.

The protocols for exchanging files and enabling searches through all the available content vary widely. In the KaZaa (fasttrack protocol) and eMule (gnutella protocol) networks queries are passed through specific connected clients. All content is public, and one can observe a number of the queries made by simply connecting.[260] Downloading documents and files occurs

[259] See, amongst others, on Napster: http://en.wikipedia.org/wiki/Napster and http://news.findlaw.com/legalnews/lit/napster/; on Kazaa: http://en.wikipedia.org/wiki/Kazaa and http://news.bbc.co.uk/2/hi/technology/5220406.stm

[260] See for instance Guillaume, Latapy and Le-Blond, Statistical analysis of a P2P query graph based on degrees and their time-evolution, available at http://hal.archives-ouvertes.fr/docs/00/05/45/86/PDF/guillaume04iwdc.pdf and The US GAO, "The Use of Peer-to-Peer networks to access pornography" (2005) and "Peer-to-Peer Networks Provide Ready Access to Child Pornography" (2003), respectively, available at http://www.gao.gov/new.items/d05634.pdf and http://www.gao.gov/new.items/d03351.pdf

by splitting the requested file into discrete pieces, thus spreading the load on the resources of individual peers.

In other cases, such as with BitTorrent a centralised tracker is used (which can even be restricted to a limited group only, where this required). The tracker keeps track of the availability of the requested content and maintains a list of users where it resides. A well known source for publicly available bittorrent files pointing to trackers is a website called "The Pirate Bay". It is currently under heavy pressure from copyright owners for making available trackers that lead to alleged copyright-infringing material and has also been mentioned in connection to various child pornography cases in the recent past.[261] Many other examples of trackers are in operation today.

In Freenet, an advanced, encrypted, highly-anonymous file sharing network, the network's content is spread throughout the network of peers, with all peers maintaining copies of parts of the entire Freenet network content. The network functions as a separate file-system that automatically maintains sufficient copies of content once it is published. This, incidentally, makes removing content even harder than with regular P2P systems, since peers themselves have no easy option of removing content which is served through their machine.

On top of this decentralised, distributed file system is a system of encrypting traffic between the peers, and an alternate addressing scheme to access content on the network. Thus, as a peer, there is no way to know what data is stored on your machine or who uses your bandwidth, and for what purpose. Also, since traffic is routed through several peers to perform the actual file exchanges (*multipath routing*), a very high degree of anonymity is guaranteed. It is virtually impossible to trace content back to the original publisher.

Freenet has two modes of operation that can also, optionally, be activated simultaneously. In the first mode, the *opennet* mode, all peers are connected to each other through automatic discovery. This means any peer may come into contact with any other, depending on the discovery process. In the *darknet* mode, only pre-defined friends are used to connect to, enabling further anonymity. As a network inside the network, Freenet has often been identified[262] as a favourite hideout for extremists and paedosexuals. Similar systems are available that go by names like Entropy, or ANTsP2P.

Later generations of peer-to-peer programs tend to bias towards hosts who respond quickly to queries. The peer-to-peer network will then favour connecting with local end users who may find themselves on the same ISP network. To effectively filter traffic, therefore, local filtering needs to be implemented including traffic between two neighbours, connected to the same network element (e.g. switch or DSLAM), in order for blocking to be effective. This requires de-centralized filtering (or, alternatively the need to lead all traffic through central filters) and have significant impact on ISPs networks and the way they are designed.

P2P overview

Program	***Technology (Protocol)***	***Encryption***	***Anonymity***	***Distributed***	***Distributed file system***	***Private sharing***
Napster	Napster	No	Low	No	No	No
KaZaa	Fasttrack	No	Medium	Yes	No	No
eMule	Gnutella	No	Medium	Yes	No	No
BitTorrent	BitTorrent	No	Medium	Yes	No	Yes
Freenet	Freenet	Yes	High	Yes	Yes	Yes

[261] See http://www.theregister.co.uk/2007/09/03/another_pirate_bay_police_case/ Cf. M.J. Smith (ed.), Child sexual abuse Issues and Challenges, p.4

5.3.6 Search engines

Although not primarily a content distribution method, it is important to recognise the crucial role that search engines have in everyday web activity. By indexing the content of websites through an automated process, these services are able to identify relevant content by way of keyword searches and complex search algorithms. Google, most notably, is known for its high market share in providing search results.

Effective Internet blocking using such complex analysis of keywords in search algorithms can sometimes be subject to commercial and trade secrets since such activities are very similar to current methods of providing accurate and relevant results to search engine queries and to online advertising campaigns.

Search engine indexing is done using web crawling technologies (among other methods). Web crawling is when a software programme, sometimes called a bot, searches through DNS servers looking for domain names, then through the associated websites and following each link on every web site which is found indexing every page of content it finds. This index is then used when users perform searches seeking specific content.

Such web crawling techniques can cause problems when the search engine is seeking content which is on a block-list and which redirects the web-crawler to a stop page warning about illegal content. The web-crawler can cause a large volume of hits on the stop page even though there is no actual user performing these accesses.

5.3.7 IM and Other

Another important tool for exchange of child pornographic content is instant messaging (IM). A 2006 Swedish study (Eneman 2006) even found that IRC chat, which is one particular form of instant messaging that revolves around central networks of servers that relay small text messages between end users, was the number two source for child sexual material.[263] The study analysed 209 court cases. File sharing mechanisms were, however, always combined with text chat so content could be exchanged effectively. The IM channel served more as a vetting and introduction mechanism, whereas content was seen being exchanged directly, using other technologies.

Modern day IM systems tend to enable file-sharing by allowing users to share part of their hard disk (cf. MSN shared folders) or allow for direct exchange of files (examples are again MSN, AIM, Skype and many others). Data that gives insight into the use of this technology for this purpose are scarce, however.

Various other digital and online means of transporting and exchanging child pornographic content are mentioned in studies into the phenomenon. Most importantly, any file storage mechanism, such as an online backup (ftp) or online 'hard-drive' system or even a web based email account (where the e-mail system is used as a storage device rather than its intended email function) can be used to transfer files between two persons.

Police investigators confirm the use of these systems in internet related cases of child pornography.[264] Incidence of these transfers appears low, judging by the number of complaints and the response from police to queries along these lines, but these statistics may, in fact be distorted by a lack of investigative resources being invested into this phenomenon.[265] Again the Swedish study appears to support this view.

There is also the possibility of using of direct transmission (for example using webcasts, using webcams or IM programs allowing for video chat) to distribute live paedosexual material.[266]

[263] A critical study of isp filtering of child pornography, Eneman, 2006; at http://is2.lse.ac.uk/asp/aspecis/20060154.pdf p.7

[264] Kaspersen (2005) p. 7

[265] Kaspersen (2005) p. 7 and Opsporing van kinderpornografie op internet een statusoverzicht (Dutch: Criminal investigations into child pornography on the internet, a status report), Oosterink, Van Eijk (2006), Dutch ministry of Justice, The Hague.

[266] Wortly and Smallbone (2006; US DOJ COPS project), "Child pornography on the internet" http://www.cops.usdoj.gov/files/RIC/Publications/e04062000.pdf mention a case where a live webcast was used and viewers could direct the actor to engage in specific sexual acts with a child, as noted by Burke, A., S. Sowerbutts, B. Blundell, and M. Sherry (2002) "Child Pornography and the Internet: Policing and Treatment Issues." Psychiatry, Psychology and Law 9(1):79–4.

5.4 Blocking Strategies & Effectiveness

5.4.1 Introduction

This section analyses blocking strategies for each distribution medium. Although several options may be available the analysis will focus on realistic scenario's that are known to be deployed in practice.

Note: The analysis will not go into detail about user level filtering programs. These are less relevant from a democratic or public policy perspective (since it is the user who chooses to limit his/her own surfing behaviour). They are also less transparent (proprietary software) and have little communalities in their design and purpose.

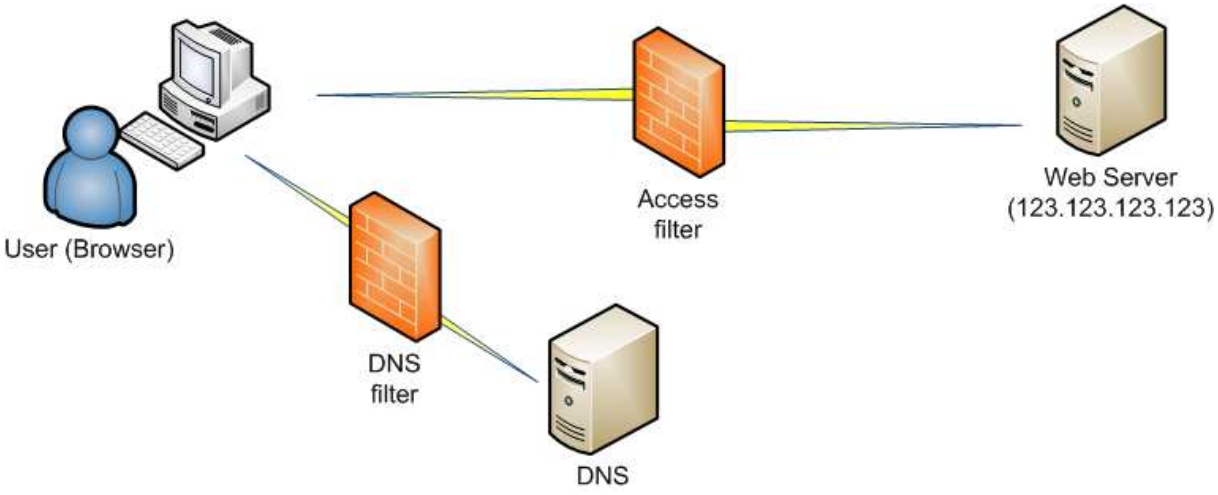
5.4.2 Website Blocking

Websites are usually the prime target for blocking attempts - especially of child pornographic content. They are a very common medium for the exchange of this material. They are accessible and are often the area of activity for potential paedosexuals searching for child pornographic content.

Usually dynamic blocking is not considered an option due to the visual nature of most child pornographic content. This makes it difficult for automatic recognition systems to recognise it effectively. Significant technical research is evolving towards a method of machine recognition of child pornographic content but is not yet sufficiently reliable or effective to comment on. Alternatively, simply scanning for textual keywords within target web-pages will make the block susceptible to simple evasion techniques (for example by leaving triggering words off the site whilst advertising through different channels or using different spelling of words).

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

- Firstly, the server that contains the website could be blocked at the level of its IP address preventing anyone using the filter to access that address. A block-list would then contain only IP addresses of known illegal content.
- Secondly, 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. The URL (note: a domain name is one form of a URL) is included in each request to a web-server. Therefore examination of each request, most commonly by proxy servers, would be needed to analyse the users web traffic with a view to finding the URLs requested. The request is then matched against the URLs on the block-list and when a match is found the web request is blocked.

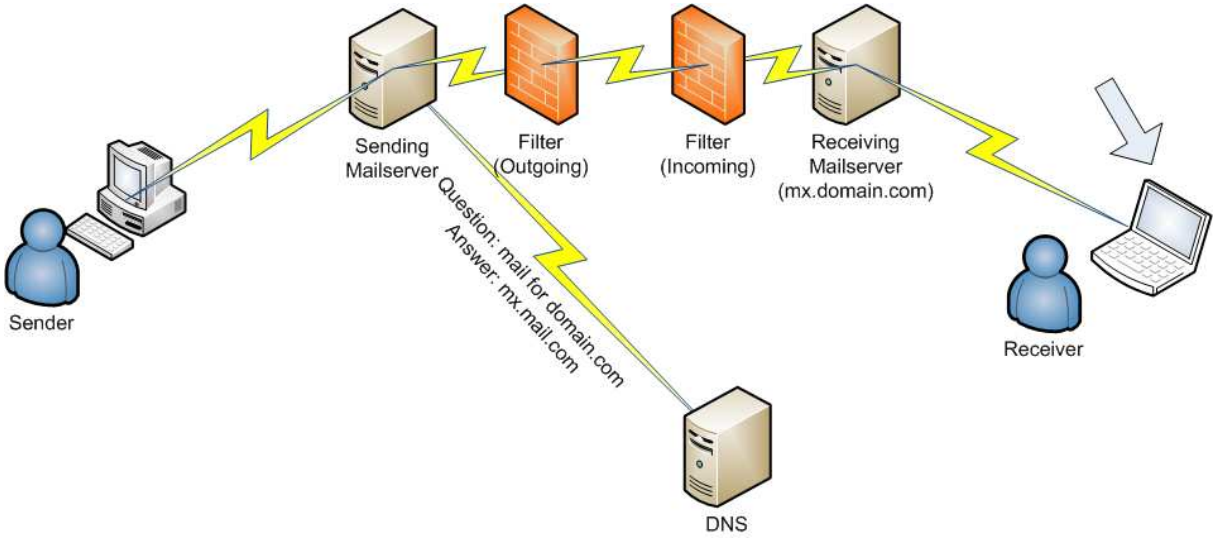


It is important to note that blocking can be attempted both in the path of the user to the remote server (the access network) and in the path of the user to the DNS service.

In the first case, 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. Attempting to block traffic to or from the remote web server by blockades in the direct path to it, means that in order to circumvent the blockade, the user will have to discover different ways to access that remote web site.

5.4.3 Email Blocking

Blocking email is common practice as a result of the large volume of spam email that traverses the net. Most of these email filters are operated on, or right before the receiving mail-server that takes incoming mail for users on a network. Depending on the setup, either the same or different hardware as the email server can be used to perform the filtering. Such filtering is nearly always done with the explicit opt-in consent of the customer of the ISP who is receiving the emails and is a service offered by ISP's to improve the quality of the email service they provide.



Often, ISPs will also filter their outgoing mail to prevent the use of their servers for spreading spam and other unwanted emails.[267]

Generally speaking, two ways of filtering email exist. Firstly, there are connection based filters that check the originating IP address of the sending mail-server against a number of blacklists. These are usually maintained by anti-spam and anti-virus filtering companies or other organisations that collect IP addresses involved in spamming. Depending on the filter settings, messages will either be marked (for example by adding a tag like "[SPAM]" to the subject line) or the connections from the block-listed IP addresses will be ignored.

Secondly, filters can use the content of messages to filter out unwanted content. For this purpose certain block-lists contain advertised URLs in spam messages. The presence of a known illegal url could then lead to the message being blocked.

Alternatively, keywords and various other characteristics can be used to dynamically filter messages. Except for obvious references to explicit keywords (like "lolita" or "preteen") or advertised URLs dynamically filtering child pornography is not easy. In particular, filtering images is very difficult and resource intensive, if not almost impossible, given the amount of email involved.[268]

The most successful strategy therefore, should likely be one based on the advertised URL, where efforts will need to be directed towards qualifying the content of advertised websites inside emails. Since these are similar lists as web oriented URL blocklists, duplication of efforts could be prevented by using these lists as primary input. That said: it may well be that spammers advertise different URLs in their spam campaigns. As a result, the legacy of such an initiative could be an invasive monitoring of e-mails which is unable – due to the changing strategies of the spammers – to fulfil the role for which it was implemented.

[267] ENISA ISP study 2007 p.6 http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf
[268] Supra p. 242

Scanning message attachments could be done using signatures of known child pornographic content (legal issues are a separate consideration: r.f. Chapter 6). This could identify incoming child pornographic spam messages, and could also be used to prevent child pornographic content from being sent out if this technology were applied on the outgoing mail stream. Especially where outgoing filters are used, there is the extra opportunity of actively identifying users spreading child pornographic content in the network and possibly, even giving their details to law enforcement. Because of the high incidence of malware, however, there is the potential for a large number of false positives that could be generated in that fashion, with all consequences this may have. [269] Since, Internet Access Providers are often considered 'common carriers' similar to the post office or telephone system and are under no obligation to monitor[270] traffic on their networks, engaging in this activity may seem contrary to their business interests and likely to lead to demands to search user e-mails for other kinds of content, such as copyright infringements. Indeed, there are also legal reasons why ISP's are not permitted to read emails no more than we would expect the post office to read all letters sent through the post.

The required infrastructure for email filtering is often already in place, given the high volume of spam and the high penetration grade of spam filters.[271] Incremental costs for blocking child pornographic content in email could therefore well be lower than they would be for website content since only additional blacklists would need to be implemented in the filter systems already in place.

In terms of effectiveness, blocking email can be considered relatively effective if adequate blacklists are in place. No evidence of precise efficiency was found in the research for this study, however, in relation to filtering of mere child pornography by spam filters already in place. As a result, it is currently impossible to assess if the costs of implementing such a system are proportionate to the problem, taking also into account that such a mechanism could be considered as total monitoring of private communications, which in turn could be considered as non acceptable whatever the efficiency of the mechanism is. See Chapter 6 ,

Potential for over-blocking is present where IP addresses or even entire originating mail-servers are blocked due to incidents involving child pornography. Similar to web content, blocking all mail from a network or IP address may lead to other, legitimate services being blocked (such as other users of the mail-system on the same address or even all users of a domain-name as per the example mentioned earlier). This has already happened repeatedly with regard to general spam blocking.[272]

No initiatives in the area of email blocking were observed in the countries that have recently undertaken web blocking efforts.[273]

[269] AOL is the only, ISP authors are aware of, that blocks pedosexual email attachments by use of a hash values database; Cf, US senate testimony given by John D. Ryan of AOL in 2006, available at: http://archives.energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Ryan.pdf
[270] Cf. 7.6.1
[271] ENISA ISP study 2007, http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf
[272] Compare, by way of example: http://www.wired.com/techbiz/media/news/2005/01/66226
[273] Cf chapter XX chapter on debate

5.4.4 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.[274] Predominantly, ISPs operating Usenet servers will refuse to host groups with explicit names such as "`alt.example.binaries.preteen`". Over-blocking is often cited in this area, since many ISPs seem to have given in to pressure like those exerted by New York Attorney General Cuomo[275], who appears to depict Usenet as the primary method for spreading paedosexual content, despite evidence suggesting that the problem is no more prevalent than it is on other internet medium.

For example, AT&T ended their Usenet service after dealings with the New York Attorney General. Unable to effectively monitor the content of the newsfeed they offered their customers, AT&T now refers its subscribers to alternative news providers which, incidentally, often offer unfiltered access to many more groups, and do so with longer retention times.[276] As a result, it could be argued that this initiative has lead to more child pornography being available to more consumers and for longer than would otherwise have been the case.

Unlike emails, which are limited in size, per message filtering is more difficult since binary files are often stretched out over many messages using encoding techniques. In practice, this means that only by shutting down parts of the Usenet hierarchy on their own servers do ISPs have any form of effective influence on the spread of paedosexual content through Usenet.

As the example shows, over-blocking is a major concern here. The practice of blocking entire groups or even hierarchies leads to many innocent discussions being blocked in the process. After the shutdown of the alt.* (where * stands for every group hosted under the 'alt.' tree) hierarchy by Verizon a Cnet reader was, by way of example, quoted as saying "This is ridiculous. I actually met my wife on `alt.personals`, 14 years ago... I still use usenet - there are a lot good discussions and a person can get answers to questions on specific topics pretty quickly. It's nice to have a decentralised place to hold discussions, one that is not beholden to a sysadmin to correctly run a forum, one that's free of blinking gifs and flash ads."[277]

Although Internet Access Providers are usually not outspoken on this issue, privately they 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.

---

[274] Cf.An example of overblocking, where the entire alt.* hierarchy was blocked by Verizon is available on Ars Technica, alt.blocked: Verizon blocks access to whole USENET hierarchy, http://arstechnica.com/old/content/2008/06/alt-blocked-verizon-blocks-access-to-whole-usenet-hierarchy.ars

[275] Cf. EFF, Jennifer Granick, More ISPs decide to Filter Usenet Newsgroups (2008), http://www.eff.org/deeplinks/2008/07/more-isps-decide-filter-usenet-newsgroups

[276] See: http://my.att.net/NewsGroup; commentary on http://www.zeropaid.com/news/86599/att-quits-free-usenet-access-july-15th/ amongst others. Other, paid services could be the likes of Supernews, Giganews, and Usenet.com.

[277] See "Verizon offers details of Usenet deletion: alt.* groups, others gone, http://news.cnet.com/8301-13578_3-9967119-38.html

5.4.5 Search engine results blocking

In order to prevent users from accessing illegal material, it is possible to prevent access to search results at the level of search engine providers. A provider like Google, for instance, could then decide to block every query for a keyword like "child pornography".

This would, in turn, invariably lead to over-blocking, since not every appearance of such a keyword is generally speaking, illegal. In order to judge whether or not to block results either a more detailed analysis of the context would be needed, which is not easy to automate. Alternatively human analysis could be done of suspicious content, identified by keyword searches, but this would lead to very high costs for human analysis of billions of indexed pages.

Another important question is the visibility of filtering, as displayed in the results pages of search engines. Some providers clearly state the filtering of results, others do not.[278]

Lastly, circumvention of this filter is easy: simply accessing the content directly would be sufficient. Although non-indexed content is not as easy to find for a new content consumer, direct exchange of URLs, optionally through dedicated websites or IM channels, could achieve much the same result, providing for easy circumvention.

[278] We found that the Dutch version of ask.com states clearly it has filtered the results when searching for child pornography. The English language (US) version does not. Google does not state whether results have been filtered either.

5.4.6 Peer-to-peer and IM Blocking

Blocking attempts of peer-to-peer traffic is a substantial task if done at a non-user level. In addition to some traffic being encrypted, it can be difficult to identify P2P and IM traffic from a technical networking perspective. 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. To make matters more complicated, mechanisms exist to alternate port numbers, which are normally used to differentiate traffic categories (like traffic to www, email and news servers).

Peer-to-peer file exchange operates largely independently of regular internet addressing schemes. With the exception of IP addresses, no further centralised conventions for identifying content are available, except for the search and download functions provided in the particular p2p application being used by the end-user.

- 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, however, is then the only remedy available. Since content is widely spread, internationally and across networks, the availability of the content involved will probably not be affected unless many countries and ISPs co-operate in a concerted fashion. In addition, retrieving these files, for human analysis or comparison to hash-based signatures, is very resource intensive.

- 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 or even to identify packets (p2p traffic) used for file-sharing. This would involve routing all traffic through central (DPI) systems and extensive efforts to rebuild the full content arriving as parts from distributed p2p networks, in order to be able to classify the contents. Alternatively, discrete parts of the content could be made into signatures thus lowering the traffic load on the DPI scanning system but leading to a much bigger block-list and a resource intensive matching process (parts of a file would need to be identified, and matched, which is not as easy as hashing an entire file).

  This strategy, with current broadband speeds, would require immense investment in order to maintain effective usability of the connections involved. It also leads to a major intrusion into the communications privacy of end users, since only a tiny minority of all traffic analysed would contain this illegal material.

  Implementing DPI is a big investment and to implement p2p content blocking for specific files, would require major efforts to classify online content. In addition the risk of under-blocking seems omnipresent given the vast quantities of data being exchanged in modern day p2p networks.

Given these technical difficulties, Internet Access Providers and private organisations come under pressure to block this type of traffic altogether, resulting in significant over-blocking. Circumvention of this type of technology is not easy but, again, usage of tunnels or proxies could well lead to effective circumvention of many DPI scenarios.[279] Encrypting the exchange of file-parts is also an effective way to circumvent a DPI blocking strategy. Already peer to peer networks like freenet are using encrypted file transfers in a system that provides ample room for a plausible deniability defence if one of the peers should be charged with being involved with spreading illegal content.

[279] Cf. The Pirate bay (a well known torrent website) has it's own VPN service ("Ipredator") (http://www.wired.com/threatlevel/2009/06/ipredator/)

Similar problems exist when it comes to instant messaging networks. Although here file exchanges are easier to recognise, since they are performed by the IM software, which is usually centrally organised and not distributed in design, having them all routed through central infrastructure is still quite an investment. Often, therefore, IM programs will exchange files directly between two peers on the IM network, thereby defying any central (signature) filtering scenario.

Given these technical challenges, the chance of effectively taking measures to block child pornography on p2p an IM networks seems low without the use of DPI technology. Using this technology, in turn, would lead to a significant intrusion into the communications privacy of all Internet users and would require massive investment.

5.4.7 Overview

This table gives an overview of the previous discussion. It lists characteristics of every blocking strategy discussed. It shows the likelihood off over- and under-blocking according to our estimates and lists the resources required to execute the blocking strategy.

It shows the block-list type and maintenance effort required for such a list and, in the last column indicates whether the communications contents will need 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 recognitiontectechnology 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	+

5.4.8 Conclusion

While the distribution methods described here vary widely, it is important to note that the target content spread using them remains the same throughout. It is either pictures or video files that are the primary targets of child pornography blocking efforts. This means that, whilst the distribution method may vary, in practice these methods function as reasonable substitutes for each other. 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 likely lead to replacement of 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.

It would also seem likely, therefore, that blocking efforts on public media such as websites or email spam, will lead to a move to more hidden platforms such as "darknet" p2p networks or direct file-sharing (with vetted IM communities). From a technical perspective, the same sharing functionalities can be achieved with these, whilst further encryption and anonymisation of the file sharing process seems a likely result if users have no other (technical or moral) inhibitions. This is a crucial consideration when assessing the purpose and proportionality of any given blocking approach.

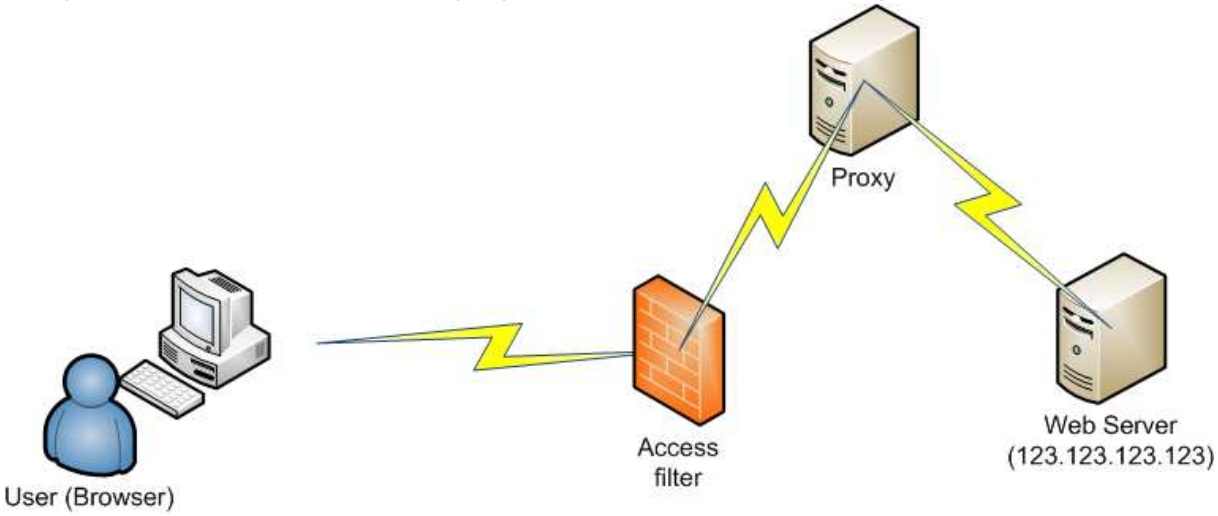
5.5 Evading Internet Blocking

5.5.1 Proxy-Servers

Circumventing this type of filter is quite trivial when the end user can use the services of a foreign proxy server (another machine outside of his ISP's or organisation's network, or even outside of his country). A proxy server is very common and most Internet Access Providers operate one on their network.

The purpose of a proxy server is to accept requests for web-pages from users, to fetch the content requested from the remote website and, optionally to cache the content locally. When a second user asks for the same cached content, the page will be available locally for the second user. 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, can thus gain access to the content to bypass local filtering.

Configuring a web-browser to use such a proxy-sever to retrieve content is a very straightforward exercise and some programs even do it automatically.



A great number of anonymising proxy servers are available on the Internet - some free, some paid. An anonymising proxy-server does not tell the remote web site who the original request came from, thereby protecting the anonymity of the original requestor. In real life scenarios the effectiveness of this website blocking strategy is therefore mediocre at best.

5.5.2 Tunnelling

Another technique to evade a filter, which requires more technical knowledge, is to use tunnelling protocols. 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.

Users use tunnelling protocols to access content from a different location. A tunnel to another machine is then used to connect to the internet from that machine, thereby evading a filter on the internet connection of the end user. This works, even if all web traffic is forced through a local filter, since the traffic inside the tunnel can not be reconstructed due to heavy encryption that is usually implemented to secure the tunnel.

Prohibiting tunnelling technology altogether in an Internet Access Provider's filtering system is virtually impossible since many companies have multiple sites around the world and use this technology to link office networks together. It would therefore be disproportionate, due to its widespread legal use. Similarly tunnelling technology is often used to secure distance working systems and to secure a myriad of transactions to sensitive systems or to secure "home office" environments.

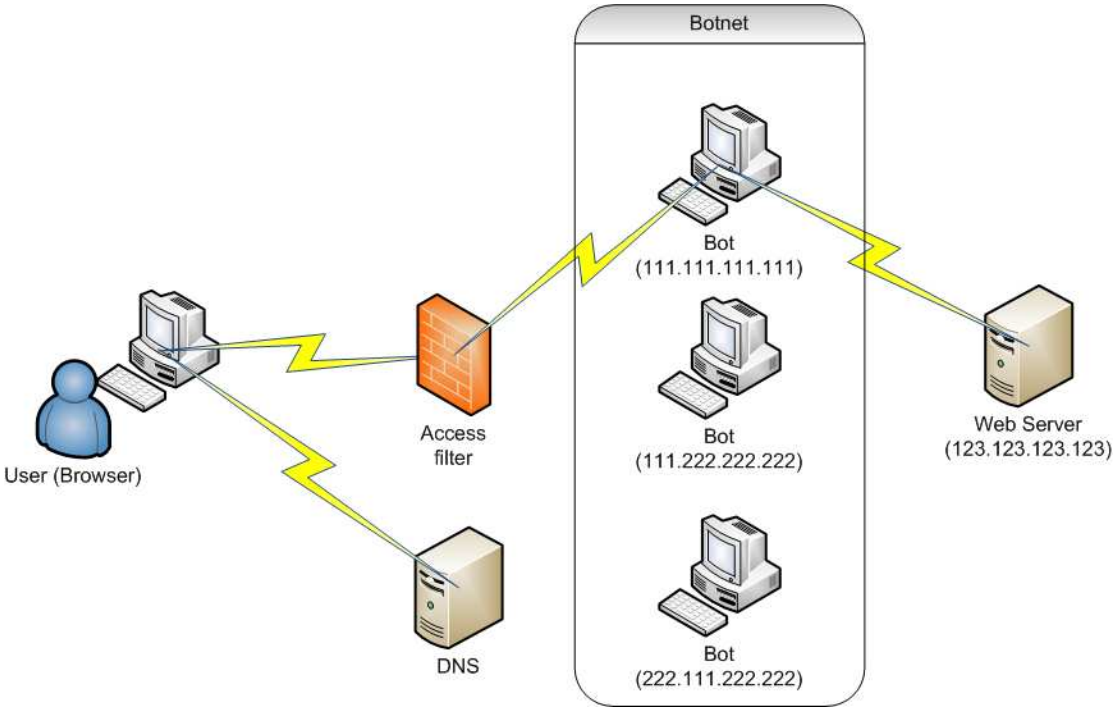
5.5.3 Hosting or URL rotation

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.

Frequent changes in the domain-name could be used to bypass filters based on URLs.

5.5.4 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 (or deflector) to the content of the web server.[280] In essence, the user's computer is turned into a non-caching proxy. They serve the content to anyone requesting it, taking it from elsewhere and relaying it to the requestor.



Instead of advertising one IP address for the content in the DNS, the content owner can now typically advertise various addresses of compromised machines in quick succession. A user who sends a request for the content to the DNS is forwarded to one such IP address of a bot. The bot will then connect to the actual content residing on a central system which sends the content back the compromised machine which in turn relays it back to the user. This would easily circumvent IP address based filters, with the exception of filters able to meet the high maintenance costs of tracking this content and the compromised machines (bots) involved in making it available.

With botnets of thousands of machines not being uncommon, spreading child pornographic content this way is also very anonymous since the address of the backend server, the one that actually holds a copy of the content and is usually easily connected to the publisher, is hidden from the end users and the IP address of the portal or proxy sites (bots) can be changed at very short intervals. Secondly no logs will be kept by the compromised machine that could aid identification of the visitor.

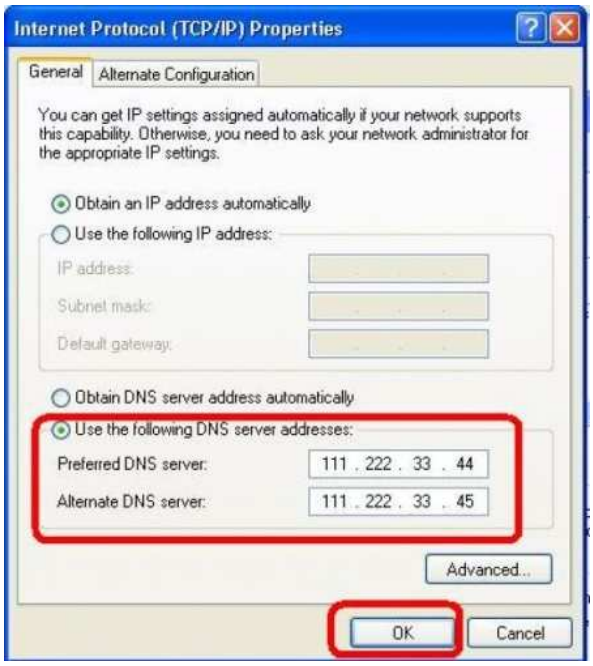
[280] Statistics on fast flux hosted sites are scarce but a good oversight of the problem is available through the ICANN GNSO fast-flux working group:
http://gnso.icann.org/files/gnso/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf
Some statistics for just one domain are available at:
http://www.honeynet.org/node/143

5.5.5 Evading DNS based filters

Even easier to bypass is blocking at the level of the DNS query.

This is the type of filtering technology was adopted in many western countries where child pornography filters were mandated or facilitated by the state government in co-operation with law enforcement or private parties.[281] This blocking method will usually intercept DNS queries and replace the answer of a query to a DNS server (usually one that is in use by an access ISP to connect its customers) with a different IP address than the one where the original content resides. This allows the operator of the filter to display alternative content, like a warning page.

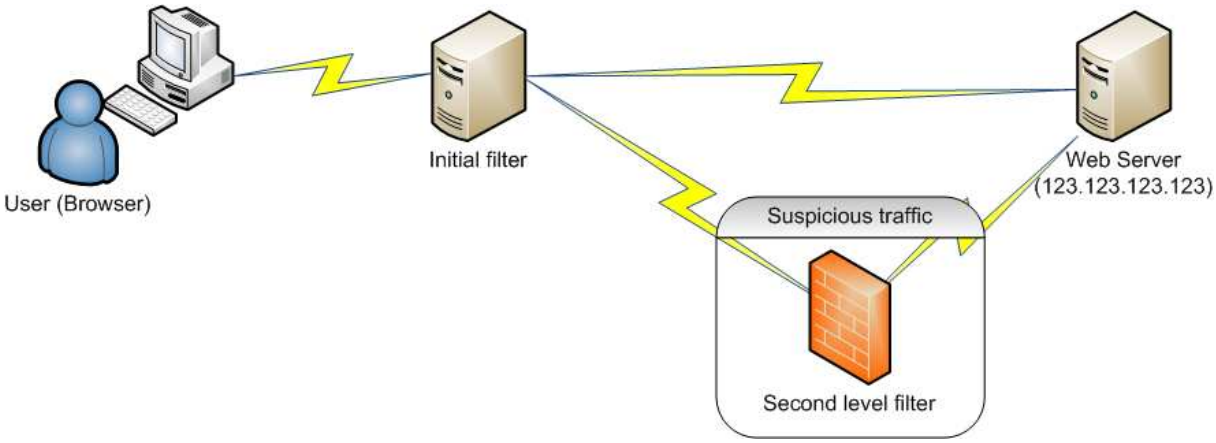
Merely changing the DNS server of the provider to a different one (which is not part of the blocking system) is enough to totally circumvent this blocking method. On top of that, many paid and free DNS servers exist on the Internet that can give answers without filtering queries.



[281] See Chapter XX p.

5.5.6 Other filters

Next to these simple blocking strategies, more specific filters can be employed to monitor **all** traffic flowing to websites by using ***file signatures***. This would usually involve a technology called ***deep packet inspection*** (analysis of the content of all traffic) or using a proxy and checking all downloaded web content against a list of known illegal content signatures. Since this is extremely resource intensive, this strategy is usually only observed at the organisation/business level, where the organisation bears the cost for the filter and agrees to the performance impact on the network.



An alternative to overcome this burden in an ISP or even country wide filter is using a hybrid system which combines several elements mentioned above into one blocking system. For example, British Telecom designed a system that reduces the network-performance impact by using a combined filtering strategy. Under the project name of BT CleanFeed they developed this hybrid system. It works by isolating traffic destined to suspect IP addresses or IP address ranges and making this traffic undergo further targeted filtering at a more detailed (URL based) level.[282] This second stage filter then makes the decision whether to block parts of the requested content or not or simply record the request has been made.

Although this may seem like a relatively effective solution, it was also proven to be open to a so called '***oracle attack***' where users could potentially use the system to identify child pornographic web-sites by closely analysing the system response when it was asked to access (previously identified) suspicious IP address ranges.[283] The filter itself thereby, became a source for information on the location of illegal content, contradicting its primary purpose in the process.

Although technical measures are possible to prevent these type of attacks it is important to note that more complex filtering strategies could well cause software reliability and network security concerns and impacts.

[282] Clayton (2005) see http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf (last accessed 1-Oct-2009)
[283] Clayton (2005), par. 4 and further

5.5.7 Conclusion

In terms of effectiveness, all of these blocking strategies suffer from similar downsides.

- Firstly, where blocking is done on anything other than a full url (path name) or a content signature, there is a significant potential for blocking more content than was intended. Domain names and IP addresses are not specific enough to always block with the required precision. This is sometimes considered acceptable collateral damage which is accepted by some to be proportionate when the type of content which is being blocked is taken into account, but may not be acceptable for all types of content. The legal and democratic issues highlighted in Chapter 6 should be taken into consideration.

- Secondly, 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. This requires the network architectural design and infrastructure to cope with wide-scale interception of traffic AND content data.

  For example, in the British Telecom project, their configuration, design and implementation costs were estimated around £1m.

Whereas previous requirements for Internet Access Providers requires them to have capacity to provide interception capability on a small number of court-ordered interceptions on known users, the scaling of such a system to manage ALL customers of an Internet Service Provider is extremely technically challenging and could not be done with any level of guaranteed success.

It can also be a significantly invasive system since access to all traffic and content of a user's communications is possible with this type of technology and all requests for data by all users need to be reviewed and matched against a blocking list. There are substantial legal and democratic obstacles to such an approach which are illustrated in Chapter 6.

All web blocking strategies are prone to circumvention in one way or another, DNS filters being the easiest to circumvent, despite being the architecture of choice in many countries that have child pornography blocking schemes. Filters may also have an adverse effect where the filter itself is being used as a tool to pinpoint illegal content – either via the technological methods described above or as a result of the almost inevitable leaking of the blocking list from time to time – all such systems create a single point of failure in an Internet infrastructure whose huge success substantially due to having no such centralisation in its own design.

Filters also 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 leading to them as operators of the website AND take steps to relocate their services to a new domain, IP address, country or hosting service anywhere else in the world. They can also 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 frequently. These movements can also be tracked and can offer useful intelligence to investigators tracking their movements and may provide useful research data on how quickly they move, how often they change ip or dns addresses or move to a new hosting provider or a new country. All this information can be very useful for investigators.

- It is worth noting that 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 (in addition to increasing the costs for the criminals) this will lead to mistakes occurring sooner. However, such resources and effort are comparable for those creating an Internet blocking system.

5.6 Implications for a democratic society

5.6.1 Introduction

This section aims to review the potential for collateral damage both in terms security and in terms of human rights. It also examines the potential for extension of internet blocking to areas beyond child pornography from a technical perspective.

5.6.2 Security issues

Security of any blocking operation is of prime concern. By design, the infrastructure required to execute a blocking strategy is capable of interfering with many critical elements of end users' internet connections. It is important to remember that one of the original design criteria for the use of the Internet was to have a trans-national communications system which would be resilient to failure, disruption, tampering *and,* as a result*,* blocking.

Therefore, the physical and technical security of these systems needs to be thoroughly reviewed in order to safeguard the proper and proportional functioning of the system. Implementing blocking in any infrastructure, therefore, adds security risks and failure points which, eventually, will need to be weighed against the positive effects of the blocking effort.

In addition, the content of (non-dynamic) block-lists is of prime interest to paedosexual offenders. They have strong motivation to use the blocking list for the opposite reason to the one that it was designed: by looking at it as a source of content (or, in the words of Clayton (2005): an oracle).

This problem can be part overcome by not transmitting or storing the content of the list in plain text format. Instead cryptographic hashing is often used to encode the content. A check on the list is then performed by hashing the requested URL or IP address and matching it against the hash database. Although this provides some security, it is not sufficient when it is used to identify lists of blocked IP addresses since these are limited in number and it is entirely possible to calculate all of their hash values in advance,[284] in order to find the entries. Therefore, additional security measures are needed to secure IP address lists in every organisation that uses such lists.

As highlighted before, Richard Clayton (Clayton 2005) discovered a method of identifying the contents of BT's hybrid "CleanFeed" blocking system. By analysing answers to specially crafted queries on a CleanFeed filtered internet connection, he showed it was possible to identify IP addresses that host child pornographic content that is filtered by BT CleanFeed.[285] Although his method requires some insight into which IP addresses are likely to host this content, in order to be practical, the example goes to show that any blocking methodology may raise additional security concerns that need to be taken into account and balanced against the expected benefits. The complexity of implementing secure blocking methods should not be underestimated.

Lastly, where security measures are required to avoid leaking the contents of a list, it becomes challenging to monitor the operation and effectiveness as well as the proportionality of a block-list operation. This is especially problematic in a scenario where the block-list is maintained by a government-funded body and may lead to concerns about the checks and balances in a democratic society[286]. A good example is the ACMA (Australian Communications and Media Authority (an independent government agency) block-list which was

[284] Resulting in a database of all ip addresses (4.2 billion) and their hash values.
[285] In technical terms, he set a low TTL in the SYN packet used in an HTTP request to a "known-to-be bad" IP address range. He found that the proxy would then emulate the three way TCP-IP handshake by replying with a SYN/ACK whereas unfiltered ip addresses would not be reached due to the low TTL, which would cause a reset (RST) response.
[286] Discussed in detail in Chapter 6

inappropriately published on the Internet and allegedly contained entries to the websites belonging to both a Queensland boarding kennel and a dentist.[287]

5.6.3 Over-blocking and Under-blocking

A major issue with any of these strategies is the problem of over- and under-blocking. Although it cannot easily be prevented in its entirety, inaccurate blocking can be significantly reduced by extensive human intervention in qualifying the blocked content and by using very specific identifiers (full URLs or hash signatures for instance) on the block-list and by adopting technology which uses this level of detail in the blocking decision.

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 limiting access to 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.

Under-blocking is also a universal phenomenon especially present in the more proportionate and specific blocking strategies. Finding and maintaining lists of all identifiers for illegal content requires a substantial effort on the part of block-list operators and a great deal of trust in their objectivity and ability to judge content based on legally specified criteria.

Whilst the potential for wrongful blocking decisions can vary depending on the blocking strategy, the most important conclusion here is that no strategy appears to fully avoid both of these phenomena. Weighing the need for blocking child pornographic content should therefore be done in the knowledge that both substantial over- *and* under-blocking remains likely.

5.6.4 Mission creep potential and re-territorialisation

It is important to note the intrusive nature of many of the blocking strategies that were discussed in this chapter. Especially the more granular, content-based filtering mechanisms (hash signature or URL based filtering primarily) 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 technology employed is in many ways comparable to features of wiretaps used by law enforcement on specifically judicially sanctioned targets. Implementing this technology in a public network means a significant amount of information is added to the network operators' logs. With its implementation comes a real risk of pressure from other areas of debate that could profit from the availability of these systems in order to use them for other purposes.

Areas where such a mission creep potential seems likely are debates ranging from copyright holders, who will be looking for methods to block the illegal spread of copyright protected material, to gambling, where governments with restrictive gambling regimes aim to limit the availability of services of foreign operators on their soil.

Whereas it is important that this public debate take place, it will need to 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. 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.

Blocking systems are rarely designed for large scale blocking of a wide variety of content as countries such as China and Saudi Arabia have discovered.

[287] The Australian, March 20th 2009, Internet filter list of porn exposed http://www.theaustralian.news.com.au/story/0,25197,25213542-2702,00.html

5.7 Conclusions

Blocking attempts are best done using strategies that require human intervention. Dynamic blocking is often observed as incomplete or wrongful (under- and over-blocking). Even then, no blocking strategy can completely prevent over- or under-blocking of content entirely.

An added challenge is that of identifying the sites to block. The fact that adults with a sexual interest in children often use private communication channels rather than very visible and detectable internet technologies such as websites or untargeted email will make fully blocking their activity virtually impossible.

Since Internet content can be exchanged over several media, the practice of blocking only a limited number of media (such as blocking only traffic to web-servers) may also easily cause substitution of 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, and therefore the proportionality of web blocking can only be demonstrated by showing that this is a significant problem. It seems unlikely that blocking strategies, as outlined in this document, are capable of substantially or effectively preventing crime or re-victimisation.

In addition, the security of the blocking list and blocking scheme is of prime concern. Instead of merely acting as a list of unwanted content, those with a compulsion for this type of content will endeavour to gain access to these lists of illegal content.

Lastly, due to the generic nature of the technology required to attempt many blocking scenarios, a risk of mission creep is always present whether intentional or otherwise. Whilst it may be implemented for one reason, the same technology can be applied for other purposes – either with or without public debate. Indeed, such technologies can be used for wide scale monitoring of Internet activities without using the intrinsic blocking capabilities. For example, this can permit live monitoring of foreign website usage without having access to that websites records.

Chapter 6 INTERNET BLOCKING AND THE LAW

6.1 Introduction

The preceding chapters have shown that the blocking of 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.

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 chapter 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 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. This chapter will

Which law?

The term "law" has many different definitions. Law can be defined as "*each standard or system of standards, of legal or extra-legal order*". This definition includes ***natural law***, which is the "*rules of conduct supposedly inherent in the relations between human beings and discoverable by reason*", and ***positive law***, which refers to "*all the rules of conduct that are in force in a given country at a given moment"* More precisely, the term of "law" can refer only to "*provisions that are voted by a Parliament; Law (is here understood) in its organic and formal meaning, as opposed to decree, regulation, ordinance, administrative orders but also to Constitution*"

The concept of law in this study is accepted as positive law, unless otherwise indicated, which includes, at a country level, the valid provisions voted by the Parliament, but also the provisions coming from decree and other administrative orders and texts, court orders and, when relevant, international and European provisions that the local system recognises and which need to be respected. European law itself will be understood as the set of valid provisions established and enforced by the European Union institutions and their interpretation by the European Court of Justice. International law refers to provisions whose subject matter is related to situations concerning several States, or which source is international coming from an institution or a Court outside the European Union's institutional structure.

* Translated from French. Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique*, 7th ed., Quadrige/PUF, June 2005, page 549, 682.
* Webster's New World Dictionary, Third College Edition, 1988, page 903.

analyse each of these areas in greater detail to enable a conclusion on the conditions under which Internet blocking might be considered acceptable under legal principles.

On this basis, section 6.2 briefly outlines why attempts at Internet Blocking and Fundamental Freedoms need to be considered in unison. Section 6.3 considers the links between these Rights and Freedom in the first place and Democracy in the second place. Section 6.4 highlights the differences between Human Rights, Fundamental Freedoms and Civil Liberties. Section 6.5 reviews the nature and legal value of texts that proclaim these Rights and Freedoms. Section 6.6 then describes the Fundamental Rights that are in conflict with Internet Blocking and section 6.7 looks at rights that would support Internet blocking measures. Section 6.8 gives an overview of the specific provision relating to Electronic Commerce in the European market and the liability of Internet Service Providers as they relate to Internet Blocking.

Chapter 7 examines how such fundamental rights are balanced with other rights in society and how conflicts can be assessed and mediated. It evaluates the range of Internet Blocking activities under consideration today and compares them with the proportionality criteria of the conflict resolution steps described within the chapter. That chapter also provides some commentary with reference to which legal contexts whereby attempts at Internet blocking might be acceptable in a democratic society.

This review is particularly useful for those countries that are debating the legitimacy of Internet blocking to know how to respect the Human Rights and Fundamental Freedoms or other specific provisions that could limit the possibility of Internet blocking.

6.2 Internet Blocking and Fundamental freedoms

Numerous national legal systems, including 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. Indeed, attempting to block Internet content or Internet communication supposes one to have the right to do this blocking and the right to deprive some people of the right to access such content or to use a communications protocol while some other persons would be deprived of the right to communicate specific content to some people or by a particular means.

These rights and freedoms do not always have the same legal force according to the original documents which advocate them and the specific legal texts which implement them in a given national system. This increases the confusion that can be sometimes felt when approaching the notion of human rights and fundamental freedoms.

However, it is also noted that some countries might not have chosen to respect human rights and fundamental freedoms.

6.3 Role of Democracy

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[288], are often considered as intrinsic in democracy[289]. However, defining Democracy and establishing a clear link between such a political system and preservation of freedoms is not as easy to do is it appears at first glance.

There are several definitions of democracy[290], and "*political scientists and observers*" themselves "*do not agree on how many democracies there are in the world (and) differ on how to classify specific regimes, the conditions for making and consolidating democracy, and the consequences of democracy for peace and development*"[291]. However, it is possible to basically say that democracy is at least a "*people self-governing*"[292], a form of "*government in which the people hold the ruling power either directly or through elected representatives*"[293]. In those circumstances where "*rulers are elected*"[294], democracy can be defined as "*a system for choosing government through free and fair electoral competition at regular intervals"*[295].

However, democracy specialists often agree that "*there is no reason that electoral democracy and liberty must go together*"[296]. Prof. Larry Diamond explains that the concept of liberty "*came about before democracy both in England and, in varying degrees, in other European states"*, and that, today, "*there are many illiberal democracies, with human rights abuses and civil strife*"[297].

6.3.1 Democracy and Fundamental Freedoms

There are also three other aspects where the relationship[298] between democracy and freedoms can be seen.

- Elections
  The first aspect is the principle of the right of participation of everybody in public life. The (theoretical) possibility for everyone "*to compete for political leadership by presenting himself to the electorate (…) will in most cases (…) mean a considerable*

[288] See above section 6.6 and 6.6.2.
[289] See for instance "Democracy", Wikipedia, the free encyclopedia, available at: http://en.wikipedia.org/wiki/Democracy.
[290] See for instance Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, p. 31: "*A key element in all these debates is lack of consensus on the meaning of democracy…*".
[291] Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, page 31.
[292] Translated from French. Larousse encyclopédique en couleurs, France Loisirs, Librairie Larousse 1978, tome 6, page 2660.
[293] Webster's New World Dictionary, Third College Edition, 1988, page 366.
[294] Adam Przeworski, "Minimalist Conception of Democracy: A Defense", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, *the democracy sourcebook*, p. 12.
[295] Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, page 29. See also Joseph Schumpeter, "Capitalism, Socialism, and Democracy", in Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, *the democracy sourcebook*, p. 9 ("another theory of Democracy"): "*the democratic method is that institutional arrangements for arriving at political decisions in which individuals acquire the power to decide by means of a competitive struggle for the people's vote*".
[296] Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, *the democracy sourcebook*, p. 30.
[297] Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, p. 30. The author concludes: "*These two facts have rekindled intellectual interest in liberal autocracy as a better, safer, more stable form of government for many transitional societes*".
[298] See Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, p. 30: "*liberal democracy provides, by definition, comparatively good protection for human rights*". See also Joseph Schumpeter, "Capitalism, Socialism, and Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, page 11: the "*democratic method does not necessarily guarantee a greater amount of individual freedom that another political method would permit in similar circumstances (…) but there is still a relation between the two".*

amount of freedom of discussion for all", which will normally ensure, *"in particular",* a *"considerable amount of freedom of the press"*[299].

- Separation of Powers
  The second aspect is the institutional structure which includes the separation of powers, as this "*limits the arbitrary and prevents abuses linked to the exercise of sovereign tasks*"[300].
- Fundamental Rights
  This third aspect, which appears as fundamental, and perhaps exists as a real consequence of democracy, takes into account the general will of citizens at a given moment, reflects the State's willingness and engagement to respect freedoms, in the general and citizens' interest, and to establish and maintain national and/or international peace.

Historically, many States choose, at a national level or/and at the international level, to legally proclaim some human rights and fundamental freedoms - often after a civil war, a revolution or national events of substantial violence. These proclamations are intended to act as a code of rights which Governments can not easily repeal, whatever the evolution of society's fears and political priorities. Furthermore, the preservation and promotion of these fundamental rights is considered as "*an ideal*" for democracy, which is itself considered to be "*the best way of achieving these objectives*", being also "*the only political system that has the capacity for self-correction*" [301].

6.3.2 Liberal Democracies

Numerous European democracies took this approach as can be seen in their texts that currently proclaim human rights and fundamental freedoms, which has led many to deem democracy as synonymous with the protection of human rights. Those European countries have generally a "*constitutional government*", which, "*as Locke, Montesquieu and the American Federalists asserted*", restrains and divides "*the temporary power of the majority*" and can in that way "*protect individual freedoms*". Prof. Diamond states that "*this fundamental insight (and value) gave birth*" to the "*concept (of) liberal democracy*", which he defines as "*a political system in which individual and group liberties are well protected and in which there exist autonomous spheres of civil society and private life, insulated from state control…*"[302].

Taking this definition as ours, we can say that the preservation of freedoms is a choice of liberal democracies, and that democracies that would like to be considered as liberal should preserve these rights, even within the framework of a blocking measure.

---

[299] Joseph Schumpeter, "Capitalism, Socialism, and Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, page 11: "*If, on principle at least, everyone is free to compete for political leadership by presenting himself to the electorate, this will in most cases though not in all mean a considerable amount of freedom of discussion for all. In particular it will normally mean a considerable amount of freedom of the press*". See also Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, p. 32: "*Minimalist conceptions of electoral democracy usually also acknowledge the need for minimum levels of freedom (of speech, press, organization, and assembly) in order for competition and participation to be meaningful*".

[300] Translation from French. Vie Publique, La Documentation Française, available at : http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/separation-pouvoirs.html, quoting powers' separation theoreticians as Locke and Montesquieu

[301] See for instance the "Universal declaration on democracy" adopted without a vote by the Inter-Parliament Council at its 161st session, http://www.ipu.org/cnl-e/161-dem.htm, Article 3: "As an ideal, democracy aims essentially to preserve and promote the dignity and fundamental rights of the individual, to achieve social justice, foster the economic and social development of the community, strengthen the cohesion of society and enhance national tranquillity, as well as to create a climate that is favourable for international peace. As a form of government, democracy is the best way of achieving these objectives; it is also the only political system that has the capacity for self-correction" (adopted without a vote because after the Declaration was adopted, the delegation of China expressed reservations to the text).

[302] For all these quotations, see Larry Diamond, "Defining and Developing Democracy", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, p. 29

This study will therefore analyse the rights that might be endangered by a blocking measure, in comparison to those rights that might justify such a measure. This analysis will allow each liberal democracy to understand the meaning of each of these rights and the conditions under which blocking might intervene in limiting some of them. Before beginning such an important study, it is important, to promote public debate by explaining the difference between human rights, fundamental freedoms and another notion that is frequently considered, that of civil liberties.

6.4 Human Rights, Civil Liberties and Fundamental 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 that proclaims that right and the importance given to protecting the latter. Beyond that, 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.

6.4.1 Human Rights

Human rights have been defined as "*inherent in the Human Being (man or woman); a set of rights considered as belonging naturally to each Human Being*"[303]. Other authors consider the concept of human rights as referring "*to the sources of the 'natural law' and to the texts that have first proclaimed such rights, at a national level (Bill of Rights of 1689,* (French Human and Citizen Rights) *Declaration of 1789…) or internationally (San Francisco Charter of 1945, Universal Declaration* (of Human Rights) *of 1948, New York Covenant of 1966, Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (…)"*)[304].

Within the "Human rights" category, some authors distinguish between

- Human rights of the first generation, "*of liberal inspiration (individual, civil and political)*"
- Human rights of the second generation, "*of socialist leanings inspiration*" (economic, social and cultural, implying a State's positive action)
- Human rights of the third generation, "*of third-world inspiration*" (Human and people rights, collective, so called "*of solidarity*": right to development, to preservation of world heritage sites")[305].

6.4.2 Civil Liberties

This notion of human rights is older than the notion of civil liberties, which is considered itself as designating "*a form of legal consecration of Human Rights*" [306]. The notion of civil liberties appeared in France with the Constitution of 14 January 1852 and is today mentioned in article 34 of the French Constitution of the 4th October 1958 and in some French legal texts.[307] International texts, declarations and conventions are also making more frequent references to this notion[308].

Civil liberties are limitations of the powers of the public authority[309] towards citizens, and include "*personal liberties*" and "*collective liberties*"[310]. As regards personal liberties,

- Professors Robert and Duffar give first priority to the "*individual or physical freedom, which means freedom of movement, to not being arbitrarily arrested or sequestered, to be judged with all legal guarantees (…), to not being affected in one's physical integrity or privacy…*"[311].

---

[303] Translated from French. Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique*, 7th ed., Quadrige/PUF, June 2005, page 330.
[304] Translated from French. Dominique Turpin, *Les libertés publiques*, mémentos, Gualino éditeur, 5th ed., 2000, page 11.
[305] See, for the discussion and quotations (translated from French), Dominique Turpin, Les libertés publiques, mémentos, Gualino éditeur, 5th ed., 2000, page 11.
[306] Translated from French. Droit des libertés fondamentales, collectif, under the coordination of Louis Favoreu, Dalloz, 3rd ed., 2005, n° 57.
[307] See Dominique Turpin, *Les libertés publiques*, mémentos, Gualino éditeur, 5th ed., 2000, page 11.
[308] François Terré, "Sur la notion de libertés et droits fondamentaux", in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11ème ed., 2005, page 5, n° 10.
[309] Claude-Albert Colliard, *Libertés publiques*, Dalloz, 6th ed., 1982, page 23.
[310] Jacques Robert and Jean Duffar, *Droits de l'homme et libertés fondamentales*, ed. Montchrestien, 7eme ed., 1999, page 27.
[311] Translated from French. Jacques Robert and Jean Duffar, *Droits de l'homme et libertés fondamentales*, ed. Montchrestien, 7eme ed., 1999, page 27.

- As a second priority, they cite the "*freedoms of spirit*", that means "*freedom of opinion, of religion, of the press, to teach*" and economic freedoms, which are the "*right to work, the freedom of commerce and industry*".
- Their third priority consists of collective freedoms which are "*the freedom of assembly, the freedom of trade-union activity, the freedom to strike…*"[312] [313].

6.4.3 Fundamental Freedoms

To the notions of human rights and civil liberties, has been added the notion of "fundamental rights" or "fundamental freedoms". These rights and freedoms, which belong both to natural persons and legal entities, can be defined as Prof. Louis Favoreu did: "*Fundamental Rights and Freedoms are,*

- *firstly, protected against the executive but also against the power of the Parliament; while Civil Liberties – under the classic French Law interpretation – are mainly protected against the executive…*
- *Secondly, Fundamental Rights are guaranteed not only by the Law but above all by the Constitution or by international and supranational texts.*
- *Thirdly, the protection of Fundamental Rights requires, protection from the executive and the parliament, through the application of the Constitution (or international texts), which is the competence not only of ordinary judges, but also of constitutional judges and even international judges*" [314].

[312] Translated from French. Jacques Robert and Jean Duffar, *Droits de l'homme et libertés fondamentales*, ed. Montchrestien, 7eme ed., 1999, page 27.

[313] Sir François Terré gives to civil liberties the same content. He distinguishes these civil liberties, which are rights that govern before all the relations between individuals and the public authority, and "*subjective rights*", which underlie Human Rights, can be seen as civil liberties extensions and principally govern "*relations between private individuals or groups, either in their relations between each other, or in their relations with goods*". Subjective rights belong to one person (see Gérard Cornu, Association Henri Capitant, Vocabulaire juridique, 7th ed., Quadrige/PUF, June 2005, page 874) and have "*clear structure and content: letter of credit, property right, usufruct right, easement right".* For the quotations see François Terré, "Sur la notion de libertés et droits fondamentaux", in Libertés et droits fondamentaux, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, page 5, n° 12, 13 and 15. See also François Terré, *Introduction générale au droit*, Précis Dalloz, 6th ed., 2003, page 160

[314] Translated from French. François Terré, "Sur la notion de libertés et droits fondamentaux", op cit, page 7; see also Serge Guinchard, "Le procès équitable : droit fondamental ?", AJDA special n° of 20 July - 20 August 1998, page 191. Both authors quoted especially Louis Favoreu, "Universalité des droits fondamentaux et diversité culturelle", in L'effectivité des droits fondamentaux dans les pays de la communauté francophone, colloque international de l'île Maurice, 29th Sept.-1st Oct. 1993, AUPELF/UREF 1994, page 48. For other analysis of the Fundamental Rights notion, see for instance Véronique Champeil-Desplats, "La notion de droit "fondamental" et le droit constitutionnel français", D. 95, page 323. For a "outline of a fundamental rights theory" (Esquisse d'une théorie des droits fondamentaux), see also *Droit des libertés fondamentales*, collectif, under the coordination of Louis Favoreu, Dalloz, 3rd ed., 2005, n° 70 and seq.

6.5 Instruments Preserving Human Rights and Fundamental Freedoms

The first texts that declared human rights and fundamental freedoms were national. International texts came after the second world war and contributed to modifying local legal systems. Their content was subsequently recognised by the European Union institutions. The analysis of the impact of these texts is intrinsically important to countries that are debating the implementation of Internet blocking. Indeed, Internet blocking attempts are analysed below 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.

6.5.1 National texts

The first texts known to have proclaimed human rights and fundamental freedoms at a national level most significantly the English Bill of Rights of 1689, the American Bill of Rights of 1787 and the French Human and Citizens' Rights Declaration of 1789. These three texts constitute what Moore calls "*the Bourgeois Route*" to "*the modern world*", the route that led England, the United States and France to end-up "*as Western Parliamentary democracies*", after "*different concrete patterns of class struggle*"[315].

6.5.2 International instruments

International instruments related to human rights and fundamental freedoms have been adopted within the framework of the United Nations and the Council of Europe.

6.5.2.1 United Nations

After the Second World War, the first international text proclaiming human rights and fundamental freedoms was the ***Charter of the United Nations*** signed in San Francisco on 26 June 1945 and which entered into force on 24 October 1945. Notably created to "*maintain international peace and security*", "*to develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples*" and to "*be a centre for harmonizing the actions of nations in the attainment of (the) common ends*" described in the Article 1 of the Charter, the United Nations also aim to "*to achieve international cooperation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion*" [316].

Universal Declaration of Human Rights (UDHR)

The second international text declaring Rights and Freedoms was the ***Universal Declaration of Human Rights (UDHR)***, proclaimed in Paris by the United Nations General assembly on 10 December 1948. Since this Declaration is not legally binding, it has been proclaimed "*as a common standard of achievements for all peoples and all nations*"[317] and is the most translated and disseminated text with "*360 different translations*"[318] on the website[319] of the Office of the High Commissioner for Human Rights (OHCHR).

---

[315] Theda Skocpol, "Social Revolutions in the Modern World", *in* Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, *the democracy sourcebook*, Massachusetts Institute of Technology, 2003, page 66 and 67.
[316] See Article 1 and 76 of the Charter, which is available at: http://www.unhchr.ch/html/menu3/b/ch-cont.htm.
[317] "Universal Declaration of Human Rights", "Introduction", on the website of the Office of the High Commissioner for Human Rights of the United Nation: http://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx.
[318] "Universal Declaration of Human Rights", "Introduction", on the website of the Office of the High Commissioner for Human Rights of the United Nation: http://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx.
[319] http://www.ohchr.org/.

This Declaration, which emphasises the principle of universality of human rights[320] and which spells out for the first time "*basic civil, political, economic, social and cultural rights that all human beings should enjoy*"[321], is usually recognised as "*the foundation of the International Law related to Human Rights*" and "*inspired a rich corpus of binding international texts in the area of Human Rights*".[322] With the ***International Covenant on Civil and Political Rights***, its two Optional Protocols, and the ***International Covenant on Economic, Social and Cultural Rights***, the UDHR forms a "*so-called International Bill of Human Rights*".[323] With seven other human rights instruments adopted between 1965 and 2006, there are today nine core international human rights instruments.[324] All 192 member States of the United Nations have ratified at least one of them, thereby undertaking a commitment to human rights, while 80% have ratified four or more of them[325].

International Covenant on Civil and Political Rights

One of the important texts of this corpus that has to be mentioned, as regards freedoms that have to be analysed within the framework of a blocking measure, is the International Covenant on Civil and Political Rights (ICCPR), adopted in New York by The United Nations General Assembly on 16 December 1966, and which entered into force on 23 March 1976 (for all provisions except those of its article 41 which entered in force on 28 March 1979). 72 countries have signed this Covenant while 164 countries are parties to it, by ratification, accession or succession,[326] undertaking that way to adopt "*laws or other measures as may be necessary to give effect to the rights recognized in the (…) Covenant*"[327], as for instance the rights to life (article 6), not to be subjected to torture or to cruel, inhuman or degrading treatment or punishment (article 7), to liberty and security of person (article 9), not to be subjected to arbitrary or unlawful interference in privacy, family, or correspondence (article 17), to freedom of thought, conscience and religion (article 18) or to freedom of expression (article 19). As the right to respect for private life and the freedom of expression are the two main freedoms that could enter in conflict with a blocking measure, as we will see below, the high number of States that recognised the necessity to preserve such rights shows the importance place that these rights have to take within the framework of the Internet blocking debate.

Convention on the Rights of the Child

Another important text is the Convention on the Rights of the Child which was adopted and opened for signature, ratification and accession by the United Nations General Assembly resolution 44/25 of 20 November 1989. It entered into force on 2 September 1990[328], and counts today 194 party countries.[329]

---

[320] "What are human rights?", website of the High Commissioner for Human Rights of the United Nation: http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx

[321] "International Human Right Law", website of the High Commissioner for Human Rights of the United Nation: http://www.ohchr.org/EN/ProfessionalInterest/Pages/InternationalLaw.aspx.

[322] Both quotations translated from French. "Déclaration Universelle des droits de l'homme", United Nation website: http://www.un.org/fr/documents/udhr/law.shtml.

[323] "International Human Right Law", website of the High Commissioner for Human Rights of the United Nation: http://www.ohchr.org/EN/ProfessionalInterest/Pages/InternationalLaw.aspx

[324] These treaties, optional protocols and monitoring bodies are listed on the United Nations High Commissioner for Human Rights's website: http://www2.ohchr.org/english/law/index.htm.

[325] "What are human rights?", website of the High Commissioner for Human Rights of the United Nation: http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx. See also "La Déclaration Universelle des droits de l'homme : fondement du droit international relatif aux droits de l'homme", United Nation website: http://www.un.org/fr/documents/udhr/law.shtml. The list of the United Nations member States is available at: http://www.un.org/en/aboutun/.

[326] Information related to the Covenant and the list of signatories and parties are available on the United Nations website at the following address: *http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en&clang=_en.*

[327] Article 2 of the Covenant.

[328] This convention is accessible at this address: http://www2.ohchr.org/english/law/crc.htm.

[329] See the related page of the United Nations' website: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en.

The preamble of this Convention recalls "*that the need to extend particular care to the child has been stated in the Geneva Declaration of the Rights of the Child of 1924 and in the Declaration of the Rights of the Child adopted by the General Assembly on 20 November 1959 and recognized in the Universal Declaration of Human Rights, in the International Covenant on Civil and Political Rights (in particular in articles 23 and 24), in the International Covenant on Economic, Social and Cultural Rights (in particular in article 10) and in the statutes and relevant instruments of specialized agencies and international organizations concerned with the welfare of children*". Article 1 adds that for the purpose of the Convention, "*a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier*".

The Convention basically awards children four categories of rights that could be in discussion within the framework of a blocking measure.

- The right to be protected against all forms of violence and exploitation.[330]
- The right to development, especially through access to information[331] and by being prepared for a "*responsible life in a free society*"[332].
- The right to have their best interests prioritised: "*In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration*".
- The right, for "*a mentally or physically disabled child",* to *"enjoy a full and decent life, in conditions which ensure dignity, promote self-reliance and facilitate the child's active participation in the community*"[333].

Article 34 places specific obligations on States party to this binding Convention to take *all appropriate national, international and multilateral actions* to *prevent* the exploitative use of children in pornographic performances and materials. Bearing in mind the pronouncements of certain government Ministers[334] as regards the apparent lack of international cooperation, it would appear that efforts to ensure respect of this binding obligation need to be undertaken.

An optional protocol to the Child Rights Convention, which deals specifically with the sale of children, child prostitution and child pornography was adopted on 25 May 2000 and entered into force on 18 January 2002.

Convention on the Rights of Persons with Disabilities

The United Nations Convention on the rights of persons with disabilities of 13 December 2006[335] specifically declares the rights of disabled persons. This text aims "*to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities, and to promote respect for their inherent dignity*"[336], recognising inter alia that "*the importance of accessibility to the physical, social, economic and cultural environment, to health and education and to information and communication, in enabling persons with disabilities to fully enjoy all human rights and fundamental freedoms*"[337]. Its article 4.1(f) holds that "*States Parties undertake to ensure and promote the full realization of all human rights and fundamental freedoms for all persons with disabilities without discrimination of any kind on the basis of disability*", notably by undertaking and promoting "*research and development of universally designed goods, services, equipment and*

[330] See articles 19, 32, 34, 36, 39 of the Convention.
[331] Article 17 of the Convention
[332] Article 29d of the Convention
[333] Article 23.1 of the Convention
[334] Australian Minister Stephen Conroy stated during a television interview that "for the overseas websites at the moment all ACMA can do if they're identified is write to the overseas server and ask them to not do it - which means nothing, in effect. See http://news.sbs.com.au/insight/episode/index/id/59#watchonline (last visited 3 September 2009)
[335] This Convention is available at http://www2.ohchr.org/english/law/disabilities-convention.htm.
[336] Article 1 of the Convention.
[337] Preamble of the Convention, v.

facilities, as defined in article 2 of the present Convention, which should require the minimum possible adaptation and the least cost to meet the specific needs of a person with disabilities, to promote their availability and use, and to promote universal design in the development of standards and guidelines" and by undertaking and promoting "*g) research and development of, and to promote the availability and use of new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities, giving priority to technologies at an affordable cost*".

Convention on the elimination of all forms of racial discrimination

The other United Nations Convention which is important within the framework of the discussion on blocking is the International Convention on the elimination of all forms of racial discrimination[338], which has been signed by 173 states[339]. This Convention aims to protect persons against "*any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life*"[340].

All these rights are also protected, in a substantially similar way, at the Council of Europe level. The Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe especially protects all the ICCPR rights we previously enumerated[341].

6.5.2.2 Council of Europe

The Council of Europe was founded on 5 May 1949 by 10 countries and has today 47 member countries[342]. Its primary aim is "*to create a common democratic and legal area throughout the whole of the continent, ensuring respect for its fundamental values: human rights, democracy and the rule of law*"[343].

European Convention on Human Rights (ECHR)

The creation of this democratic and legal area is primary based on the principles stated within the ***Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights or ECHR***), signed in Rome on 4 November 1950 and entered into force on 3 September 1953, which is considered as being generally thought of as the "*Constitutional Charter of Europe and as the favoured main line for the construction of a united and democratic Europe*"[344].

The main innovation in this Convention is the institutional mechanism that was created to oversee the respect of the declared rights and freedoms. Initially composed by three decision-making organs (the Commission for investigations and conciliations, the Court for judiciary decisions and the Committee of Ministries for political decisions), the control mechanism only consists today of the European Court of Human Rights, which has been substituted to the

---

[338] Adopted and opened for signature and ratification by General Assembly resolution 2106 (XX) of 21 December 1965, entered into force on 4 January 1969, available at the following address: http://www2.ohchr.org/english/law/cerd.htm.

[339] See the Committee on the Elimination of Racial Discrimination website, available at: http://www2.ohchr.org/english/bodies/cerd/index.htm.

[340] Article 1 of the Convention.

[341] Respectively articles 2, 3, 5, 8, 9 and 10.

[342] "Who we are" in "The Council of Europe in brief", Council of Europe Website, http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=en.

[343] "Our objectives" in "The Council of Europe in brief", Council of Europe Website, *http://www.coe.int/aboutCoe/index.asp?l=en&page=nosObjectifs*.

[344] Translated from French. Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", in Libertés et droits fondamentaux, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, page 35, n° 61. See also Pär Hallström, "The European Union – From Reciprocity to Loyalty", Scandinavian Studies in Law, vol. 39, 2000; pages 79-88, available at: *http://www.cenneth.com/sisl/pdf/39-5.pdf*, page 82: "The Convention is meant to function as a European "super constitution" that guarantees everyone, regardless of nationality, its inclusive rights".

three previous organs by protocol number 11, signed on 11 May 1994 and which entered into force on 1st November 1998[345]. All alleged violations of human rights are in consequence referred directly to the Court[346].

How the European Convention on Human Rights is transposed into legal local systems varies from country to country. Generally, the obligation to achieve the result of respecting treaties related to Human Rights by states[347], which cannot require the principle of reciprocity[348], is executed through law, but countries stay free to use the means they deem appropriate to reach that aim[349], in accordance with their Constitution[350]. As a result, the place of the Convention into the norms hierarchy is not the same in each country that respects the international text.

For instance, the Convention has been directly integrated into the local legal system by the Constitution in the Netherlands, Belgium, Spain and Bulgaria, and has been integrated by a law in Malta, Finland, Denmark, Iceland, Norway, United Kingdom and Sweden. As regards the place of the Convention into the norms hierarchy, it has a supra-constitutional force in the Netherlands, a constitutional force in Austria, an infra-constitutional but supra-legal force in Belgium, Greece, Swiss and Spain, and a simple legal force in Germany, Turkey and Finland[351]. In France, the Convention is directly integrated into the local system by the Constitution, as its article 55 states that "*Treaties or agreements duly ratified or approved shall, upon publication, prevail over Acts of Parliament, subject, with respect to each agreement or treaty, to its application by the other party*".[352] The Convention is therefore of infra-constitutional but supra-legal force, even if the national law is subsequent to the Convention[353].

The Convention on Human Rights is considered as being one of the fundamental texts that ensure the protection of children's rights, since it applies to every human being[354], as well as

---

[345] See Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", in Libertés et droits fondamentaux, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, page 35, n° 61.

[346] Convention for the Protection of Human Rights and Fundamental Freedoms, Summary of the treaty, Council of Europe website: http://conventions.coe.int/Treaty/en/Summaries/Html/005.htm.

[347] See Claudia Sciotti-Lam, L'applicabilité des traits internationaux relatifs aux droits de l'homme en droit interne, thesis, Bruylant Bruxelles, 2004, page 35 and seq. See also

[348] See Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 and seq., especially p. 28: "*The Convention has from its earliest days been regarded as articulating a European public order which was not, therefore, subject to the principle of reciprocity which is more generally found in the application of international obligations by States*", referring to *Austria v. Italy*, 4 YBECHR 112 (1961). See also Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, page 37, n° 65 ; Pär Hallström, "The European Union – From Reciprocity to Loyalty", Scandinavian Studies in Law, vol. 39, 2000; pages 79-88, especially page 82, available at: http://www.cenneth.com/sisl/pdf/39-5.pdf; Claudia Sciotti-Lam, *L'applicabilité des traités internationaux relatifs aux droits de l'homme en droit interne*, thesis, Bruylant Bruxelles, 2004, page 297 *and seq.* The principle of reciprocity allows a State to not execute one of its engagements when another party to a treaty does not execute its own.

[349] See Claudia Sciotti-Lam, *L'applicabilité des traités internationaux relatifs aux droits de l'homme en droit interne*, thesis, Bruylant Bruxelles, 2004, page 65 *et seq*. See also "Convention for the Protection of Human Rights and Fundamental Freedoms", Summary of the treaty, Council of Europe website: http://conventions.coe.int/Treaty/en/Summaries/Html/005.htm: "*Parties undertake to secure these rights and freedoms to everyone within their jurisdiction*".

[350] See Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux", in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, page 39, n° 68.

[351] Frédéric Sudre, op-cit, page 39, n° 68.

[352] Frédéric Sudre, op-cit, page 39, n° 68. The second part of the text does not receive application because the principle of reciprocity does not apply as regards the ECHR.

[353] Frédéric Sudre, op-cit, page 39, n° 69.

[354] See the Council of Europe website, "Building a Europe for and with children", key legal texts, available at: http://www.coe.int/t/transversalprojects/children/keyLegalTexts/Default_en.asp.

the Council of Europe Convention on Action against trafficking in Human Beings[355]. Among the other Council of Europe instruments that protect children we can also mention the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[356], which has however not entered yet into force due to a lack of ratifications[357].

Convention on Cybercrime

The Council of Europe Convention on Cybercrime of 23 November 2001[358] also makes provisions for protecting children, which are also "*persons under 18 years of age*",[359] by asking country parties to criminalise child pornography. This Convention, acceded to or ratified by 26 countries,[360] does not proclaim as such the right for children to not being the victim of the production of child pornography images. It is for this reason difficult to state such a right as a fundamental freedom in itself. However, it is possible to consider the Convention on Cybercrime as indicating the means to put in place mechanisms to achieve the protection of the rights stated in other international texts, such as the right to be protected from violence and the right for development, proclaimed into the United Nations Convention on the Rights of the Child.[361] (The use, procuring or offering of a child for the production of pornography is also prohibited by the 1999 International Labour Organisation Convention on the Worst Forms of Child Labour (Convention Number 182), which was ratified by 171 countries.)

The Convention on Human Rights applies also to persons who suffer from a disability. However, the Council of Europe relies on other initiatives to protect those people. Noteworthy, for instance, is the Recommendation Rec(2006)5 of the Committee of Ministers to Member States "*on the Council of Europe Action Plan to promote the rights and full participation of people with disabilities in society: improving the quality of life of people with disabilities in Europe 2006-2015*"[362]. This document notably holds in its section 1.2.1 that "*Member states will continue to work within anti-discriminatory and human rights frameworks to enhance independence, freedom of choice and the quality of life of people with disabilities and to raise awareness of disabilities as a part of human diversity*". It adds that "*due account is taken of relevant existing European and international instruments, treaties and plans, particularly the developments in relation to the draft United Nations international convention on the rights of persons with disabilities*".

As regards freedoms that could be relevant within the framework of a discussion on Internet blocking, it is important to mention the protocol n° 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, which holds in its article 1 a "*general prohibition of discrimination*".

The protection of people against discrimination is also ensured at the European Union level.

---

[355] Convention on Action against trafficking in Human Beings, CETS N°.:197, opened for signatures on 16 May 2005, entered into force on 1st February 2008 (16 signatures not followed by ratifications and 25 ratifications/accessions on 19 august 2009), available at:

[356] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS N).:201, opened for signature on 25 October 2007. The Convention is available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=&CL=ENG.

[357] On 19 August 2009, 35 countries had signed the Convention without having ratified it and 2 countries had ratified or accessed it, while 5 ratifications including at least three member States of the Council of Europe were necessary to allow the Convention to enter into force. See the related page of the Council of Europe website, available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=&CL=ENG.

[358] This Convention is available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[359] Article 9, 3 of the Convention.

[360] See the dedicated page of the Council of Europe website, available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG.

[361] The Convention on cybercrime makes for instance a reference to the United Nations Convention on the Rights of the Child in its preamble, § 12.

[362] This recommendation was adopted by the Committee of Ministers on 5 April 2006 at the 961st meeting of the Ministers'Deputies). It is available at http://www.coe.int/t/e/social_cohesion/soc-sp/Rec_2006_5%20Disability%20Action%20Plan.pdf.

6.5.2.3 The European Union

The European Union today consists of 27 countries, which are all members of the Council of Europe.[363] Even if the European Union has not yet adhered to the European Convention on Human Rights, for the main reason that treaties have to be modified in that purpose,[364] the European Union has recognised the necessity to preserve fundamental freedoms and to respect the ECHR.

The Treaty establishing the European community states for instance in article 6 that the "*Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States*", and that "*the Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law*"[365]. Article 7 of the Treaty organises a procedure allowing the Council to "*determine the existence of a serious and persistent breach by a Member State*" of these principles, after "*obtaining the assent of the European Parliament*", and to "*suspend certain of the rights deriving from the application of this treaty to the Member State in question, including the voting rights of the representative of the government of that Member State in the Council*".

The European Court of Justice, on 28 March 1996, considered that the "*respect for human rights is (…) a condition of the lawfulness of Community acts*"[366]). The EU Charter of Fundamental Rights, which was included in the EU Constitution that France and Netherland rejected, is itself "*the first formal EU document to combine and declare all the values and fundamental rights (economic and social as well as civil and political) to which EU citizens should be entitled*", assembling "*existing rights that were previously scattered over a range of international sources*", with the main aim to "*make these rights more visible*"[367]. The necessary respect of fundamental freedoms is also usually declared within the EU Directives.[368]

Therefore, belonging to the European Union implies respect of human rights and fundamental freedoms, in particular those protected by the European Convention on Human Rights.

The European Union also emphasises certain categories of rights as well as the international texts we have previously analysed, such as children's rights and the right of disabled people or the right to not be discriminated against.

---

[363] "Do not get confused" *in* "The Council of Europe in brief", Council of Europe Website, http://www.coe.int/aboutCoe/index.asp?l=en&page=nepasconfondre.

[364] See the Opinion 2/94 of the Court of 28 March 1996, Accession by the Communities to the Convention for the protection of Human Rights and Fundamental Freedoms, Accessible at http://www.pravo.hr/_download/repository/Opinion_2_1994.pdf. See also "Adhésion de l'Union européenne à la Convention européenne des Droits de l'Homme", Audition organisée par la Commission des questions juridiques et des droits de l'homme, à Paris, le 11 septembre 2007, Intervention de Florence Benoît-Rohmer, Professeur à l'Université Robert Schuman (Strasbourg), Projet - 10.09.2007, available on the European Parliament website at this address: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/background_document_rohmer_/background_document_rohmer_fr.pdf: "after having been the subject of high reserves from several EU member States, the adhesion of the Union to the ECHR is today unanimously sustained" (translated from French).

[365] European Union, consolidated versions of the treaty on European Union and of the treaty establishing the European Community, Official Journal of the European Union, 29 December 2006, C 321 E/1 to 331, available at this address: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0001:0331:EN:pdf.

[366] Opinion 2/94 of the Court of 28 March 1996, Accession by the Communities to the Convention for the protection of Human Rights and Fundamental Freedoms, Accessible at http://www.pravo.hr/_download/repository/Opinion_2_1994.pdf, n° 34.

[367] EU Charter of Fundamental Rights website, "introduction", available at http://www.eucharter.org/.

[368] See for instance the Directive 95/46/EC, § 1: "Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include (…) preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms".

- Firstly, the European Union has adopted numerous acts and instruments related to protection of children's rights[369]. Among them is the Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, [370] which is currently being revised.
- Secondly, the European Union Disability Action Plan (DAP) 2003-2010 which seeks "*to make equal opportunities for disabled people a reality*".[371] It notably aims "*to provide disabled people with the same individual choices and control in their daily lives as non-disabled people*"[372].
- Thirdly, since the European Union needed "*to tackle discrimination based on a number of other grounds*" other than sex, the 1997 Amsterdam Treaty included "*Article 13, which empowers the Community to take action to deal with discrimination based on a whole new range of grounds, including racial or ethnic origin, religion or belief, age, disability and sexual orientation*"[373]. On this basis, the Council of the European Union adopted the Racial Equality Directive on 29 June 2000, which notably prohibits "*all forms of discrimination on grounds of race or ethnic origin*"[374].

All these specific provisions can be seen either as a declaration of fundamental rights and freedoms or, at least, as an indication of the means to put in place measures to ensure some fundamental rights or freedoms stated in the ECHR, its additional protocols and other international instruments.

Within this whole of rights and freedoms we analysed, some might appear in opposition within the framework of a blocking measure while others might be evoked to justify the same measure.

[369] The complete list can be found on the European Union website at this address: http://eur-lex.europa.eu/en/dossier/dossier_30.htm.
[370] O.J.E.C. of 20 January 2004, L 013, pp. 0044-0048, available at this address: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML
[371] See the European Commission website, "employment, Social Affairs and Equal Opportunities", "The EU Disability Action Plan", available at this address: http://ec.europa.eu/social/main.jsp?catId=430&langId=en.
[372] See the European Commission website, "employment, Social Affairs and Equal Opportunities", "People with disabilities", available at this address: http://ec.europa.eu/social/main.jsp?catId=429&langId=en.
[373] See the EU website, Summaries of EU legislation, equality and non-discrimination in an enlarged European Union, available at this address: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/l14157_en.htm.
[374] See the EU website, Summaries of EU legislation, Equal treatment on grounds of racial and ethnic origin, available at the following address: http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33114_en.htm

6.6 Fundamental freedoms that might be in opposition with blocking

Some human rights and fundamental freedoms might be in opposition to Internet blocking, while the preservation of other rights might be a justification of such a technical measure.

The balance between these rights needs to be done (as described in Section 7.6) in the light of the public order clause, described in detail in Chapter 7

Internet blocking can have an impact on some human rights and fundamental freedoms, which are an important part of values that the International community and the European Union have made direct commitments to respect.

- Firstly, 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 uses of the Internet and therefore preventing the possibility to create certain connections or to make some connection choices. These limitations fall within the right to freedom of private life. This is particularly the case with regard to the inevitable over-blocking that impacts on completely innocent websites.
- Secondly, Internet blocking attempts can interfere with the freedom of expression, by preventing people from accessing online information or making available such information. It has therefore a negative impact on information broadcasting, communication and reception.
- Thirdly, Internet blocking attempts can interfere with the specific rights awarded to some categories of people, as the right for disabled persons to access electronic communications.
- Fourthly, blocking may be seen as a substitute for respecting the obligations in the Child Rights Convention to take all appropriate international steps to prevent the exploitation of children for pornographic purposes. This is illustrated by the Australian Minister's comments (mentioned above) when he stated that passing on reports amounted to "nothing".

6.6.1 The right to respect for private and family life

6.6.1.1 The main texts

The right to respect for private and family life is declared in article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, article 8 of the European Convention on Human Rights and article 7 of the EU Charter of Fundamental rights, which has the same meaning and scope than the European Convention on Human Rights[375]. This right is therefore a human right and a fundamental freedom[376], and is therefore, in numerous states, 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.

These texts all protect individuals from arbitrary interference with their privacy, family, home or correspondence and from attacks upon their honour and reputation (only the ECHR comments on this last aspect - the European Court of Human Rights protects also one's reputation under article 8[377]). 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 subject to the conditions described within the so called "public order clause" described in Chapter 7 which includes the principle of lawfulness.

The right to respect for private and family life is moreover protected by several Constitutions at the national level. The right for private and family life is for instance protected by the French Constitutional Council in "*articles 2 and 4*[378] *of the French Human and Citizens Rights Declaration of 1789*"[379], whereby Article 4 is included in the so-called French "constitutionality bloc". The French Constitutional Council also protects some aspects of the right to respect for private life under the personal freedom principle,[380] where the guarantor is the Parliament, in accordance with article 34 of the Constitution[381]. Finally, the right for private and family life is

---

[375] EU Charter of Fundamental Rights website, "Art 7. Respect for private and family life", available at this address: http://www.eucharter.org/home.php?page_id=14.

[376] See also Emmanuel Dreyer, « Le respect de la vie privée, objet d'un droit fondamental », Comm., com. élec. n° 5, May 2005, Etudes, 18.

[377] See for instance *Fayed v. the United Kingdom,* judgment of 21 September 1994, Series A n° 294 B, pp. 50-51, § 67; *Chauvy and Others v. France*, n° 64915/01, § 70, ECHR 2004, VI; *Gunnarsson v. Iceland*, n° 4591/04, 20 October 2005. For all these references, see "Key case-law issues, the concepts of "private and family life", European Court of Human Rights, 24/01/2007, available at this address: http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf

[378] Article 2: "The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, Safety and Resistance to Oppression"; Article 4: "Liberty consists in being able to do anything that does not harm others: thus, the exercise of the natural rights of every man has no bounds other than those that ensure to the other members of society the enjoyment of these same rights. These bounds may be determined only by Law". The Declaration is available in English on the Constitutional Council website at this address: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/cst2.pdf.

[379] See for instance decision n° 2004-492 DC, 2 March 2004, J.O. 10 March 2004, page 4 637, "considérant" n° 4.

[380] Other elements of personal freedom are, under French law, the freedom of movement, the right to not being arbitrary arrested or sequestered, the right to be judged with all legal guarantees and the principle of domicile inviolability. See Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales*, éd. Montchrestien, 7ème éd., 1999, p. 27; article 136 of the Code of Criminal procedure; Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux", 4 June 2009, Juriscom.net, page 3, available at this address: http://www.juriscom.net/uni/visu.php?ID=1133.

[381] The Constitutional Council considers that the refusal to take into consideration the right to respect of private life can be liable to hurt personal freedom: decision n° 94-352 DC, 18 Jan. 1995, J.O. 21 January 1995, page 1154 and JCP 1995, II, 22 525, note Frédérique Lafay. The Council also analysed the implementation of technical mechanisms allowing picking-up, fixing or registering word or images without the consent of interested people, in the light of personal freedom: decision n° 2004-492 DC, 2 March 2004, J.O.R.F. 10 March 2004, p. 4 637. The Council extends also the notion to some personal data filing systems: decision n°

protected by the French civil judge, in addition to some criminal rules that protect specific private life aspects, such as the right of correspondence[382].

6.6.1.2 Private life and Internet blocking

The specific content of the right for private and family life varies through time and across countries, and is mainly defined by judges and doctrine, as texts only declare the general principle, without other precisions. In 1965, the Supreme Court of the United States defined that right as the one, for each individual, "*to make decisions by himself into his zone of privacy*". Previously, two American lawyers had defined the same right as the "*right to be left alone*".[383] In France, the analysis of court cases allows Prof. François Terré to see private life as composed of several circles. At the centre, would be "personal life", which contains "*data related to identity, to racial origin, to physical or mental health, to one's character or morals*".[384] Genetic information would also be inherent in private life, even if their statute is still discussed. A larger circle would then include data related to "*sentimental, conjugal, extra-conjugal and familial life*", to "*friendly relations*", to "*the participation in private assembly*"[385]. The domicile[386] and private correspondence[387] are also protected under this same principle of respect to private life.

The European Court of Human Rights is considered to have a more extensive understanding of private life than several countries,[388] even if it "*does not consider it is possible or necessary to attempt an exhaustive definition of the notion of "private life"*[389]*,* which is a "*broad term*".[390] The Court considers however that "*it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle*".[391] Under

---

2004-492 DC, 2 March 2004, J.O.R.F. of 10 March 2004, p. 4 637, § n° 64. On all these elements, see Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux", op cit and Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 20. French Constitution is available in English on the Constitutional Council website at this address: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/constiution_anglais_juillet2008.pdf

[382] See for instance Article 226-15 of the French penal Code: "Maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of €45,000"."The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions".

[383] For the discussion and both quotations (translated from French) see Pierre Tabatoni, « Avant-propos », in La protection de la vie privée dans la société d'information, under the dir. of Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, 1st ed., Jan. 2002, page 4.

[384] François Terré, « La vie privée », in La protection de la vie privée dans la société d'information, under the dir. of Pierre Tabatoni, 3 tomes, Cahier des sciences morales et politique, PUF, 1ère éd., janv. 2002, page 138. See also Estelle De Marco, L'anonymat sur Internet et le droit, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 41 and seq.

[385] François Terré, « La vie privée », op cit, page 139. Estelle De Marco, L'anonymat sur Internet et le droit, op cit, n° 41.

[386] See for ex. Cass. Civ. 3ème, 25 fév. 2004, Bull. civ. III, n° 41, p. 38.

[387] See for instance the so called « Nikon » Court case, Cass. soc., 2 Oct. 2001, Bull. civ. V, n° 291, page 233.

[388] Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, page 27 and seq. See, for a definition of private life on the criteria of the legitimacy of others to get information about the private life of another person, instead of the criteria of the extensive or restrictive conception of private life, see Estelle de Marco, L'anonymat sur Internet et le droit, op cit, n° 109 and seq.

[389] *Niemietz v. Germany*, judgment of 16 December 1992, Series A no. 251 B, p. 33, § 29, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695764&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[390] See for instance *Peck v. the United Kingdom*, n° 44647/98, § 57, ECHR 2003-I, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=698775&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[391] *Niemietz v. Germany*, judgment of 16 December 1992, Series A no. 251 B, p. 33, § 29, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695764&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. See "Key case-law issues, the concepts of private and family life", European Court of Human Rights, 24/01/2007, available at this address: http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-

article 8 of the ECHR, the Court protects four "*areas of personal autonomy*" (private life, family life, home and correspondence), which are not "*mutually exclusive*", which means for instance that "*a measure can simultaneously interfere with both private and family life*"[392].

The only one distinction that can be seen within each definition of private life is a distinction between the ***privacy of private life***, which is "*opaqueness for others of the personal and family life*" and the ***freedom of private life***, which is "*the power, for a person, to take the decisions that seem to her the bests for this part of her life*"[393]. We will see that blocking can interfere with both of these aspects.

6.6.1.3 Privacy of private life and Internet blocking

As regards the privacy of private life and other concepts protected under article 8 of the ECHR, the European Court protects the inviolability of the home[394] which includes professional offices[395], "*aspects of an individual's physical and social identity*"[396] and the inviolability of correspondence[397] which includes notably letters[398], telephone conversations[399], paper messages[400], professional correspondence[401], correspondence intercepted in the course of business or from business premises[402] and electronic communications[403].

The principle of inviolability of correspondence whereby the European Court of Human Rights aims to "*protect the confidentiality of private communications*"[404], is one of the fundamental

---

D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf.

[392] See for instance *Menteş and Others* v. Turkey, judgment of 28 November 1997, Reports of Judgments and Decisions 1997 VIII, p. 2711, § 73; *Stjerna v. Finland*, judgment of 25 November 1994, Series A no. 299 B, p. 60, § 37; *López Ostra v. Spain*, judgment of 9 December 1994, Series A no. 303 C, p. 54, § 51; *Burghartz v. Switzerland*, judgment of 22 February 1994, Series A no. 280 B, p. 53, § 24; *Płoski v. Poland*, no. 26761/95, § 32, 12 November 2002. On the discussion, these judgements and for each quotation, see "Key case-law issues, the concepts of private and family life", European Court of Human Rights, 24/01/2007, available at this address: http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf

[393] Translated from French. Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, page 12. See also Estelle De Marco, L'anonymat sur Internet et le droit, op cit page 99 and seq.

[394] Chappell Court case, 30 March 1989, Court publications, n° 152, Serie A; Niemetz c/ Germany, 16 December 1992, volume n° 251B, Serie A; See Pierre Kayser, op cit, page 43 and 44 and footnote n° 158.

[395] Pierre Kayser, op cit, page 44, referring to the case "Niemietz c/ Germany", op cit.

[396] *Mikulić v. Croatia*, no. 53176/99, § 53, ECHR 2002 II, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=697912&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. See also "Key case-law issues, the concepts of private and family life", European Court of Human Rights, op cit.

[397] See for instance *B.C. v. Switzerland*, n° 21353/93, Commission decision of 27 February 1995; Silver and Others v. the United Kingdom, judgment of 25 March 1983, Series A n° 61, p. 32, § 84.

[398] See for instance *Silver and Others v. the United Kingdom*, judgment of 25 March 1983, Series A n° 61, p. 32, § 84.

[399] See for instance *Malone v. The United Kingdom*, judgment of 2 August 1984, Series A, n° 28, p. 21, § 41.

[400] *Taylor-Sabori v. the United Kingdom*, n° 47114/99, 22 October 2002. On this issue and the two previous one, see "Key case-law issues, the concepts of "home" and "correspondence", European Court of Human Rights, 31/01/2007, available at this address: http://www.echr.coe.int/NR/rdonlyres/7CD3BA4D-30AC-4E34-8131-8B9EE3647B94/0/COURT_n1898123_v2_Key_caselaw_issues__Article_8_home_and_correspondence2.pdf

[401] Pierre Kayser, op cit, page 44, referring to the case "Niemietz c/ Germany", op cit.

[402] *Kopp v. Switzerland*, judgment of 25 March 1998, Reports of Judgments and Decisions 1998, II, p. 539, § 50; Halford v. the United Kingdom, judgment of 25 June 1997, Reports of Judgments and Decisions 1997, III, p. 1016, §§ 44-46; quoted by "Key case-law issues, the concepts of "home" and "correspondence"", op cit.

[403] See Copland v. the United Kingdom, n° 62617/00, 3 April 2007, § 41: "According to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Article 8 § 1 (see Halford, op cit, § 44 and Amann v. Switzerland [GC], no. 27798/95, § 43, ECHR 2000-II). It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal internet usage". The judgment is available at the following address: http://cmiskp.echr.coe.int////tkp197/viewhbkm.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=21690&sessionId=27467944&skin=hudoc-en&attachment=true

[404] "Key case-law issues, the concepts of "home" and "correspondence", op cit, referring to *B.C. v. Switzerland*, n° 21353/93, Commission decision of 27 February 1995.

freedoms that could be directly undermined by an Internet blocking measure. Correspondence has been defined by the doctrine as a "*personal and temporal communication, allowing interactivity, and addressed to determined and individualised persons*".[405] This definition is considered by some as defining the nature of correspondence that is protected by the French Criminal Code, and is therefore very precise and might correspond to the definition retained by several countries. The definition applies to both the mechanism of the information and the information communicated, during the time of its transmission. Therefore, each means of communication that allows interactivity can support "correspondence", such as email, FTP or peer to peer[406]. The web can also be used under this definition of correspondence. It will be for instance the case when the sender and the receiver will use a private web space to exchange information, as a private forum of discussion or a part of a private mailbox where both will be able to connect to chat.

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 (logs, records, etc), Internet blocking attempts can sometimes lead to the retention of the content of the message, or to some details of this content in relation to a specific person, without the consent of this person. That would be seen as an interference in the right protected by article 8 of the ECHR, as it was specifically said by the European Court that "*the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8*"[407].

Definition of Correspondence

It could be said that, taking into account the restrictive definition of "correspondence", communications of other types between people could be subjected to more restrictions without interfering with the right of private life. Such a conclusion has to be carefully considered.

- **Personal and Temporal Nature of Correspondence**
  Firstly, the definition of correspondence partly depends on the personal and temporal nature of the content of the message. A communication is personal when the content of the message informs the recipient in a way that relates directly to the recipient's situation, and could not fit to everybody's situation. Therefore, advertising is not personal, unless the offer is adapted to the recipient and to his precise consumption choices[408]. A communication is temporal when it belongs to a determined time, and could not "*belong to every age: past, present and future*"[409].

  Therefore, in order to determine the communication *is not* correspondence requires the analyst to read the content of the communication, where such reading is not permitted if it appears that it is a correspondence in the first place. Communications between people benefit therefore by a factual presumption of being correspondence, which prohibits violating them, whatever their content is. This conclusion is also the one of the European Court of Human Rights, which considers that "*the content of a correspondence*

[405] Estelle De Marco, L'anonymat sur Internet et le droit, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 637. See also Virginie Peltier, Le secret des correspondances, PU d'Aix-Marseille, 1999.

[406] As regards the protection of some kind of electronic communications, see the following paragraph or our first paragraph in the current section.

[407] *Copland v. the United Kingdom*, n° 62617/00, 3 April 2007, available at http://cmiskp.echr.coe.int////tkp197/viewhbkm.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=21690&sessionId=27467944&skin=hudoc-en&attachment=true (Sep 2009)

[408] Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999, page 239; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 636.

[409] Virginie Peltier, *Le secret des correspondances*, op cit, page 239; See also Estelle De Marco, *L'anonymat sur Internet et le droit*, op cit, n° 636.

is irrelevant to the question of an interference"[410] and that "*there is no de minimis principle for an interference to occur; opening one letter is enough"*[411].

- **Opaqueness to others**
  Secondly, the right to respect for private life implies the opaqueness to others of the private life, as it was previously said, which implies that it is not permitted for others to take notice of what a person does, reads or exchanges with other people, within the framework of their private zone. For this reason, every form of monitoring is under the strict authority of the European Court of Human Rights.[412]

Thus, even if the communications received or sent by a person are not correspondence, they are protected at least 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.

Protection of Personal Data

Another aspect or sphere[413] of the privacy of private life is the protection of personal data. While the European Court of Human Rights protects this right under article 8 of the Convention, the EU Charter of Fundamental rights declares this right separately, in its article 8.[414] The right to protection of personal data is therefore a fundamental right in Europe,[415] and is ensured at the national level by all member states, which had to integrate into their national law the European Directives that ensure personal data protection, the most fundamental being Directives 95/46/EC and 2002/58/EC (the latter is currently being updated). Data Protection Authorities ensure the respect of these rights in the Member States and an independent authority of the same nature was created at the European Level, which is the European guardian of personal data protection (EDPS), "*to ensure these rights in the EU administration"*[416].

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 as is the case, for example, with an IP address. There is a debate around the question if an IP

---

[410] "Key case-law issues, the concepts of "home" and "correspondence", op cit, referring to A. v. France, judgement of 23 November 1993, Series A, n° 277 B, p. 49, §§ 35 and 37.

[411] "Key case-law issues, the concepts of "home" and "correspondence", op cit referring to *Narinen v. Finland*, n° 45027/98, § 32, 1st June 2004: "*The opening of one letter is, however, sufficient to disclose an interference with the applicant's right to respect for his correspondence*".

[412] See for instance *Copland v. the United Kingdom*, n° 62617/00, 3 April 2007, § 44: "the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8". About "*Monitoring by technological means of (a) public scene*", see *P.G. and J.H. v. the United Kingdom*, n°. 44787/98, § 57, ECHR 2001 IX, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=697542&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. About telephone monitoring, see for instance *Klass and Others v. Germany*, judgment of 6 September 1978, Series A, n° 28, p. 21, § 41; *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A, n°. 82, pp. 30-31, § 64; *Kruslin v. France*, judgment of 24 April 1990, Series A, n°. 176 A, p. 20, § 26).

[413] See Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, page 42.

[414] This provision has been written "on the basis on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995) as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States": EU Charter of Fundamental Rights website, "Art 8. Protection of personal data", available at this address: http://www.eucharter.org/home.php?page_id=15.

[415] EDPS website, in "The EDPS", "Introduction", available at http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/15.

[416] EDPS website, in "The EDPS", "Introduction", available at this address: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/15.

address is personal data,[417] but this debate seems to confuse the issue of personal data and the issue of liability.

Indeed, personal data is "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".[418]

This is objectively the case of an IP address since this address enables the identification of the owner of the Internet access point. The personal data is at least that "Mr. X, who ***can*** be identified, is the owner of an Internet access" or that "Mr. X, who ***can*** be identified, is the owner of an Internet access that was used the 12 June 2009 at 10:00 am to access a particular website". Once this is said, it is appropriate that this identification should not facilitate making a link between a natural person and a given situation, such as a website access or an infringement. Personal data will give information about the owner of the access line which was used to consult a website or to commit an infringement but will provide information about the person who was physically using the Internet access to access this website or commit this infringement. This is a question of liability, and has no links with the definition of personal data. However, the retention of an IP address in links with a factual situation on the Internet is all the more dangerous since it can not be considered as knowledge or as a proof of a liability or behaviour.

As a result, an Internet blocking measure put in place in an EU Member State should not lead to the storage of data that identifies at least the holder of an Internet account, without respecting the conditions listed by the EU Directives 95/46/EC[419], 2002/58/EC and 2006/24/CE that modified the latter, and by national laws that have implemented them.

An Internet blocking measure put in place in countries that are not EU Member States but which have agreed to respect private life, especially those that are parties to the European Convention on Human Rights, cannot do so without respecting the conditions imposed by the European Court of Human Rights, which is studied below ("public order clause"). This was notably emphasised by the Data Protection working Party, usually called "Article 29 Working Group"[420], which considered, on the basis of "*the right to privacy (Article 8, ECHR and similarly incorporated into Community law)*"[421], that "*the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace*".[422] This was also emphasised by the European Court of Human Rights, which considers that "*the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge,*

---

[417] See for instance Aoife White, "IP addresses are personal data, E.U. Regulator says", Washingtonpost.com, 22 January 2008, available at he following address: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html.

[418] Article 2, a, of the Directive 95/46/EC.

[419] For instance, data shall be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"; they are "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"; "the data subject has unambiguously given his consent", or the collect is necessary to reach one of the other criteria listed in the convention: respectively article 6b, 6e, and 7a of the Directive 95/46/EC.

[420] This Group has been created by article 29 of the Directive 95/46/EC. Article 15, 3 of the Directive 2002/58/EC, which allows States to set up a preventive and systematic retention of some technical data, states that "The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector".

[421] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, recommendation 3/97, "Anonymity on the Internet", 3 December 1997, WP 6, DG MARKT D/5022/97, website of the European Commission, Justice and Home affairs, Freedom, Security and Justice, Data Protection, Working party, Documents adopted in 1997, page 4. Available at this address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp6_en.pdf.

[422] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, recommendation 3/97, op cit, page 5.

amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8".[423]

This was further emphasised by lawyers and researchers, who consider that each piece of data enabling the surveillance of people is considered dangerous, even if it is not used, especially in a democratic state.[424] Since "*even in State bodies the more estimable and respectable, there are temptations, weaknesses, brittlenesses*".[425] Privacy is therefore "*a society issue*"[426] and some authors consider that the way society ensures privacy protection enables an assessment of its "*democratic maturity*"[427] and to know if it has "*accepted the primacy of the human being or if it requires his submission*".[428] According to authors who subscribe to that doctrine, "*it is therefore useful, even essential, to enable protection systems*"[429].

6.6.1.4 Freedom of private life and Internet blocking

Freedom of private life is also protected on the basis of the European Convention on Human Rights.

The European Commission of Human Rights considered, in 1976, that the right to respect for private life includes "*to a certain degree, the right to establish and develop relationships with other human beings, notably in the affective domain, to develop and to blossom one's own personality*"[430]. The European Court of Human Rights confirmed this analysis, extending the right to professional and commercial relationships[431]. The Court protects therefore the "*right to identity and personal development and (…) to establish and develop relationships with other human beings and the outside world*"[432], the "*right to self-determination and personal autonomy*"[433], and "*the physical and psychological integrity of a person*"[434]. The Court explained also that "*the right to respect for private life is of such a scope as to secure to the*

---

[423] *Copland v. the United Kingdom*, n° 62617/00, 3 April 2007, § 44, available at this address: http://cmiskp.echr.coe.int////tkp197/viewhbkm.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=21690&sessionId=27467944&skin=hudoc-en&attachment=true

[424] See Raymond Aron, Essai sur les libertés, éd. Hachette, coll. Pluriel, 1976, pp. 132-133. On the whole paragraph, see Estelle De Marco, L'anonymat sur Internet et le droit, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 84.

[425] Noël Chahid-Nourai, speech to the panel « Secret et nouvelles technologies », conference dedicated to professional secret organised by the the « Conférence des bâtonniers », Les petites affiches, n° 122, 20 June 2001, page 25 et seq.

[426] Michel Benichou, « Le résistible déclin du secret », Les petites affiches, 20 June 2001, n° 122, page 3 et seq.

[427] Michel Benichou, « Le résistible déclin du secret », Les petites affiches, 20 June 2001, n° 122, page 3 et seq.

[428] Michel Bénichou, op cit.; as regards criticism of « transparence », see also Jacques Ribs, Opening of the conference « Droit et démocratie » (Law and Democracy) on the topic « Internet et les libertés » (Internet and Freedoms), Les petites affiches n° 224, 10 November 1999, page 2 et seq., especially page p. 3 : "it is therefore a singular challenge for democracy, for the protection of personal freedom and private life, which are essential principles for our conception itself of democracy"; Erik Izraelewicz, « La dictature de la transparence », Revue des deux mondes, Feb. 2001, page 62.

[429] Noël Chahid-Nourai, speech to the panel « Secret et nouvelles technologies », conference dedicated to professional secret organised by the the « Conférence des bâtonniers », Les petites affiches, n° 122, 20 June 2001, page 25 et seq.

[430] Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, page 45, quoting the decision X. v. Island, decision of the Commission, 18 May 1976, year 1976, req. N° 6825/74, page 343 (translation from French). See also Jacques Robert and Jean Duffar, *Droits de l'homme et libertés fondamentales,* Montchrestien, 7th ed., 1999, page 437.

[431] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, page 45, referring to the decision Niemetz c/ Germany, 16 December 1992, volume n° 251B, Serie A.

[432] *P.G. and J.H. v. the United Kingdom*, no. 44787/98, ECHR 2001, IX, § 56, referring to *Burghartz v. Switzerland*, judgment of 22 February 1994, Series A, n° 280 B, p. 28, §24. See also *Pretty v. The United Kingdom*, n° 2346/02, ECHR 2002, III, § 61, referring to the same judgment. See also "Key case-law issues, the concepts of "private and family life", op cit, referring to *Friedl v. Austria*, judgment of 31 January 1995, Series A, n° 305 B, opinion of the Commission, p. 20, § 45.

[433] "Key case-law issues, the concepts of "private and family life", op cit, referring to *Pretty v. The United Kingdom*, n° 2346/02, ECHR 2002, III, §§ 61 and 67.

[434] "Key case-law issues, the concepts of "private and family life", European Court of Human Rights, 24/01/2007, available at this address: http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf, referring to *X and Y v. the Netherlands*, judgment of 26 March 1985, Series A, n°. 91, p. 11, § 22.

individual a sphere within which he can freely pursue the development and fulfilment of his personality"[435], but "*it is not confined to measures that affect a person in their home or private premises: there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life"*[436].

Freedom of private life can therefore be understood as the freedom to establish and maintain relationships, also via electronic communications[437], but also to make online cultural, leisure or consumption choices, or to freely surf and reach information on the network[438].

An Internet blocking measure that would consequently interfere in such rights would be therefore an interference with the freedom of private life. It would be the case of a measure that would prevent people from making some online choices, by blocking some legal websites, or that would oblige them to use certain communication protocols instead of the one that is blocked. It would also be the case of a blocking measure applying to an Internet user, preventing him from exercising his private life on the network.

Freedom of Correspondence

As regards the freedom of correspondence, the European Court of Human Rights mainly had the opportunity to analyse the prisoner's right to correspond[439].

The freedom of correspondence, which is the power to correspond with chosen persons, is itself protected by the right to secrecy of correspondence, according to Virginie Peltier. This author considers that "*one must be able to stay alone (…)*" to consider the correspondence as being "*really free*"[440]. This is also true for electronic correspondence. According to the author, "*it is the tranquillity in which takes place the correspondence action that determines the freedom*"[441].

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. It would be the case, for instance, of an Internet blocking measure that would lead to making it impossible to correspond with one's contacts, by attempting to block a website or a domain that hosts a mailbox or a private discussion space, or by attempting to block contents on a P2P protocol (or attempting to block the protocol itself), preventing a person from the sending or receiving a file because of the overly restrictive rules put in place. More generally, it would also be the case for each Internet blocking measure that would lead to blocking a means or a mechanism of correspondence. Such interference could simultaneously be qualified as interference in the right for family life, if the blocking measure prevents a couple or children and parents from communicating with each other. The European Court of Human Rights considers that "*the*

---

[435] *Brüggeman and Scheuten v. Germany*, n° 6959/75, Commission's report of 12 July 1977, Decisions and Reports (DR) 10, p. 115, §55, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=open&documentId=816971&portal=hbhbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[436] "Key case-law issues, the concepts of "private and family life", op cit, referring to *P.G. and J.H. v. the United Kingdom*, n° 44787/98, ECHR 2001, IX, § 56.

[437] See above, section 6.6.1.3. and case law Copland v. the United Kingdom, n° 62617/00, 3 April 2007, § 41. For a case of protection of private life on the Internet, see also *K.U. v. Finland*, application n° 2872/02, judgment of the 2 December 2008, for instance § 49: "*freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected*"..

[438] See Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux", 4 June 2009, Juriscom.net, page 4, available at http://www.juriscom.net/uni/visu.php?ID=1133; Estelle De Marco, L'anonymat sur Internet et le droit, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 137.

[439] Court case « Silver and others », Court publications, Serie A, n° 61. See Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, page 61, and footnote n° 249.

[440] Translated from French. Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999, page 99. See also Estelle De Marco, *L'anonymat sur Internet et le droit*, op cit, n° 146.

[441] Translated from French. Virginie Peltier, *Le secret des correspondences*, op cit, page 99.

notion of family life is an autonomous concept"[442] and that "*is essentially a question of fact depending upon the real existence in practice of close personal ties"*[443]. "*Living together without being married can constitute family life"*[444] and "*even in the absence of cohabitation there may still be sufficient ties for family life"*[445].

Other rights that are protected by the Convention on Human Rights under the respect of private life principle are not covered in this report as the purpose here is only to analyse the freedoms that Internet blocking could interfere with.

It is important to note that 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. On this point, we can refer to the opinion of Sir Chahid-Nourai, who was Council member of the French Data Protection Authority (CNIL), concerning the French INSEE Code (N.I.R.) which is an identification number given to people: *"if the N.I.R. had officially and operationally existed in 1943 and if we would have liked to select every people who were born in Poland because we thought they were potentially Jewish, we would have had the possibility to do it. If we want today to select also all the foreign people, it is sufficient to take the 99, which is the identification number for people who were born abroad, category which widely covers the previous one. If we want to be more subtle and want to select, for example, to discriminate them, each person who was born in Iran, in Iraq or in Yugoslavia, we can do it (…). In a crisis time, it can be useful…"*[446].

As soon as a blocking measure is susceptible to interfering with a Fundamental Freedom, its implementation must respect the "public order clause" applied by the European Court of Human Rights described in Chapter 7 .

[442] "Key case-law issues, the concepts of "private and family life", European Court of Human Rights, 24/01/2007, available at http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf, referring to Marckx v. Belgium, judgment of 13 June 1979, Series A, n° 31, p. 11, § 31, Commission's report of 10 December 1977, Series B-29, p.44, § 69.

[443] "Key case-law issues, the concepts of "private and family life", op cit, referring to *K. v. the United Kingdom*, n° 11468/85, Commission decision of 15 October 1986, Decisions and Reports (DR) 50, p. 199, 207.

[444] "Key case-law issues, the concepts of "private and family life", op cit, referring to Johnston and Others v. Ireland, judgment of 18 December 1986, Series A, n° 112, p. 19, § 56.

[445] "Key case-law issues, the concepts of "private and family life", op cit, referring to *Kroon and Others v. the Netherlands*, judgment of 27 October 1994, Series A, n° 297 C, p. 56, § 30.

[446] Noël Chahid-Nourai, speech to the panel « Secret et nouvelles technologies », conference dedicated to professional secret organised by the « Conférence des bâtonniers », Les petites affiches, n° 122, 20 June 2001, page 25 et seq. See also Estelle De Marco, *L'anonymat sur Internet et le droit*, op cit, n° 80.

6.6.2 Freedom of expression

6.6.2.1 Main texts

Freedom of expression is protected by article 19 of the Universal Declaration of Human Rights, article 19 of the International Covenant on Civil and Political Rights, article 10 of the European Convention on Human Rights and article 11 of the EU Charter of Fundamental rights, whose meaning and scope are considered as to be "*the same as those guaranteed by the ECHR*".[447] As a result freedom of expression is a Human Right and a Fundamental Freedom, and therefore, in numerous States, a Civil Liberty. It applies to 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 freedom of expression in article 13.

On the basis of these texts, this right includes "*freedom to hold opinions and to receive and impart information and ideas*", "*regardless of frontiers*". The UDHR, the ECHR and the EU Charter add the fact that this right shall be exercised "*without interference by public authority*". The UDHR and the ICCPR add to the definition 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 EU Charter of Human Rights states finally in a second paragraph that "*the freedom and pluralism of the media shall be respected*". This paragraph spells out "*the consequences of paragraph 1 regarding freedom of the media*", and is based, "*in particular on Court of Justice case law regarding television, particularly in case C-288/89 (judgment of 25 July 1991, Stichting Collectieve Antennevoorziening Gouda and others [1991] ECR I-4007), and on the Protocol on the system of public broadcasting in the Member States annexed to the EC Treaty and now to the Constitution, and on Council Directive 89/552/EC (particularly its seventeenth recital)*" [448].

Duties and Responsibilities

As regards limitations to this freedom, 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. As regards the ICCPR, these restrictions "*shall only be such as are provided by law and are necessary (…) for respect of the rights or reputations of others*" or "*for the protection of national security or of public order (ordre public), or of public health or morals*". As regards the European Convention on Human Rights, these restrictions (or other formalities, conditions, or penalties) must be "*prescribed by law and (…) necessary in a democratic society*" in some listed aims. Both of these sentences correspond to the "public order clause" that is described in Chapter 7 .

Freedom of expression is moreover protected by several Constitutions at the national level. In France, this freedom is protected by article 11 of the Declaration of Human and Citizen's Rights of 1789[449], which belongs to the French "Constitutional bloc". The Constitutional Council add that "*freedom of expression and communication are all the more precious since*

[447] EU Charter of Fundamental Rights website, "Art 11. Freedom of expression and information", available at this address: http://www.eucharter.org/home.php?page_id=18
[448] EU Charter of Fundamental Rights website, "Art 11. Freedom of expression and information", available at this address: http://www.eucharter.org/home.php?page_id=18
[449] Article 11 states: "The free communication of ideas and opinions is one of the most precious rights of man. Every citizen may thus speak, write and publish freely, except when such freedom is misused in cases determined by Law".

they are one of the cornerstones of a democratic society and one of the guarantees of respect for other rights and freedoms"[450].

6.6.2.2 Freedom of expression and Internet blocking

Freedom of expression, which "*constitutes one of the essential foundations of a democratic society*"[451], is at least the right to hold opinions and to receive and impart information and ideas regardless of frontiers - according to the texts that proclaim it.

The European Court of Human Rights adds that article 10 of the ECHR "*guarantees not only the right to impart information but also the right of the public to receive it*" [452] and "*is applicable not only to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population*".[453] Regarding criticism, limits "*are wider as regards a politician as such than as regards a private individual*".[454] The Court considers further that "*in light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10*"[455].

Thus, 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.

The French Constitutional Council confirmed this analysis, by considering the right to access the Internet to be protected under the principle of freedom of expression: "*In the current state of the means of communication and given the generalised development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, (the) right (to communicate freely ideas and opinions) implies freedom to access such services*"[456].

The European Parliament considers that the interruption of Internet access is in conflict with human rights guarantees, without yet stating if it was only because Internet allows the exercise of those freedoms or if Internet access is a fundamental right in itself. Through a resolution of 10 April 2008, the Parliament called on "*the Commission and the Member States*

---

[450] Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 15. This decision is available in English at this address: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf.

[451] *Sunday Times v. The United Kingdom*, judgment of 26 April 1979, application n° 6538/74, Series A, n° 30, § 65, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=freedom%20|%20expression&sessionid=27574169&skin=hudoc-en.

[452] *Times newspapers LTD* (n° 1 and 2) v. The United Kingdom, Judgment of 10 March 2009**,** application 3002/03 and 23676/03), § 27, referring to *Observer and Guardian v. the United Kingdom*, 26 November 1991, § 59(b), Series A, n° 216 and *Guerra and Others v. Italy*, 19 February 1998, § 53, *Reports of Judgments and Decisions* 1998-I. The Times newspapers LTD decision is available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=internet&sessionid=27488178&skin=hudoc-en.

[453] *Sunday Times v. The United Kingdom*, op cit, § 65, referring to the *Handyside v. The United Kingdom* court case (application 5493/72, judgment of the 7 December 1976, Series A, n° 24, p. 23, § 9).

[454] *Lindon, Otchakovsky-Laurens and July v. France*, judgment of 22 October 2007, applications n°s 21279/02 and 36448/02, § 46, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?item=4&portal=hbkm&action=html&highlight=freedom%20|%20expression&sessionid=27650785&skin=hudoc-en.

[455] *Times newspapers LTD* (n° 1 and 2) v. The United Kingdom, op cit, §27.

[456] Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 12. This decision is available in English at this address: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf.

to recognise that 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 "*to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access*".[457]

Within the framework of the reform of telecom legislation (telecom package), the Parliament reinstated, on 6 May 2009, one of the first-reading amendments saying 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*"[458]. The Parliament concluded in its press releases that "*a user's Internet access cannot be restricted without prior ruling by the judicial authorities*"[459]. These amendments, called the "Bono amendment", "amendment 138" or "amendment 46" when it was introduced again into the European text in discussion at the occasion of its second reading in March 2009[460], was argued against by France[461]. At time of writing the fate of this text is unclear, as the Council of the European Union is opposing this text in the conciliation procedure launched after the Parliament's second vote.

Several authors and European Parliament members believed that the adoption of this "Bono amendment" was recognition of Internet access as being a fundamental right[462]. The European Parliament itself stated, in a press release of 26 March 2009, that the "*EU Charter of Fundamental Rights does not directly mention Internet access, but the "right to freedom of expression". This right includes "the right to hold opinions and the freedom to receive and impart information or ideas without interference by public authority and regardless of frontiers". If Internet access is considered as a fundamental right within the EU, France could then be in contradiction with European Law*"[463] assuming adoption of the then-proposed version of the "Loi Hadopi".

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 strives to prevent people from accessing information is therefore in conflict with that freedom. More globally, it can be said that each blocking measure limits the right to freedom of expression, to a greater or lesser extent depending on the blocking characteristics

---

[457] 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.

[458] "No agreement on reform of telecom legislation", Information society, Press release, 6 May 2009, available at this address: http://www.europarl.europa.eu/news/expert/infopress_page/058-55086-124-05-19-909-20090505IPR55085-04-05-2009-2009-true/default_en.htm.

[459] Ibid.

[460] See the website of Guy Bono, member of the European Parliament, "amendement 46 = Amendement 138", press release, 6 March 2009, available at this address: http://www.guy-bono.fr/article/articleview/8805/1/1378/.

[461] France was, at the same time, debating before its own Parliament the draft-law called "Creative Works and the Internet", which was authorizing a newly-created administrative authority to enforce an Internet suspension against an Internet user when the IP address of the user was linked with an intellectual property rights (IPR) infringement and the user could not prove his non-liability. This mechanism was censored by the French Constitutional council, notably because it was not respecting the innocence presumption principle and because he was giving to an administrative authority a power that belongs only to the judge of the judiciary. See Decision n° 2009-580 DC of 10 June 2009, op cit.

[462] See for instance "Le Parlement européen redit non à la coupure de l'accès à internet comme sanction », press release, 26 March 2009, accessible at this address: http://www.guy-bono.fr/article/articleview/8880/1/2096/, quoting Guy Bono: "*despite many pressures from the (French) UMP (party) and French authorities, members of the European Parliament maintained their position: Internet access is a fundamental right for social inclusion*" (translated from French) ; see also Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux", 4 June 2009, Juriscom.net, page 5, footnote n° 32, available at this address: http://www.juriscom.net/uni/visu.php?ID=1133.

[463] Translated from French. "Les droits fondamentaux doivent aussi s'appliquer sur Internet », European Parliament, press release, 26 March 2009, reference available only in the French version, available at this address: http://www.europarl.europa.eu/news/expert/infopress_page/017-52613-082-03-13-902-20090325IPR52612-23-03-2009-2009-false/default_fr.htm.

and the degree of over-blocking, as the clear aim of such a measure is to limit the accessibility of content.

6.6.2.3 Children's specific right to freedom of expression

In light of the analysis done by the European Court of Human Right (which includes the right to receive information in the right to freedom of expression, especially through the Internet) it is possible to consider that some specific children's rights proclaimed by the United Nations Convention on the Rights of the Child are only details of the children's right to protection of freedom of expression.

The Convention states that "*States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health*"[464]. The Convention also states that States Parties "*agree that the education of the child shall be directed to (…)The preparation of the child for responsible life in a free society, in the spirit of understanding, peace, tolerance, equality of sexes, and friendship among all peoples, ethnic, national and religious groups and persons of indigenous origin*"[465].

Therefore, each Internet blocking measure that would lead to prevent children accessing information which would be useful for their development and education to 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. Indeed, article 5 of the Convention states that "*States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention*".

This issue is important since the Internet blocking debate sometimes includes a discussion on the usefulness of blocking some content, to protect children's health and development[466], Accessing content, under parental control and assistance, can also help children understand that some Internet content may be dangerous and should be avoided (or handled in a responsible way). This can therefore contribute towards educating them for a responsible life in a free society, in line with Article 29 of the Convention. Whatever the conclusion of such a discussion would be, it seems important to recall that "*Governments should respect the rights and responsibilities of families to direct and guide their children so that, as they grow, they learn to use their rights properly*"[467].

[464] Article 17 of the Convention.
[465] Article 29, d of the Convention.
[466] In September 2005, a French draft law that has not been adopted was intending to oblige Internet access providers to block automatically and by default each website susceptible to put minors "in peril", which would have covered a broad range of websites (Internet access providers "*operate for all their customers, automatically, outstanding technical devices activated by default that enable to retrain the access to online public communication services that put minors in peril*"). See Marc Rees, "Le filtrage par les FAI confirmé par le 1er Ministre", 22 September 2005, PC Inpact, available at the fhttp://www.pcinpact.com/actu/news/Le_filtrage_par_les_FAI_confirme_par_le_1er_Minist.htm.
[467] Unicef, "Fact sheet: A summary of the rights under the Convention on the Rights of the Child", available on the Unicef website, in "Rights under the Convention on the Rights of the Child" ("more information"), at this address: http://www.unicef.org/crc/files/Rights_overview.pdf.

6.6.3 The right of disabled persons to access electronic communications

Disabled people have, as well as people without disabilities, the fundamental rights notably proclaimed in the ECHR and the ICCPR. However, their disability might sometimes pose a challenge to those people to fully exercise their rights. They can be assisted through the use of electronic communications - including Internet services. For example, the Internet might facilitate the autonomous purchase of goods, communication with their close relations or basic communication with the outside world. Internet is therefore, for some disabled people, more than just a general freedom and more than a freedom protected by the right to freedom of expression even in the situation where accessing the Internet is not considered a fundamental right in itself[468]. It is a tool that can enable them to exercise the fundamental freedoms they could not exercise otherwise. It is therefore a means to exercise those rights and freedoms, especially the right for private life. Limiting that means could be considered as a limitation of the right of disabled persons to access electronic communications, as has been similarly considered for non-disabled people with regards to Internet and freedom of expression.

Furthermore, a positive action is required from countries that have taken the commitment to respect fundamental freedoms, within the framework of the United Nations[469] or of the Council of Europe[470]. They must take the necessary measures to enable *"persons with disabilities to fully enjoy all human rights and fundamental freedoms"*[471].

For that purpose, countries shall notably *"promote the availability and use of new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities, giving priority to technologies at an affordable cost"*[472]. The European Union Action Plan (DAP) 2003-2010 aims itself *"to provide disabled people with the same individual choices and control in their daily lives as non-disabled people"*[473]. Additional specific measures for disabled people are taken within the framework of European Directives that regulate electronic communications[474].

As a result, 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. For example, there is no obligatory copyright exception in European law for the copying of files in order to make them accessible for people with disabilities. As a result, blocking of sites permitting this functionality (as part of a wider block on sites accused of breaching copyright, such as that currently enforced by Eircom in Ireland[475]) would be detrimental to the rights of disabled persons. Such a measure would therefore cause much more damage in terms of freedoms for disabled persons than a measure that would only lead to prevent non-disabled people from the same access. It would be the same of a blocking measure that would lead to prevent a disabled person of using one communication protocol that would be for her of importance, as regards the effects such a measure could have on non disabled persons.

---

[468] See previous section.
[469] Convention on the rights of persons with disabilities of 13 December 2006.
[470] Recommendation Rec(2006)5 of the Committee of Ministers to Member States "on the Council of Europe Action Plan to promote the rights and full participation of people with disabilities in society: improving the quality of life of people with disabilities in Europe 2006-2015", adopted by the Committee of Ministers on 5 April 2006 at the 961st meeting of the Ministers'Deputies, available at http://www.coe.int/t/e/social_cohesion/soc-sp/Rec_2006_5%20Disability%20Action%20Plan.pdf, section 1.2.1: "due account is taken of relevant existing European and international instruments, treaties and plans, particularly the developments in relation to the draft United Nations international convention on the rights of persons with disabilities".
[471] Convention on the rights of persons with disabilities of 13 December 2006, preamble, v.
[472] Convention on the rights of persons with disabilities of 13 December 2006, article 4, 1, g.
[473] See the European Commission website, "employment, Social Affairs and Equal Opportunities", "People with disabilities", available at this address: http://ec.europa.eu/social/main.jsp?catId=429&langId=en.
[474] See below, section Chapter 7
[475] See Eircom press release at http://news.eircom.net/breakingnews/16288287/ (last visited 3 September, 2009, for example)

This issue will have to be taken into account within the framework of any discussion on blocking, even if the rights of disabled people, as well as the right to protection of private life and freedom of expression, have to be balanced with the other rights that might, on the contrary, justify the implementation of a blocking measure.

6.7 Fundamental Rights and Freedoms that might support Internet blocking

Section 6.6 studied some rights and freedoms that might be endangered by a blocking measure. On the contrary, 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 not to be discriminated against
- intellectual property rights

6.7.1 Children's right to be protected from violence

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

- The first one is the important number of texts focused on child protection and not adult protection, which emphasise the prohibition of mental and physical violence towards children, especially of a sexual nature.
- The second one is the prohibition of the image itself of a crime of sexual nature committed against a child, through the prohibition of child pornography.

The United Nations Convention on the Rights of the Child proclaims the children's rights to be protected against "*all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child*"[476], the right to be protected "*from economic exploitation*"[477], from "*all forms of sexual exploitation and sexual abuse*"[478] and "*against all other forms of exploitation prejudicial to any aspects of the child's welfare*"[479]. States Parties shall furthermore take "*all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of: any form of neglect, exploitation, or abuse; torture or any other form of cruel, inhuman or degrading treatment or punishment; or armed conflicts (…)*"[480].

While the Council of Europe Convention on Action against Trafficking in Human Beings aims to "*prevent and combat trafficking in human beings, while guaranteeing gender equality*", applies to adults and children whatever their race or religion[481], the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[482] also aims to "*prevent and combat sexual exploitation and sexual abuse of children,*" to "*protect the rights of child victims of sexual exploitation and sexual abuse*" and to "*promote national and international co-operation against sexual exploitation and sexual abuse of children*".[483] This Convention, which is not yet entered into force due to lack of ratifications[484], adds that all forms of sexual

[476] Article 19 of the Convention
[477] Article 32 of the Convention
[478] Article 34 of the Convention
[479] Article 36 of the Convention
[480] Article 39 of the Convention
[481] Article 1 of the Convention on Action against trafficking in Human Beings, CETS N°.:197, opened for signatures on 16 May 2005, entered into force on 1st February 2008 (16 signatures not followed by ratifications and 25 ratifications/accessions on 19 august 2009), available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=197&CM=1&CL=ENG. As regards the non discrimination principle, see article 3.
[482] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS N).:201, opened for signature on 25 October 2007. The Convention is available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=&CL=ENG.
[483] Article 1 of the Convention.
[484] On 19 August 2009, 35 countries had signed the Convention without having ratified it and 2 countries had ratified or accessed it, while 5 ratifications including at least three member States of the Council of Europe were necessary to allow the Convention to enter into force. See the related page of the Council of Europe website, available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=&CL=ENG.

abuse of children are considered as "*destructive to children's health and psycho-social development*"[485].

Regarding the prohibition of images of a crime scene where the victim is a child, the optional protocol to the Convention on the rights of the Child on the sale of children, child prostitution and child pornography holds that "*each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or trans-nationally or on an individual or organized basis*", listing especially "*producing, distributing, disseminating, importing, exporting, offering, selling or possessing for (purposes listed above in the protocol) child pornography*".

Article 9 of the Council of Europe Convention on Cybercrime holds that "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right*", some listed activities including "*producing child pornography for the purpose of its distribution through a computer system*", "*offering or making available child pornography through a computer system*", "*distributing or transmitting child pornography through a computer system*", "*procuring child pornography through a computer system for oneself or for another person*" and "*possessing child pornography in a computer system or on a computer-data storage medium*".

Both aspects of child protection mentioned above are also emphasised by the EU Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography[486], which notably holds that "*each Member State shall take the necessary measures to ensure that (some listed) intentional conduct (are) punishable*", such as "*coercing a child into prostitution or into participating in pornographic performances*" and "*engaging in sexual activities with a child*", in some listed circumstances[487]. The Council Framework Decision holds moreover in its article 3 that Member States shall ensure that production of child pornography is punishable, "*when committed without right*", as well as "*distribution, dissemination or transmission of child pornography*", "*supplying or making available child pornography*" and "*acquisition or possession of child pornography*".

However, only the right to protection against crime appears specifically as a human right, a fundamental freedom and, in most of countries, a civil liberty. The right for children to not be the victim of a child pornography image is indeed not specifically identified in itself in the texts analysed.[488] Those texts do not aim to declare such a right, but are rather pursuing the aim to favour the implementation, into national legal systems, some crucial means that the protection of children's other fundamental rights, especially the right to be protected from sexual violence and the right to development.

However, the importance of the fight against child pornography, as well as the importance of protecting children against violence and impaired personal development, is very often an argument to justify the implementation of Internet blocking measures. In some countries it is often the only justification by governments or private entities who are requesting the implementation of an Internet blocking measure – often requesting that such blocking be restricted to child pornographic content only.

This justification, which seems highly reasonable, is however, difficult to understand from a legal point of view. 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.

[485] Preamble of the Convention, § 4.
[486] O.J.E.C. of 20 January 2004, L 013, pp. 0044-0048, available at this address: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML
[487] Article 2 of the Council framework Decision.
[488] See 6.5.2.2.

6.7.2 The protection of people against 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 emphasis specifically the right to any individual to be protected against discrimination. Such texts refer to "*any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life*"[489].

The United Nations International Convention on the elimination of all forms of racial discrimination[490] therefore holds that "*each State Party shall prohibit and bring to an end, by all appropriate means, including legislation as required by circumstances, racial discrimination by any persons, group or organization*"[491]. State Parties shall also "*condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention*"[492].

The "general prohibition of discrimination" stated in article 1 of the protocol n° 12 to the European Convention on Human Rights holds that "*the enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status*". As analysed previously[493], the EU Council Directive of 29 June 2000, "*implementing the principle of equal treatment on grounds of racial and ethnic origins*" also prohibits "*all forms of discrimination on grounds of race or ethnic origin*"[494].

Protection of people against discrimination is therefore of high importance, internationally, and is a human right and a fundamental freedom. It is also, in most countries, a civil liberty. This specific protection additionally includes in one of its parts a general prohibition of violence or torture, which can be repressed in a more severe way, at the national level, when committed for racist motives[495].

On the Internet, content that falls under these prohibitions can be texts encouraging discrimination, but also images of torture or murders, committed for racial motives. The latter, as well as torture or murders in general, are very disturbing and would also offer an equally valid justification of Internet blocking, in addition to child pornography, in such cases where Internet blocking were possible and would correspond to certain conditions provided for at the international level, which are covered in Chapter 7 .

From a legal point of view, other content such as intellectual property rights (IPR) infringements could, following the same logic, also justify an Internet blocking measure, since

---

[489] Article 1 of the Convention.
[490] Adopted and opened for signature and ratification by General Assembly resolution 2106 (XX) of 21 December 1965, entered into force on 4 January 1969, available at the following address: http://www2.ohchr.org/english/law/cerd.htm.
[491] Article 2, d, of the Convention.
[492] Article 4 of the Convention.
[493] See above, section 6.5.2.3.
[494] See the EU website, Summaries of EU legislation, Equal treatment on grounds of racial and ethnic origin, available at the following address: http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33114_en.htm
[495] See for instance articles 222-3, 222-8 and 222-10 of the French penal Code, available in English at this address: http://www.legifrance.gouv.fr/.

they are also illegal within the framework of the Council of Europe. This is true even if they are less prejudicial to the human being than the previous contents outlined above.

6.7.3 Intellectual property rights

Intellectual property rights (IPR) are protected by numerous treaties at the international level. This document limits such analysis to the general declarations of such rights, which notably include copyrights and related rights, which "*protect the rights of authors, performers, producers and broadcasters, and contribute to the cultural and economic development of nations*"[496].

Intellectual property rights are first protected by article 27, 2 of the Universal Declaration on Human Rights, which holds that "*everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author*". These rights are also protected by article 15, 1 of the International Covenant on Economic, Social and Cultural Rights, which holds that "*the States Parties to the present Covenant recognize the right of everyone (…) to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author*".

In the Council of Europe, the European Court of Human Rights protects rights of ownership of non-material goods under article 1 of the first additional protocol to the ECHR[497]. At the national level, the French constitutional Council for instance also protects such rights[498]. At the EU level, the EU Charter on Fundamental Rights also states, in its article 17, 2, that "Intellectual property shall be protected" [499].

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 actually protect it.

A rather simplistic reading of the European Court of Justice Promusicae judgement by certain authors[500] interprets this as demanding a rebalancing of rights, making intellectual property more important, relatively speaking.

---

[496] World Intellectual Property Organization (WIPO), "Copyright and Related Rights", available on the WIPO website at this address: http://www.wipo.int/copyright/en/.

[497] See for instance *Anheuser-Busch Inc. V. Portugal*, Judgment of the Court of 11 January 2007, application n° 73049/01, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=intellectual%20|%20property&sessionid=28001124&skin=hudoc-en. The decision holds in its § 63 that "*The concept of "possessions" referred to in the first part of Article 1 of Protocol No. 1 has an autonomous meaning which is not limited to ownership of physical goods and is independent from the formal classification in domestic law: certain other rights and interests constituting assets can also be regarded as "property rights", and thus as "possessions" for the purposes of this provision*". § 71 of this decision recalls that "*in the case of Melnychuk v. Ukraine, which concerned an alleged violation of the applicant's copyright, the Court reiterated that Article 1 of Protocol No 1 was applicable to intellectual property*". §§ 67 and 68 recall that a patent might also "*falls within the scope of the term 'possessions' in Article 1 of Protocol No. 1*".

[498] See for instance decision n°2006-540 DC of 27 July 2006, J.O.R.F. of 3 August 2006, p. 11541, §§ 13 and 14.

[499] On each on the issues raised in these two first paragraphs, see Christophe Caron, "Droits d'auteurs et droits voisins", Litec, 2006, page 8.

[500] See, for example, Fanny Coudert and Evi Werkers, "In The Aftermath of the Promusicae Case: How to Strike the Balance?", International Journal of Law and Information Technology Advance Access published online on October 25, 2008

6.8 Specific provisions related to electronic communications

An Internet blocking measure that interferes in freedoms has to be prescribed by law and has to respect the other elements of the European public order clause, which often requires the involvement of a judge, who will be able to assess the proportionality of the blocking measure within the framework of the guarantees that have to apply to any criminal trial.

Such a blocking measure provided for within the European Union must furthermore comply with European rules applying to electronic communications. Those rules are especially the ISPs obligations in terms of quality of service and universal service and the ISP's obligation of neutrality. Moreover, the rules concerning the Internet Service Provider liability regime are a further basis for Internet Service Providers to argue against blocking measures that are implemented outside the framework of a law.

6.8.1 ISP universal service and quality of service obligations

In "*response to the convergence of technology, which increasingly makes it possible for all forms of content to be delivered over all types of networks*", the EU Parliament and the Council adopted "*five directives that extends the regulatory framework for telecommunications to cover all forms of electronic communications infrastructure, including cable networks, satellite networks, networks used for broadcast transmission, IP networks, power line communications systems, as well as the traditional fixed and mobile network used for voice or data*" [501].

Among those five Directives, , the "Framework Directive" 2002/21/EC [502] and the "Universal service Directive" 2002/22/EC[503] hold provisions related to the Universal service and to the quality of certain services, which may be in conflict with an Internet blocking measure[504].

6.8.1.1 Right to access basic communication services

The EU Directive 2002/22/EC aims "*to ensure the availability throughout the Community of good quality publicly available (electronic communications) services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market*"[505].

The Directive defines therefore the "*minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition"* [506], which corresponds to the definition of the "universal service"[507]. The Directive "*also sets out obligations with regard to the provision of certain mandatory services (…)*" [508].

According to article 3.1 of the Directive, "*Member States shall ensure that the services set out in (Chapter II) are made available at the quality specified to all end-users in their territory, independently of geographical location, and, in the light of specific national conditions, at an affordable price*".

Within that framework, Member States may also, "*in the context of universal service obligations and in the light of national conditions, take specific measures for consumers in*

---

[501] Antony Oodan, Keith Ward, Catherine Savolaine, Mahmoud Daneshmand, Peter Hoath, "Telecommunications Quality of Service Management, from legacy to emerging services", Institution of Electrical Engineers, IEE Telecommunications series 48, 2002, p. 382.

[502] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002, on a common regulatory framework for electronic communications networks and services (Framework Directive), O.J.C.E. of 24 April 2002, L 108/33.

[503] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002, on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), O.J.E.C. of 24 April 2002, L 108/51.

[504] Beside Directive 2002/21/EC and Directive 2002/22/EC, the other Directives of the Telecom Package are the **Directive 2002/19/EC** of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), O.J.C.E. of 24 April 2002, L 108, pp. 0007-0020; **Directive 2002/20/EC** of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), O.J.E.C. of 24 April 2002, L 108/21; **Directive 2002/58/EC** of the European Parliament and of the Council of 7 March 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), J.O.E.C. of 31 July 2002, L 201, pp. 0037-0047.

[505] Article 1 of the Directive. See also Antony Oodan, Keith Ward, Catherine Savolaine, Mahmoud Daneshmand, Peter Hoath, "Telecommunications Quality of Service Management, from legacy to emerging services", op cit, p. 383.

[506] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002, Article 1, 2). See also § 4 of the Directive.

[507] See § 4 of the Directive: "Ensuring universal service (that is to say, the provision of a defined minimum set of services to all end-users at an affordable price) (…)".

[508] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002, Article 1, 2). See also § 4 of the Directive.

rural or geographically isolated areas to ensure their access to the services set out in the Chapter II and the affordability of those services, as well as ensure under the same conditions this access, in particular for the elderly, the disabled and for people with special social needs. Such measures may also include measures directly targeted at consumers with special social needs providing support to identified consumers, for example by means of specific measures, taken after the examination of individual requests, such as the paying off of debts".

Services included in the universal service obligation are "*basic communications services, including voice communications and a connection to the Internet*"[509]. Article 4 of the Directive holds that "*Member States shall ensure that all reasonable requests for connection at a fixed location to the public telephone network and for access to publicly available telephone services at a fixed location are met by at least one undertaking*". Paragraph 2 of article 4 holds that "*the connection provided shall be capable of allowing end-users to make and receive local, national and international telephone calls, facsimile communications and data communications, at data rates that are sufficient to permit functional Internet access, taking into account prevailing technologies used by the majority of subscribers and technological feasibility*". *(…)".*

Both of these services, that is to say access to the public telephone network and access to the Internet, may suffer from an Internet blocking measure.

6.8.1.1.1 *Access to the public telephone network*

The Directive aims to ensure the EU citizens' can connect to the public telephone network and also to ensure the quality of the service provided. It notably creates an assessment mechanism of such a quality in its article 11, 4, adding that national regulatory authorities, which are defined by art. 3 of the Directive 2002/21/EC, "*shall be able to set performance targets for those undertakings with universal service obligations at least under Article 4. In so doing, national regulatory authorities shall take account of views of interested parties (…)*". Other obligations are provided for, as the one for Member States to "*ensure that, in addition to any other national emergency call numbers specified by the national regulatory authorities, all end-users of publicly available telephone services, including users of public pay telephones, are able to call the emergency services free of charge, by using the single European emergency call number 112*"[510].

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. This would be the case for a measure that would lead to the suspension or the interruption of an Internet triple play offer, which allows the Internet user to access not only the Internet but also to the telephone and the television. If the proposals to interrupt an Internet access are currently related only to the Internet, and not the telephone offer that could accompany the global offer[511], the difficulty to make such a distinction has been highlighted at the French level[512]. In any case,, where the distinction is technically feasible through the implementation

[509] European Commission website, Europe's Information Society, Thematic portal, Policies, eCommunications, "Universal service", available at the following address: http://ec.europa.eu/information_society/policy/ecomm/current/consumer_rights/universal_service/index_en.htm.

[510] Article 26, 1 of the Directive 2002/22/EC.

[511] It is at least the aim of the French initiative against IPR infringements.

[512] See for instance the report of the French regulatory authority, called "ARCEP", to the French government within the framework of the discussions of the draft law called "creation and Internet". The authority considered that ISPs must "ensure a permanent and continuous networks' exploitation, and guarantee a non-interrupted access to emergency services. Failing that, the ISP would incur administrative and penal sanctions" (translated from French): "L'Arcep dénonce l'excès de precipitation de la loi Hadopi", 29 May 2008, Pc Inpact, available at http://www.pcinpact.com/actu/news/43857-arcep-report-hadopi-olivennes-loi.htm; Estelle Dumout, "Riposte graduée: l'Arcep demande au gouvernement de retoucher sa copie", 28 May 2008, ZDNet, available at: http://www.zdnet.fr/actualites/internet/0,39020774,39381371,00.htm. See also Jean Berbinau, Jean-Claude Gorichon, Dominique Varenne, « Création et Internet », rapport n° IV-3.3-2008 – Décembre 2008, pp. 16 and seq., report available at this address: http://www.lesechos.fr/medias/2009/0304/300333937.pdf.

of some specific mechanisms on the network, such a technical mechanism may be source of technical problems or breakdowns, which may logically lead to more frequent telephone interruptions.

Beside the difficulty that such an Internet-access interruption can create as regards universal service obligations, it can also put some people in danger, when the Internet subscription is the only way to make a phone call. Such a measure could also be more severe for disabled people, whose right to access electronic communications seems to be protected under the freedom they are able to exercise thanks to these communications[513], and who could be more particularly reliant on a permanent connection to the public phone network, at the most affordable price.

All these developments emphasise the necessity to impose Internet access suspension or interruption as a sanction in only certain specific situations, where the behaviour being sanctioned can only be appropriately suppressed by such a suspension or interruption[514], after having verified that the Internet user is at this occasion not deprived from its ability to make a telephone call, at least in case of danger.

Such a conclusion is further validated by the fact that Internet access is also an element of universal service, at least as regards "functional" low-speed access.

6.8.1.1.2 *Access to the Internet*

Article 4 of the Directive holds that the connection "*at a fixed location to the public telephone network*" shall be provided to citizens "*at data rates that are sufficient to permit functional Internet access, taking into account prevailing technologies used by the majority of subscribers and technological feasibility*".

Recital 8 of the Directive adds that "*the requirement is limited to a single narrowband network connection*" and that "*the speed of Internet access experienced by a given user may depend on a number of factors including the provider(s) of Internet connectivity as well as the given application for which a connection is being used*". Therefore, this paragraphs holds that "*it is not appropriate to mandate a specific data or bit rate at Community level*", noticing that "*currently available voice band modems typically offer a data rate of 56 kbit/sec and employ automatic data rate adaptation to cater for variable line quality, with the result that the achieved data rate may be lower than 56 kbit/sec*".

Therefore, the universal service obligation includes at least low-speed Internet access. Any Internet service suspension or interruption that would prevent a person to access internet at least at low-speed could be therefore in contradiction with the Directive.

Indeed, the universal service obligation is above all stated in terms of providing a material connection, by ensuring that each home has the possibility to connect to the Internet, and not in terms of effective connection. Allowing citizens to access the Internet stays an objective that has to be balanced with other rights or freedoms, or the general interest of the public. But the inclusion of this obligation into the universal service obligations, which constitute for the French Senate "*the concrete expression of legal main principles of the public service (service public): equality, continuity, adaptability*"[515], implies the importance of electronic communications for the exercise of fundamental freedoms and a country should not deliberately restrict the right to use such communications without a reason that would be

[513] See above, section 6.6.3.
[514] See above section 7.6.4.
[515] Sénat, session ordinaire de 2003-2004, Annexe au procès-verbal de la séance du 15 octobre 2003, Rapport fait au nom de la commission des Affaires économiques sur le projet de loi relatif aux obligations de service public des télécommunications et à France Télécom, par M. Gérard Larcher, Sénateur, available at this address: http://cubitus.senat.fr/rap/l03-021/l03-0210.html; (quotation *in* Exposé général, I, A, 1., b) les prestations de service universel, available at the following address: http://cubitus.senat.fr/rap/l03-021/l03-0211.html).

proportionate to the aim that has to be reached. Internet access is supposed to have the same statute within the EU as the telephone, and no EU country seems to have thought, for instance, about preventing a citizen from accessing to the telephone network from his home to repress a penal offence committed by using this same telephone connection.

This necessity not to prevent a person from accessing the Internet or a part of it outside the framework of a decision that balances this right with another interest of equivalent value and a decision to do so should be taken by a court of law[516]. This approach appears in the draft texts voted by the Parliament within the framework of the reform of the EU telecom legislation.

New paragraph 3a of the Directive 2009/…/EC in preparation, amending Directives 2002/21/EC, 2002/19/EC and 2002/20/EC[517], declares that: "*Recognising that the internet is essential for education and for the practical exercise of freedom of expression and access to information, any restriction imposed on the exercise of these fundamental rights should be in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms. Concerning those issues, the Commission should start a wide public consultation*".

Point 8 of the same draft Directive adds, to paragraph 4 of article 8 of the existing Directive 2002/21/EC, "*the national regulatory authorities shall promote the interests of the citizens of the European Union by inter alia:*", the two following new points: *"g) promoting the ability of end-users to access and distribute information or run applications and services of their choice*" and "*h) applying the principle that no restriction may be imposed on the fundamental rights and freedoms of end-users, without a prior ruling by the judicial authorities, notably in accordance with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information, save when public security is threatened in which case the ruling may be subsequent*".

New paragraph 22a of the Directive 2009/…/EC in preparation, amending Directives 2002/22/EC, Directive 2002/58/EC and Regulation (EC) n° 2006/2004,[518] holds that "*Directive 2002/22/EC (Universal Service Directive) neither mandates nor prohibits conditions imposed by providers, in accordance with national law, limiting users' access to and/or use of services and applications but does provide for information regarding such conditions. Member States wishing to implement measures regarding users' access to and/or use of services and applications must respect the fundamental rights of citizens, including in relation to privacy and due process, and any such measures should take full account of policy goals adopted at Community level, such as furthering the development of the Community information society*".

Article 1 of the same Directive 2009 amends Directive 2002/22/EC, by including in its article 1 that "*This Directive neither mandates nor prohibits conditions, imposed by providers of publicly available electronic communications and services, limiting users' access to and/or use of services and applications, where allowed under national law and in conformity with Community law, but does provide for information regarding such conditions. National*

---

[516] See above section 7.8.2.

[517] Position of the European Parliament adopted at second reading on 6 May 2009 with a view to the adoption of a Directive 2009/…/EC of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on acces to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, P6_TC2-COD(2007)0247, available at the following address: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20090506+ITEMS+DOC+XML+V0//EN&language=EN#BKMD-22.

[518] Position of the European Parliament adopted at second reading on 6 May 2009 with a view to the adoption of a Directive 2009/…/EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and user's rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, P6_TC2-COD(2007)0248, available at the following address: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20090506+ITEMS+DOC+XML+V0//EN&language=EN#BKMD-15.

measures regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process, as defined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms"[519]. The article adds that "*the provisions of this Directive concerning end-users' rights shall apply without prejudice to Community rules on consumer protection, in particular Directives 93/13/EEC and 97/7/EC, and national rules in conformity with Community law*"[520].

In addition, high speed Internet could be included in the universal service in the future.

The Council of Europe's Committee of Ministers, in a Recommendation that was considered as a recognition of the Internet access as a fundamental right[521], declared the following: "*Aware of the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions, entertainment) and the resulting legitimate expectation that Internet services be accessible, affordable, secure, reliable and ongoing and recalling in this regard Recommendation Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet*"[522].

At a more international level, a joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of Media and the OAS Special Rapporteur on Freedom of Expression declares that "*the right to freedom of expression imposes an obligation on all States to devote adequate resources to promote universal access to the Internet, including via public access points*"[523].

At the EU level, the European Commission itself declared to the French government that the "*diffusion of high speed"* Internet access was an "*important objective*" and that "*the need to fight against online piracy*" had to be balanced with it. The Commission noted on this occasion that "*the French presidency of the EU was upholding the high speed notion as coming under the universal service*"[524].

As regards the modification of the telecom legislation, §2 of recital 3a of the draft Directive 2009/…/EC, amending Directives 2002/22/EC, Directive 2002/58/EC and Regulation (EC) n° 2006/2004[525], no longer limits "*the requirement (…) to a single narrowband network connection*"[526]. It holds that "*it is not appropriate to mandate a specific data or bit rate at*

[519] §2a of the new article 1 of Directive 2002/22/EC.
[520] §3 of the new article 1 of Directive 2002/22/EC.
[521] See Monica Ermert for Intellectual Property Watch, "Council of Europe: Access to internet is a fundamental right", 10 June 2009, available at: http://www.ip-watch.org/weblog/2009/06/08/council-of-europe-access-to-internet-is-a-fundamental-right/ or http://oneworldsee.org/node/18675.
[522] Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, § 12, available at the following address: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.
[523] Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of Media and the OAS Special Rapporteur on Freedom of Expression, 21 December 2005, § 13, available at the following address: http://www.article19.org/pdfs/standards/three-mandates-dec-2005.pdf.
[524] Translated from French. La Tribune.fr, "Loi antipiratage sur Internet: les observations de Bruxelles", 27 November 2008, available at the following address: http://www.latribune.fr/entreprises/communication/telecom-internet/20081127trib000314818/loi-antipiratage-sur-internet-les-observations-de-bruxelles-.html.
[525] Position of the European Parliament adopted at second reading on 6 May 2009 with a view to the adoption of a Directive 2009/…/EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and user's rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, P6_TC2-COD(2007)0248, available at the following address: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20090506+ITEMS+DOC+XML+V0//EN&language=EN#BKMD-15.
[526] See above, first § of the current sub-section.

Community level. Flexibility is required to allow Member States to take measures where necessary to ensure that a data connection is capable of supporting satisfactory data rates, which are sufficient to permit functional internet access, as defined by the Member States, taking due account of specific circumstances in national markets, for instance the ***prevailing bandwidth used by the majority of subscribers in that Member State****, and technological feasibility, provided that these measures seek to minimize market distortion (…)".* The draft Directive adds in the same recital, that "*this is without prejudice to the need for the Commission to conduct a review of the universal service obligations, which may include the financing of such obligations, in accordance with Article 15 of Directive 2002/22/EC, and if appropriate, present proposals for reform to meet public interest objectives*".

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, there would be specific EU legal provisions recalling that a state is not authorised to take any user or content 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.

Whatever the conclusion of the debate on the telecom package will be, an Internet access service must currently meet certain quality requirements that may also be endangered by a blocking measure.

6.8.1.2 Quality of the Internet access service

Directive 2002/22/EC is notably about quality of service, which can be defined as the "*collective effect of the performance levels of all parameters considered pertinent to a service. The set of parameters for a given service may have different priorities and performance level requirements by different segment of users*"[527].

Paragraph 1 of article 22 of the Directive holds that "*Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to require undertakings that provide publicly available electronic communications services to publish comparable, adequate and up-to-date information for end-users on the quality of their services (…)*". Paragraph 2 holds that "*National regulatory authorities may specify, inter alia, the quality of service parameters to be measured, and the content, form and manner of information to be published, in order to ensure that end-users have access to comprehensive, comparable and user-friendly information. Where appropriate, the parameters, definitions and measurement methods given in Annex III could be used*".

Member States that have implemented this Directive also have national provisions in that area. In France, for instance, article L. 33-1 of the Posts and electronic communications Code holds that "*the establishment and exploitation of networks open to the public and the provision to the public of electronic communications services are submitted to the respect of rules related to (…) the conditions of permanence, quality and availability of the network and of the service*". Article D. 98-4 of the same Code holds in a first section entitled "*conditions of permanence of the network and of the services*" that "*the operator must make the necessary arrangements to ensure on a continuous and permanent way the exploitation of the network and of the electronic communications services and to ensure a remedy is found to the effects of a system's fault debasing the quality of service for the whole or a part of the customers, with absolutely minimum delays. It makes all the arrangements in order to guarantee uninterrupted access to emergency services. The operator implements the necessary protections and redundancies to guarantee a satisfactory quality and availability of service*".

[527] Antony Oodan, Keith Ward, Catherine Savolaine, Mahmoud Daneshmand, Peter Hoath, "Telecommunications Quality of Service Management, from legacy to emerging services", Institution of Electrical Engineers, IEE Telecommunications series 48, 2002, p. xxii (Glossary).

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

However, it is noted in Chapter 5 that networks are technically very complex and that most Internet blocking measures are susceptible to increase breakdowns and latencies. This is because they always implement some new options on equipment that was not originally designed to support such functionalities, or to implement new equipment at the level of access equipment (DSLAM ADSL, optic DSLAM –FTTH- for fixed internet, Node B or BTS for wireless), which will prevent operators from having good visibility on network operations and functioning.

As a result, operating an electronic communications network and blocking are philosophically in opposition, and asking an operator to implement a blocking measure would put it in a position where two obligations with contradictory effects have to be respected.

This is another argument for not requesting the industry of a given country to implement blocking on the basis of a contract or an agreement with the government, but to hold the measure within a law, which would take into account the possible interference of the blocking measure in the other obligations the operators are legally responsible for.

Such a law should also respect the Internet Service Provider's obligation of neutrality.

6.8.2 ISP's obligation of neutrality

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 telephone and post), especially justified by an imperative of protecting the secrecy of Internet users' private life and correspondence, in addition to the necessary protection of the freedom of expression, which implies that only a judge should have the power to prevent the distribution of specific content[528].

This obligation is declared in Directive 2000/31/CE, which aims "*to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such*"[529]. Recital 14 of the Directive specifies that "*the implementation and application of this Directive should be made in full compliance with the principles* ***relating to the protection of personal data, in particular as regards (…) the liability of intermediaries***". Recital 15 of the Directive declares that "***The confidentiality of communications is guaranteed*** *by Article 5 Directive 97/66/EC[530]; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised*".

Directive 2002/58/EC moreover holds, in its article 5, 1, that "*Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality*".

At the local level, countries have generally also made provisions to guarantee the confidentiality of communications, at least at the occasion of the implementation of the Directive. In France, for example, the ISP's obligation of neutrality is currently expressed by the Code of posts and electronic communications (CPEC). Article L.33-1 of this Code holds that "*the establishment and the exploitation of networks open to the public and the provision to the public of electronic communications services are submitted to the respect of rules related to (…)b) conditions of confidentiality and of neutrality as regards messages transmitted and information linked to communications".* Article D. 98-5 of the CPEC holds that the operator "*takes the necessary measures to guarantee the neutrality of its services vis-à-vis the content of messages transmitted on its network and the secrecy of correspondence*". On the basis of article L. 32-1, II, 5° of the CPEC, the Ministry in charge of electronic communications and the national regulatory authority are in charge of ensuring that this obligation is respected. Criminal provisions ensure the respect, in a general way, of the privacy of correspondence[531].

---

[528] See section 7.8.

[529] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), O.J.E.C. of 17 July 2000, L 178, pp. 0001 – 0016, Ground 8, available at the following address: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

[530] Directive 97/66/EC has been repealed and replaced by Directive 2002/58/CE.

[531] 432-9 of the French penal Code holds: "Except where provided for by law, the ordering, committing or facilitation of the misappropriation, suppression or opening of correspondence, and the disclosure of the contents of such correspondence, by a person holding public authority or discharging a public service mission acting in the course of or on the occasion of his office or duty, is punished by three years' imprisonment and a fine of €45,000"; "The same penalties apply to the persons referred to under the previous paragraph, or to employees of electronic communication networks open to the public, or to employees of a supplier of telecommunication services, who, acting in the performing of their office, order, commit or facilitate, except where provided for by law, any interception or misappropriation of

To this obligation for an ISP to stay neutral vis-à-vis the content of the messages that are exchanged on its network, the Directive adds the impossibility, for a member state, to *"impose a general obligation on providers, when providing the services covered by Articles 12 (access or "mere conduit" service), 13 (caching service) and 14 (hosting service), to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity"*[532].

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 of a legal obligation that would justify its non respect of the neutrality principle.

An Internet Service Provider does not have the possibility to monitor contents that are exchanged through its network, except on the basis of a specific obligation stated by the law, to preserve a legitimate aim.

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. That would be the case of any measure that would allow monitoring content sent on the Internet by a user, e.g. by writing on a particular forum or by transmitting a file via FTP (File Transfer Protocol).

Such a law would further not be able to provide for a general obligation, for the ISP, to monitor the content it transmits. This European provision can be a huge obstacle to a blocking measure, since each blocking measure implies monitoring of all the content sent or received on a given protocol, in order to block the specific kind of content that have to be blocked.

Without a law that obliges them to block some kinds of content, ISPs can also not monitor and block web content, without being in breach of the condition of their liability waiver provided by the EU Directive, and therefore risking liability for all content they transmit.

correspondence sent, transmitted or received by a means of telecommunication, or the use or the disclosure of its contents"; Article 226-15 of the penal Code holds: "Maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of €45,000"; "The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions".

[532] Article 15 of the Directive.

6.8.3 The Internet Service Provider liability mechanism

Article 12 of Directive 2000/31/EC holds that "*Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission*".

Article 12.3 adds that these provisions "*shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement*".

These provisions were also integrated into the national legal systems of the Member states. In France, article L. 32-3-3 of the CPEC states that persons "*who ensure a service that consists of content transmission in a communication network or of the provision of access to a communication network*" can only be liable for those contents, on a civil or penal point of view, "*when they are at the origin of the litigious transmission, when they select the recipient of the transmission, or when they select or modify content that are the subject of the transmission*".

As a result, an ISP that would select some content to block, without being obliged to do so by the law, would be susceptible to fall outside the requirements for the application of this specific liability scheme. Such an ISP would therefore take the risk of seeing its liability challenged before a court for every piece of illegal content that would be potentially transmitted through its services such as IPR infringements, privacy violations or slander. Such a situation would be legally very uncertain. It would endanger the Internet Service Provider sector itself, and more globally the technological development of the country.

Chapter 7 BALANCING FUNDAMENTAL FREEDOMS

7.1 Introduction

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, with the aim of preserving another.

Within the framework of an Internet blocking measure, children's rights, the right of persons not to be discriminated against or intellectual property rights, have to be balanced with the rights and freedoms 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[533], as the right to respect for private life and the right to freedom of expression.

This chapter covers all the issues relevant to such limitations. Section 7.2 describes the public order clause which provides guidelines on how fundamental rights can be legitimately restricted. Section 7.3 explains the principle of a legitimate aim which is used to identify the purpose for which an Internet blocking measure is put in place and whether this purpose is reasonable. This section reviews a range of concrete aims for Internet blocking and explains how each of these might be seen as legitimate or not. Section 7.5 considers the principle of necessity in a democratic society and whether Internet blocking measure fulfils a pressing social need. Several specific social needs are identified and reviewed. This principle of necessity includes a requirement that any limitation on fundamental freedoms needs to be proportionate to the legitimate aim pursued.

Section 7.6 reviews the proportionality criteria in comparison to Internet blocking attempts in the context of different Internet services and the objectives that blocking attempt is trying to achieve. Section 7.7 explains the additional interferences which are enabled by several Internet blocking measures and how guarantees are needed to ensure the blocking system is prevented from extending its functionality specified in its original legitimate aim. Section 7.8 explains the role of a judge in determining if an Internet blocking measure is proportional and what content can be blocked. It describes the problems if this role is taken on by others. Section 7.9 concludes with a summary of what steps need to be taken to ensure that an Internet blocking measure is legitimate in a democratic society. Section 7.10 provides a list of additional studies which are needed in order to properly consider the proportionality of several Internet blocking measures.

7.2 The "Public Order Clause"

Such a limitation must respect certain conditions, which will directly depend on the nature of the protected freedom or right. Each Internet blocking measure must respect the conditions under which a limitation of fundamental freedoms is possible.

[533] Frédéric Sudre, op-cit, pages 44-45.

These conditions are provided for by the European Convention on Human Rights and in some extent by the International Covenant on Civil and Politic Rights, within a so-called "public order clause", supervised and clarified by the European Court of Human Rights.

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, such as article 5 of the ECHR related to the right to liberty and security[534].
- Other provisions that proclaim conditional rights, such 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*" [535] 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*"[536] [537].

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*"[538]
    - corresponds to a "*pressing social need*"[539]
    - is "*proportionate to the legitimate aim pursued*"[540].

This public order clause, as interpreted by the European Court of Human Rights, should also be applied to any restriction to the right to freedom of expression guaranteed by article 19 of the ICCPR,[541] as this article uses almost the same wording as the European Convention on Human Rights.[542] Countries that are party to the ICCPR but not the ECHR can take inspiration of the Court's interpretation, with the aim of harmonisation of interpretation of International law in the field of human rights. With regards to article 17 of the ICCPR related to the right of

[534] Article 5 holds six possible cases of dispensations that have to be brought "*in accordance with a procedure prescribed by law*".
[535] Frédéric Sudre, op cit pages 44-45.
[536] *Sunday Times v. The United Kingdom*, application n° 6538/74, 26 April 1979, Series A, n° 30, § 45, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=freedom%20|%20expression&sessionid=27574169&skin=hudoc-en. See also *Times newspapers LTD* (n° 1 and 2) *v. The United Kingdom*, Judgment of 10 March 2009**,** application 3002/03 and 23676/03), § 37: "*Such interference breaches Article 10 unless it was "prescribed by law", pursued one or more of the legitimate aims referred to in Article 10 § 2 and was "necessary in a democratic society" to attain such aim or aims*".
[537] On this discussion see also Jeremy McBride, "Proportionality and the European Convention on Human Rights, in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et seq., especially p. 24.
[538] Joint dissenting opinion of judges Wiarda, Cremona, Thór Vilhjálmsson, Ryssdal, Ganshof van der Meersch, Sir Gerald Fitzmaurice, Bindschedler-Robert, Liesch and Matscher, §8, available under the Sunday Times court case, op cit.
[539] Sunday Times v. The United Kingdom, op cit, § 59.
[540] *Sunday Times v. The United Kingdom*, op cit, § 63. See also Frédéric Sudre, op cit, page 43; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 86.
[541] Article 19 holds in its point 3: "The exercise of the rights (to hold opinions and to freedom of expression) carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others, (b) For the protection of national security or of public order (ordre public), or of public health or morals".
[542] Except it does not refer to "a democratic country" and lists less legitimate aims in which an interference is acceptable.

private life[543], this does not use the same terminology as the ECHR and could therefore permit interferences that would not be qualified as solely "arbitrary" or "unlawful", by public authorities that would choose to not follow the more restrictive criteria of the European Convention on Human Rights.

As a result, the conditions listed in this public order clause, which also apply to the rights proclaimed in the EU charter[544], and which influence national constitutional courts such as the French Constitutional Council[545], should be respected in relation to any Internet blocking measure that interferes in the right to freedom of expression within the 164 countries that are parties to the ICCPR. These conditions also have to be respected by the 47 countries that are parties to the ECHR. These conditions must be respected within the framework of a blocking measure that interferes in the right to respect for private life, at least for the ECHR party countries. Lack of respect for these conditions would mean that the interference is *"a violation"*[546] of Articles 8 or 10 of the ECHR. Therefore, it is important to analyse blocking in detail in the light of each of the conditions.

[543] Article 17 holds: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation"; "2. Everyone has the right to the protection of the law against such interference or attacks".

[544] Article 52 of the EU Charter holds: "Insofar as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection". This provision "is intended to ensure the necessary consistency between the Charter and the ECHR by establishing the rule that, insofar as the rights in the present Charter also correspond to rights guaranteed by the ECHR, the meaning and scope of those rights, including authorised limitations, are the same as those laid down by the ECHR". See the EU Charter of Fundamental Rights website, "7. General Provisions", "Art. 52. Scope of guaranteed rights", available at this address: http://www.eucharter.org/home.php?page_id=62.

[545] The French Constitutional Council recognises the exclusive competence of the Parliament to hold limitations to freedoms, accordingly to article 34 of the Constitution and art. 4 of the French Human and Citizen Rights Declaration of 1789. This Council also considers that the lawmaker "*can only limit the exercise of a freedom for a constitutional imperative*" (see Frédérique Lafay, note under the Council decision of 18 January 1995, JCP 95, II, 22 525). This council considers furthermore that "*any restrictions placed on the exercising of (freedoms) must necessarily be* adapted and proportionate to the purpose it is sought to achieve" (see for instance Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 15).

[546] Sunday Times v. The United Kingdom, op cit, § 45.

7.3 The principle of lawfulness

Each time the European Court of Human Rights has to pronounce on an alleged violation of the right of private life or the right to freedom of expression, it analyses first if the interference was "*in accordance with the law*"[547].

According to the Court, this formula, which has to be reconciled "*as far as possible*" with other notions such as "*prescribed by law*" or "*provided for by law*"[548], to "*realise the aim and achieve the object of the treaty*", implies at least two requirements[549].

- First, "*the law must be adequately accessible*", which means that "*the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case*"[550].

  Law is here understood "*in its substantive sense, not its formal one"*. It includes therefore "*non-written law*", "*enactments of lower rank than statutes*", and sometimes case law, that "*has traditionally played a major role in continental countries, to such an extent that whole branches of positive law are largely the outcome of decisions by the courts*". "*In a sphere covered by the written law, the "law"*" is therefore "*the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments*" [551].

- Secondly, "*a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct*". The citizen must therefore "*be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*"[552]. This condition of clarity of the law was also linked to the legal security principle by the European Court of Justice[553]. At the national level, it was for instance implemented by article 34 of the French Constitution by the French Constitutional Council[554], which considers more globally that the principles of clarity, accessibility and intelligibility of the law impose on the law-maker to "*adopt disposals of sufficient precision and non-equivocal formula in order to prevent subjects of the law[555] from an interpretation that would be in opposition with the Constitution or from the risk of arbitrary*"[556].

---

[547] See for instance, in relation with the right of private life, *Niemietz v. Germany*, judgment of 16 December 1992, Series A no. 251 B, p. 33, § 29, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695764&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[548] The Court considers that these notions are "equally authentic but not exactly the same".

[549] See *Sunday Times v. The United Kingdom*, judgment of 26 April 1979, application n° 6538/74, Series A, n° 30, § 48, available at this address: http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=freedom%20|%20expression&sessionid=27574169&skin=hudoc-en.

[550] *Sunday Times v. The United Kingdom*, op cit, § 49. On this question, see also Pascale Deumier, « La publication de la loi et le mythe de sa connaissance », Les petites affiches, 6th March 2000, n° 46.

[551] All quotations are coming from the European Court of Human Rights case *Kruslin v. France*, judgment of 24 April 1990, Series A, n° 176 A, p. 20, § 29. On this issue see also Frédéric Sudre, op cit, page 43; R. Koering-Joulin, D. 90, chron. p. 187.

[552] All quotations are coming from the European Court of Human Rights case *Sunday Times v. The United Kingdom*, op cit, § 49. See also Frédéric Sudre, op cit, page 43; Steve Foster, Human Rights and Civil Liberties, 2nd ed., 2008, p. 464.

[553] See Frédéric Pollaud-Dulian, « A propos de la sécurité juridique », RTDCiv. (3) juill.-sept. 2001, p. 487, ref. p. 489.

[554] Decision n° 2001-455 DC of 12 January 2002, J.O.R.F. of 18 Jan. 2002, p. 1 053, § 9; decision n° 2004-503 DC of 12 August 2004, J.O.R.F. of 17 August 2004, p. 14 648, § 29.

[555] For a definition of subject of law in international law, which has the same meaning into the French legal system as regards French law, see Collected courses of the Hague Academy of International Law, vol. 5, vol. 255, 1996, 464 p., page 51: "*the classical definition of a subject of the law is that it is an entity capable of possessing rights and duties under international law and having the capacity to maintain its rights by making international claims*".

[556] Decision n° 2004-503 of 12 August 2004, op cit, § 29.

Any blocking measure, at least within the framework of the ECHR, must therefore be provided for by a law responding to this definition. The possibility, at a national level, to make provisions for blocking in a text that would not be a text from the legislative authority will mainly result from the constitutional provisions. If the latter holds for instance that only the Parliament has the possibility to interfere with the rights for private life and to freedom of expression, or if the effect of the constitutional provisions is so, any blocking measure will have to be provided for by a text from the Parliament. France is an example of such a system.

Accordingly to article 34 of the French Constitution[557], the legislative authority cannot transfer its competence to determine the rules regarding freedoms to the administrative authority or to the judiciary[558]. That prohibits, for instance, every agreement that would provide for blocking between the ISP Industry and the French government, or any administrative decision in that sense.

Only one kind of agreement that would allow a blocking measure or something that can be more or less comparable[559] would be the contract between the Internet user and the ISP. This would be the case, on the one hand, if the user openly consents not to access some types of content, provided that he can make freely this choice which is not imposed to him[560] and, on the other hand, if the contract offers the possibility for the ISP to terminate the contract, if some 'non- abuse' rules of conduct (which aim to preserve the service that his offered to the consumer) are not respected by this user[561]. The legality of such a measure would depend very much on the type of content being accessed and the nature of the breach and the evidence needed. 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 (Council Directive 93/13/EC).

The French civil judge always remains competent to verify if such a blocking measure or such a contract termination was legitimate. This judge is also competent to pronounce a filtering measure under certain conditions, but this is because this possibility is already provided for in articles 808 and 809 of the Code of civil procedure[562] and article 6, I, 8 of the law n° 2004-575[563]. French ISPs can implement spam blocking measures, because of the general principle, confirmed in the French penal code[564] that allows a person to defend themselves or their goods (including ancillary services) against attacks. Moreover, quality of service levels are a

[557] Article 34 holds that only the legislative authority can "determine the rules concerning (…) civic rights and the fundamental guarantees granted to citizens for the exercise of their civil liberties (…)".
[558] Decision n° 2004-503 DC of 12 August 2004, J.O.R.F. of 17 August 2004, p. 14 648, § 29.
[559] We will notably evoke the termination of a contract, which is legally speaking not the same as a blocking measure.
[560] Such a blocking that could not be refused could be judged as a abusive contractual clause, as it would limit without legitimacy the freedom of expression of the user, and can limit the latter right to freedom of private life.
[561] See for instance T. Com. Paris, judgment of 5 May 2004, Microsoft Corp. et AOL France v. Monsieur K., available on the Juriscom.net website at this address: http://www.juriscom.net/jpt/visu.php?ID=510. See also below section 7.5.1.
[562] Article 808 holds: "In all cases of urgency, the president of the High Court may order in a summary procedure all measures that do not encounter any serious challenge or which the existence of the dispute justifies". Article 809 holds: "The president may always, even where confronted with a serious challenge, order in a summary procedure such protective measures or measures to restore (the parties) to (their) previous state as required, either to avoid an imminent damage or to abate a manifestly illegal nuisance"; "In cases where the existence of the obligation is not seriously challenged, he may award an interim payment to the creditor or order the mandatory performance of the obligation even where it is an obligation to do a particular thing".
[563] Law of 21 June 2004, JORF n°143 of 22 June 2004, page 11168. Article 6, I, 8 holds: "the judicial authority may order through summary orders or orders upon petition, to each (hosting provider) or, failing that, to each (access provider), all measures suitable to prevent a damage or to stop a damage caused by the content of a service of online communication to the public".
[564] French penal Code holds in its article 122-5, §2: "A person is not criminally liable if, to interrupt the commission of a felony or a misdemeanour against property, he performs an act of defence other than wilful murder, where the act is strictly necessary for the intended objective the means used are proportionate to the gravity of the offence".

legal obligation for Internet Service Providers[565] and this can be understood as justifying spam blocking.

[565] See for instance article L. 33-1 of the Code of Posts and electronic communications that holds, in its I, §4, that "the establishment and the exploitation of networks open to the public and the providing of electronic communications services are submitted to the respect of rules regarding (…) the conditions of permanence, quality and availability of the network and the service".

7.4 The principle of a legitimate aim

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

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. For instance, a country that is party to the ECHR shall not set up an Internet blocking measure that interferes with the right to private life if this measure is pursuing a different aim from the ones listed in article 8 of the ECHR.

Depending on the nature of the blocking measure adopted, one of the key issues can be to determine the pursued interest or aim of the measure. For an exhaustive overview of the debate on Internet blocking and to facilitate understanding of the characteristics of child pornography Internet blocking in comparison with other types of blocking, each main Internet blocking measure is analysed below. These measures are currently debated in some countries in the light of the legitimate aims listed by international texts.

7.4.1 Spam blocking and IPR preservation

The easiest activity to understand is spam blocking. Spam blocking's aims are clearly, on the one hand, the protection of the rights of the ISP to preserve the existence of its e-mail service, and, on the other hand, 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.

As regards an Internet blocking measure, applied on a P2P network or to the web, which would aim to block files or to prevent people from accessing files that constitute an IPR infringement, the intention would be to protect the rights of the rights owners. Such a measure, that would at least cause limitations on the freedom of expression[566] and potentially the right for private life[567] seems to be responding to the aim of protecting "*the (…) rights of others*", which is also a legitimate aim accordingly to article 8 and 10 of the ECHR, and 19 of the ICCPR. The wider context (proportionality in terms of cost, "collateral damage" to networks, over-blocking, etc) would also need to be assessed in such a case to determine legality in such circumstances.

If the aim of both of these blocking measures seems clear, it remains difficult to determine clearly the legitimate aims (as opposed to the subjective aims) of a blocking measure that would prevent people from accessing a website or a file if the "blocked" content was (easily and freely) available through via another protocol or via a circumvention mechanism (such as a proxy server).

[566] See section 6.6.2.2.
[567] See section 6.6.1.

7.4.2 The aim to protect the interest of the victim

One of the aims pursued by 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 (for example images of child abuse or images of racial hatred where the images of the victim are clearly visible). 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. However, not all abusive images of children include identifiable information. Indeed, if such identifiable information was readily available more successful investigations might result from deep analysis of these images.

However, it could also be argued that the interest of victims could also be vindicated in that same scenario, by facilitating complaints against the crime and encouraging investigations to find victims, perpetrators, producers and distributors.

It seems that such a debate cannot be concluded without a study that would take into account opinions of specialists, citizens and identified and rescued victims themselves, and analysis of the victim interest vis-à-vis people who would access images accidentally (and the proportion of such people), and vis-à-vis people who are searching to view such images. The result of such a study would allow a determination as to whether the protection of victims' interest could be used in justification of a blocking measure.

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

Another aim pursued by an Internet blocking measure targeting illegal content could be to prevent people from seeing illegal content, to protect morals or to protect the sensibilities of weaker members of society, which means also protecting those peoples' health. Both of these aims fit with the "*protection of health or morals"* interest, provided for by articles 8 and 10 of the ECHR and 10 of the ICCPR.

However, if the aim of protecting the sensibilities of weaker citizens can be seen as legitimate, the links with morals seems on the contrary to be very weak, especially in Europe, since people usually report illegal content, such as child pornography, for investigation, for the crimes that such images reflect, and not because morality could suffer because of it. According to the European Court of Human Rights, for which "*the scope of the domestic power of appreciation (of States) is not identical as regards each of the aims listed in Article 10*", the "*view taken by the Contracting States of the "requirements of morals" (…) varies from time to time and from place to place*", and "*State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements*".[568]

Therefore, the aim might be legitimate based on the country's concept of morality, in other words if the society considers that illegal content must be fought for the crimes they depict, or if it considers that people must be mainly protected from viewing such contents. Firstly, it seems that the protection of morals might not be validly invoked to justify a blocking measure. Secondly, while the protection of morals could appear as a legitimate aim, protecting people from accessing some defined content for morals purposes might not correspond to the democratic understanding of freedom to access information, at least in liberal democracies.[569]

---

[568] *Sunday Times v. The United Kingdom*, afore quoted, § 59, referring to the *Handyside v. The United Kingdom* case (application 5493/72, judgment of the 7 December 1976, Series A, n° 24).

[569] See for instance the joint declaration of the OSCE representative on freedom of the media and Reporters without borders on guaranteeing media freedom on the Internet, June 17-18, 2005, accessible at http://www.rsf.org/IMG/pdf/declaration_anglais.pdf: "*In a democratic and open society it is up to the citizens to decide what they whish to access and view on the Internet. Filtering or rating of online content by governments is unacceptable. Filters should only be installed by Internet users themselves. Any policy of filtering, be it at a national or local level, conflicts with the principle of free flow of information*"; the joint declaration by UN commission of human rights, OSCE and OAS, 21 December 2005, www.article19.org/pdfs/standards/three-mandates-dec-2005.pdf: "*Filtering systems which are not end-user controlled - whether imposed by a government or commercial service provider - are a form of prior-censorship and cannot be justified (...)*" ; Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, accessible at https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75: "*Recalling the Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003, which stresses that public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers, but that this does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries*" ; "*Users' awareness, understanding of and ability to effectively use Internet filters are key factors which enable them to fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information, and to participate actively in democratic processes. When confronted with filters, users must be informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering the content they access is subject to. Moreover, they should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies*".

7.4.4 The aim to prevent crime

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

- Firstly, some people propose that child pornography could cause some persons, who are not paedophiles, to develop such behaviour by regularly viewing illegal child pornography images Research in this area is at an underdeveloped stage.[570] Such a hypothesis and its extent urgently needs be demonstrated, within a study that would explain the "taking action" process and highlight the percentage of the 'at risk' population before crime prevention could be considered a legitimate aim under the ECHR or the ICCPR.

- Secondly, it is sometimes explained that Internet blocking attempts can disrupt commercial child pornography business and therefore prevent crime. Such an aim seems legitimate, since real business exploiting child pornography does exist. Another issue to consider here would be the real short- and long-term impact of Internet blocking on this business, which is discussed in section 7.5

  A study on the real impact of blocking on these businesses would be needed, to determine if such an aim as achievable (and sustainable) and therefore legitimate. Such a study would for instance show on the approximate proportion of business done via these websites that are or could be blocked. It should review ways in which these websites are accessible and the potential and impact of available circumvention methods. It should consider the other Internet protocols that are used to sell the materials and the potential transfer rate of content and clients, between the web and those other protocols, in case of web-blocking.

[570] See for instance Michael Seto, "Assessing the Risk of Sexual Offending Posed by Child Pornography Offenders", Centre for Addiction and Mental Health and University of Toronto, presentation at the 2nd International Symposium on online child exploitation, available at: http://www.innovationlaw.org/Assets/events/Symposium2007/Seto+Presentation.pdf.

7.4.5 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. It is also clear that Internet blocking can, almost always, be circumvented[571] and nor does it facilitate (indeed it does not aim to facilitate) investigations to find perpetrators or victims.

However, some countries could decide to block people to sanction a crime or an infringement, i.e. to impose the suspension, restriction or interruption of Internet access as a sanction. This sanction could also aim at crime prevention, avoiding a subsequent offence. In this case, Internet blocking would have a legitimate aim within the framework of the public order clause.

Such a sanction is what France attempted to implemented in the draft law called "Creative Works and the Internet", in response to IPR infringements. This draft law was blocked on this precise issue by the French Constitutional Council on 10 June 2009, which notably considered that disconnecting Internet access can only be decided by a judge, when the freedoms in opposition are on the first hand the freedom of expression and on the other hand an intangible property right, and must meet the requirements of the presumption of innocence, both conditions that the draft law did not respect. France now plans new draft legislation that aims to address these concerns.

A legitimate aim, pursued by a law that permits an Internet blocking measure, is however not sufficient for a limitation of a freedom to be considered legitimate under the relevant clause of the ECHR. The measure must also be *necessary in a democratic country*.

[571] See 5.6.2in "security and integrity", 4.7

7.5 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*",[572] corresponds to a "*pressing social need*"[573] and is "*proportionate to the legitimate aim pursued*".[574]

Some judges of the Court added that "*there can be no democratic society unless "pluralism, tolerance and broad-mindedness" find effective expression in the society's institutional system, and unless this system is subject to the rule of law, makes basic provision for an effective control of executive action to be exercised, without prejudice to parliamentary control, by an independent judiciary, and assures respect of the human person*".[575]

The principle of necessity implies therefore two elements: a pressing social need and proportionality between the interference and the legitimate aim pursued.

7.5.1 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"".*[576] The Court adds that the "*domestic margin of appreciation*" outlined by article 10 of the ECHR to the Contracting States goes "*hand in hand with a European supervision*" which "*covers not only the basic legislation but also the decision applying it, even one given by an independent court*".

An Internet blocking measure must therefore correspond to a real need of society, which also implies the effectiveness of the measure to allow that need to be satisfied. For example, spam blocking seems to meet such requirements, as it blocks a huge amount of spam every day thereby enabling the email service to stay usable and yet still responds to the Internet users' need in terms of freedom to correspond. A similar conclusion seems difficult to achieve with regard to other types of Internet blocking measures.

7.5.1.1 Protecting Intellectual Property Rights

It is difficult to categorically state that an Internet blocking measure, which would serve the interest of IPR owners, would correspond to a pressing social need.

In fact, society currently debates the business model of the music and the movie industry on the Internet, especially the low availability of online legal content, and the appropriate levels of artists' remuneration. Therefore, Internet blocking is perhaps not the most appropriate means to preserve intellectual property interests, which could only

---

[572] Joint dissenting opinion of judges Wiarda, Cremona, Thór Vilhjálmsson, Ryssdal, Ganshof van der Meersch, Sir Gerald Fitzmaurice, Bindschedler-Robert, Liesch and Matscher, §8, available under the court case *Sunday Times v. The United Kingdom*, application n° 6538/74, 26 April 1979, Series A, n° 30, § 45, available at: http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=freedom%20|%20expression&sessionid=27574169&skin=hudoc-en.

[573] Sunday Times v. The United Kingdom, op cit, § 59.

[574] *Sunday Times v. The United Kingdom*, op cit, § 63. See also Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, page 33, page 43; Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 86.

[575] Joint dissenting opinion of judges Wiarda and others available under the Sunday Times court case, afore quoted, § 8 of the opinion, referring to the following court-cases: *Handyside v. The United Kingdom*, application 5493/72, judgment of the 7 December 1976, Series A, n° 24, § 49; *Klass and others v. Germany*, judgment of 6 September 1978, Series A, n° 28, §49.

[576] Sunday Times v. The United Kingdom, op cit, § 59.

be ultimately determined by a specific study on each of these elements and the reaction and views from society.

Whatever will be the result of the business model debate, and even if Internet blocking for that purpose would be seen as a real actual need, there still remains the concern of the usefulness and effectiveness of the measure. Section 5.4.6 explained that a P2P blocking measure would likely lead, within a period of some months, to the encoding and encryption of P2P exchanges[577]. This would likely prevent any attempt of blocking or even monitoring of P2P contents. A web-blocking measure can be by-passed very easily, by the Internet user or the website owner. A P2P or a web-blocking measure seems therefore not adapted to fight against intellectual property rights (IPR) infringements, since it will not prevent people from exchanging files.

7.5.1.2 Morality and Protecting People from viewing child pornography

An Internet blocking measure that would prevent people from accessing illegal content on the web could have for its aim to protect morals or to protect the sensitivities of some people. In such cases, once the blocking measure only affected people that would only see those contents by accidental access, we could say that the measure could be effective, by protecting those people from viewing contents they do not want to see.

The existence of a pressing social need of a blocking measure for these purposes would moreover depend, firstly, on the volume of the population to protect - which means the percentage of the population that accidentally finds illegal content or content considered immoral by that society, and the efficiency of blocking to ensure their protection, and secondly on the percentage of the content that could hurt the concerned persons but that would not be blocked (by choice or because these contents are not illegal). Indeed, an Internet blocking measure that would block only certain kinds of shocking or immoral content, and not the most upsetting one, could be assessed as irrelevant to reach its aim.

Therefore, a study on all these issues would be necessary. It could highlight the size of the population needed to be protected (which implies the need to know the percentage of access attempts done by Internet robots or other devices), its characteristics, and the impact of the filtering measure on the blocked websites (to know if some of them reappear, to which extent and after what time period, and if the new websites present the same characteristics of accessibility). This study would also analyse the percentage of each type of content that are easily accessible on the Internet. The study could emphasise the main identified types of objectionable content (child pornography, murders, rapes, other kind of violence or tortures), but also deal with each content that could harm a specific population, for instance on the basis of the required filtering rules by users of end user filtering tools.

If such a study resulted in proving an Internet blocking measure was needed to protect morals, the reality of this need for society would also depend on the concept of morality in the concerned country. The definition of "morals" vary from country to country, and an Internet blocking measure which aims to protect morality could be legitimate if the

[577] See also Jean Cedras, "le téléchargement illicite d'oeuvres protégées par le droit d'auteur » (illicit download of creations protected by copyright) », Rapport à Monsieur le Ministre de la Culture et de la communication (report to Mr. the Minister of Culture and communication), April 2007, available at: *www.odebi.org/docs/RapportCedras.pdf or* http://www.laquadrature.net/files/rapport_cedras.pdf, page 19 (translated from French): "*These softwares as Kaméléon, Mute or Share are equipped with a encryption system very elaborated, because of which blocking and users identification are practically impossible. Of course, even if the communication is encrypted, we can always now which are the IP addresses or the sender and of the receiver. But to materialise the infringement, on the opposite, we have to be able to analyse the flow, and therefore "break" the encryption, which is arduous. Better is therefore to directly go to carry out a search into the hard drive of the user, before having reached a high presumption of the existence of a criminal behaviour, which is problematic as regards personal freedoms*" ; see also http://www.technewsworld.com/story/34052.html?wlc=1250777621.

society considers that morality includes primarily the need to protect persons from viewing illegal images, and less the need to stimulate and mobilise people to report and fight against the crimes that such contents are promoting. As the notion of morality should be determined by the majority of the citizens in a democratic country, the content of this notion of morality should also correspond to a social need. Therefore, the requirement of a pressing social need will mainly depend on the way a society assesses child pornography i.e. if the society is in a position of "defence" or "attack" vis-à-vis this crime.

7.5.1.3 Protection of victims

An Internet blocking measure can aim to protect the image of victims of crimes such as child pornography or racial hatred. Such an aim could however be challenged[578] by people who could argue that the first interest of victims could be to acknowledge the crime they have suffered and to enable investigations demands from citizens.

Section 7.4.2 identified the necessity to conduct a study to conclude this debate. If such a study can confirm that the main interest of victims would be to not be seen (at least by paedophiles) Internet blocking could then be considered as a possible answer to a pressing social need. In this context, it is interesting to note the existence of a victims group called "Missbrauchsopfer gegen Internetsperren" (Abuse Victims Against Internet Blocking) that actively campaigns against blocking in Germany

However, Internet blocking can only adequately answer this need if it is capable of effectively hiding victims' images from those persons who would have been identified as causing damage to victims' interests by accessing their image, from those other persons who are searching for such images and those persons who would accidentally find them. It could lead to the necessity to preserve victims' images from all of these categories. A study on the capability of blocking to reach that aim would therefore also be required.

7.5.1.4 Prevention of Crime

An Internet blocking measure can aim to prevent crime, by preventing people from becoming paedophiles (which might be a reasoned argument only ~~a~~after an appropriate study as outlined in section 7.4.4 or by disrupting the child pornography business model for commercial child pornography or by preventing exchanges of child pornography.

Preventing Persons from becoming Paedophiles
The usefulness of Internet blocking however implies, firstly, to be certain that blocking would effectively lead, for example, to preventing the population assessed from becoming paedophiles as a result of viewing child pornography, from viewing child pornography. On that issue, the study required for section 7.4.4 should also identify the several Internet protocols used by the population to prevent from becoming paedophile to access child pornography, and their expected behaviour in case of blocking. Another subject of research could be the issue to verify whether people who become paedophiles by viewing some kind of images would never have became so if the images had not been seen. Such a study could show on if blocking would effectively prevent some people from becoming paedophiles either by bypassing filters or using a non blocked communication protocol, or despite the reduced access to illegal images.

Disrupting Child Pornography Business Model
As regards the aim of disrupting the child pornography business model for commercial child pornography, the usefulness of blocking should also not be accepted before a relevant study is completed. This study should for instance show the approximate proportion of business done via websites that are or could be blocked. It should review

[578] See section 6.3.3.2.

in which ways these websites are accessible and the durable impact of these ways on an Internet blocking measure in terms, for instance, of bypassing the measure. It should consider the other Internet protocols that are used to sell materials and the potential transfer rate of content and clients, between the web and those other protocols, in case of web-blocking.

Preventing Exchanges of Child Pornography
As regards the aim of preventing the exchange of child pornography, the usefulness of the measure and its response to a pressing social need would imply a study is completed demonstrating that blocking would effectively lead to a proportionately worthwhile prevention of such exchanges. This study could examine the approximate proportion of child pornography accessed through the protocol that is planned to be the subject of the blocking attempt, as regards the approximate proportion of materials distributed by criminal through other protocols. This would produce results on the impact of such a blocking attempt on the behaviour of people who distribute and access child pornography through the blocked protocol to know the potential transfer rate of content and consumers of such content, between the blocked protocol and other ones.

If these studies can demonstrate that blocking can reach its pursued aim at least to a sufficiently significant extent that would meet the needs of the proportionality assessment we would be able to confirm the usefulness of the measure and its response to a real social need,

7.5.1.5 Repression of Crime

A last issue is however the blocking of a person's Internet access to prevent or repress an offence or a crime, as France is planning to do through the draft law called "penal protection of literary and artistic property on the Internet", brought in before the Senate on 24 June 2009, following the rejection by the Constitutional Council of a similar mechanism that was contained in the previous "Creative Works and the Internet" draft law. The usefulness of such a measure can not really be challenged, as the internet user would no longer be able to access to the Internet from his home at least not via an internet connection registered in his own name. It would then be more difficult for the sanctioned user to commit a further offence.

The question is therefore if such a measure responds to a pressing social need. The answer is difficult to give, as it will depend on the importance that society places on the Internet, not just as a leisure or academic tool, but also as a means of interaction of the citizen with the state (see http://www.service-public.fr/, for example). In Europe, this place is substantial as some entities and authors seem to consider Internet access as an independent fundamental right.[579] At a minimum, Internet access is accepted as a means of exercising two fundamental freedoms - the right of private life and the right to freedom of expression.[580] Therefore, if the prevention and repression of crime is a social need, the interruption of an internet access can only be analysed as a social need if this interruption is proportionate to the actions that have to be prevented or punished. This would be a question of circumstances.

Two early reviews were already given on this issue, at the French level.

- Disconnection due to spamming
  The first analysis was given by the French judge at the occasion of an interruption of a user's access contract following the sending of spam was on the basis of the contractual law. Even if such a disconnection is not a blocking measure and is related to civil law and not penal law, it is still interesting to analyse as it gives an example of the assessment of proportionality between the acts and the "sanction".

[579] See section 6.6.2
[580] See sections 6.3.1.2 and 6.3.2.2.

On 5 May 2004, the French judge considered that an ISP had the right to terminate the contract of a spammer for the violation of the contractual provisions, recognising that the prohibition of spamming was included in the contract and also that the ISP suffered damages because of spam, in terms of reputation and resources involved in the fight again spam.[581] Previously, on 15 January 2002, the County Court of Paris considered that an ISP could terminate an internet access contract for spamming, because the user, by using "*the technique of spam in a manifest and repetitive manner*", had "*gravely disrupted the network equilibrium, causing numerous reactions from displeased Internet users whose email services were overloaded and who had to delete the unsolicited messages while suffering the costs and the inconvenience of such activities*" .[582]

- Disconnection due to IPR violation
  The second analysis was the initiative of the French Constitutional Council. In its decision of the 10 June 2009, the Council considered that, in a field where the rights of the "*holders of* copyright *and related rights*" and the "*right of any person to exercise his right to express himself and communicate freely, in particular from his own home*", are in opposition, a court of law is the only one institution that can receive the power to give a verdict on the legitimacy of restricting or denying access to the Internet.[583] As we can see, this decision did not really discuss the disconnection measure in the light of the specific offence that would have led to this sanction, as the Council considered any offences to rights owners as a whole. This decision is therefore also related to the debate on the proportionality between the interference and the legitimate aim pursued, which is the last requirement of the public order clause.

7.5.2 Proportionate to the legitimate aim pursued

Interference 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 (or the ICCPR) and to respond to a "pressing social need".

7.5.2.1 The proportionality criteria

The principle of proportionality is "*recognised as one of the central principles governing the application of the rights and freedoms"* contained within the European Convention on Human Rights and its additional Protocols.[584] Allowing "*some evaluation of how much of a contribution a particular restriction can make towards securing a given objective*",[585] the principle of proportionality responds to the need "*for balancing entailed when giving effect to the rights*" that are concerned by the public order clause since, without it, "*the formulation to the*

[581] T. Com. Paris, judgment of 5 May 2004, Microsoft Corp. et AOL France v. Monsieur K., available on the Juriscom.net website at this address: http://www.juriscom.net/jpt/visu.php?ID=510

[582] TGI Paris, ref., 15 January 2002, Monsieur P. V. v. Société Liberty Surf et Société Free, available at this address : http://www.juriscom.net/txt/jurisfr/cti/tgiparis20020115.htm.

[583] See Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 16, decision available in English at this address: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf: "*The powers to impose penalties created by the challenged provisions vest the Committee for the protection of copyright, which is not a court of law, with the power to restrict or deny access to the internet by access holders and those persons whom the latter allow to access the internet. The powers vested in this administrative authority are not limited to a specific category of persons but extend to the entire population. The powers of this Committee may thus lead to restricting the right of any person to exercise his right to express himself and communicate freely, in particular from his own home. In these conditions, in view of the freedom guaranteed by Article 11 of the Declaration of 1789, Parliament was not at liberty, irrespective of the guarantees accompanying the imposition of penalties, to vest an administrative authority with such powers for the purpose of protecting holders of copyright and related rights*".

[584] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et seq., quotation p. 23.

[585] Jeremy McBride, op cit, p. 24.

Convention provisions would be open to restrictions depriving the rights and freedoms of all content so long as they were prescribed by law and for a legitimate purpose"[586], in addition to responding to a pressing social need.

A number of factors "*in determining where the balance lies in particular cases*" has been highlighted by Jeremy Mc Bride[587] through the judgements of European Human Rights institutions.

One of these factors is "*the overall effect of a particular restriction*".[588] For instance, "*political activities of local authority officer*" can be subjected to restrictions "*where their visibility meant that they were likely to be linked with a particular party line in the eyes of the public (…) since the officers were still free to join a party and engage in some political activities*".[589] On the other hand, it "*was found to be unacceptable*" to prevent "*the applicant making certain statements about the dangers of microwave ovens*", because "*it affected the very substance of his views; it effectively prevented him making his contribution to the public debate*"[590].

Another factor used by the European Court of Human Rights is to know "*whether there was a sufficient basis for believing that a particular interest was in peril*". For instance, in the case previously quoted, "*there was no evidence that the sale of microwave ovens had been affected by the applicant's remarks*".[591]

Moreover, such an assessment can lead the European Court of Human Rights to assess "*the proportionality of the very behaviour which is being restricted*". For instance, the Court considered that the "*remarks made by journalists about the conduct of views of judges and politicians when considering whether they had sufficient factual basis to fall within the protection extended to the expression of value judgments under Article 10*".[592].

Further, the Court verifies if the interference's aim "*can be satisfactorily addressed in some other, less restrictive way*".[593] For instance, "*an order requiring a journalist to disclose his source for a leak about the financial affairs of a company was considered to be unjustified (…) insofar as the objective was to prevent dissemination of confidential information since this legitimate concern was already being secured by an injunction restraining publication of the information that had been disclosed*".[594]

McBride analyses also, within the decisions of the European Court of Justice, a "*variable approach*"[595] of what he calls the "*proportionality test*",[596] depending on the freedoms that are suffering an interference. He sees this variable approach as "*particularly evident in the assessment of restrictions on freedom of expression*",[597] which must be strongly justified to

[586] Jeremy McBride, op cit, p. 24.
[587] Jeremy McBride, op cit, p. 24 *et seq*.
[588] Jeremy McBride, op cit, p. 24.
[589] Jeremy McBride, op cit, p. 25, referring to *Ahmed and Others v. The United Kingdom*, judgment of the Court, 2 September 1998.
[590] Jeremy McBride, op cit, p. 25, referring to the court case *Hertel v. Switzerland*, judgment of the Court, 25 August 1998.
[591] Jeremy McBride, op cit, p. 25. In the same sense, the "Article 29 Group" was noticing "that representatives of the law enforcement community have failed to provide any evidence as to the need for such far reaching measures", in its opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism", adopted on 9 November 2004, WP99, quotation page 4, available at the following address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf.
[592] Jeremy McBride, op cit, pp. 24 and 25, referring to *De Haes and Gijsels* v. Belgium, judgment of the Court, 24 Feb. 1997, and *Oberschlick v. Austria* (n°2), judgment of the Court, 1 July 1997.
[593] Jeremy McBride, op cit, p. 26.
[594] Jeremy McBride, op cit, p. 26, referring to *Goodwin v. United Kingdom*, judgment of the Court, 27 Mar. 1996.
[595] Jeremy McBride, op cit, pages 28 *and seq*.
[596] Jeremy McBride, op cit, p. 29.
[597] Jeremy McBride, op cit, p. 30.

prevail, "*the burden of justification (falling) very much on the defendant State*".[598] An example is the "*considerable readiness to accept that there is a justification for the belief that morals are being endangered*".[599]

[598] Jeremy McBride, op cit, p. 30.
[599] Jeremy McBride, op cit, p. 30.

7.6 Internet blocking and proportionality criteria

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

7.6.1 Spam blocking

Spam blocking aims to preserve the existence and quality of the ISP service and to preserve the user's freedom of private life and achieves such aims to a reasonable extent.. Therefore it can be said that the overall effect of the measure is proportionate as long as it effectively preserves the possibility to use email boxes and the SMTP protocol, while the blocked sender still have the possibility to reach the team of the ISP to solve their sending problem and send their emails again, and while the user chooses to use or not use the filters that will deliver suspected spam into a spam mailbox.

Spam blocking is moreover based on the real peril that endangers email services, while the behaviour which is restricted is the right to send email without respecting rules set up by ISPs to avoid too much 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.

7.6.2 P2P or web blocking in the interest of the IPR industry

A web or P2P blocking measure that would serve the interest of the intellectual property 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 (for instance within the framework of investigations aimed at bringing criminals before a court, or on statistical purposes without retaining personal data).
- Secondly, it would imply high costs for the ISP industry,[600] the government[601] and the Internet users.[602]
- Thirdly, it will lead to the blocking of legal files (since technical recognition currently remains imperfect) which will restrain the freedom of communication and the freedom of privacy in a larger extent than the one needed to protect the rights owners' interests.[603] Web blocking for the same purpose would lead to the same conclusion, except the fact that encryption is only possible on the https protocol, not http, and therefore the costs for ISPs and government should be lower.

Regarding the criterion requiring that there be "*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 imprecise. Such studies do not take into account, for instance, how many persons who accessed to an illegal IPR resource would have paid to own it were it not available illegally online, nor the issue of the potential sale of derived products (concert tickets, merchandising, etc) that could be generated as a result of access to an illegal resource. Such a study has been already initiated and would be highly necessary in this debate.[604]

---

[600] The cost, for the ISP industry, of implementing a mechanism allowing blocking users without shutting down the phone and TV when it is feasible was estimated at « *70 million of euros at least for the period 2009-2012* »: Jean Berbinau, Jean-Claude Gorichon, Dominique Varenne, « Création et Internet », rapport n° IV-3.3-2008 – Décembre 2008, report available at this address: http://www.lesechos.fr/medias/2009/0304/300333937.pdf.

[601] In countries where the costs of measures set up in the general interest have to be taken in charge by the government, like in France (see for instance the Constitutional Council's decision n° 2000-441 DC of 28 December 2000. This principle has also been declared in several French legal provisions).

[602] Where the cost of his internet access could increase, and will in any cases suffer increased network latencies and breakdowns.

[603] As regards the non-relevance of P2P blocking, see for instance Philippe Astor, « Filtrage du P2P : les tests du SNEP font un flop », 8 April 2008, Electron Libre, http://electronlibre.info/Filtrage-du-P2P-les-tests-du-SNEP,060; Damien Bancal, « Filtrage du trafic P2P : le grand bide », 10 April 2008, Zataz.com, http://www.zataz.com/news/16894/Filtrage-du-trafic-P2P;-le-grande-bide.html; A.Brugidou et G. Kahn, « Etude des solutions de filtrage des échanges de musique sur Internet dans le domaine du peer-to-peer, rapport d'étude, 9 mars 2005, http://ww.culture.gouv.fr/culture/actualites/rapports/filtrage/charte.pdf; Guillaume Champeau, « Hadopi SE2E04 : faites entrer les juristes », 5 May 2009, Numerama, http://www.numerama.com/magazine/12826-Hadopi-SE2E04-faites-entrer-les-juristes.html. As regards the issue of web filtering, see also Marc Rees, « Free ne veut pas entendre parler de filtrage et explique pourquoi », 5 November 2008, PC Inpact, http://www.pcinpact.com/actu/news/47097-free-filtrage-forum-droits-internet.htm.

[604] See for instance an Ipsos Germany study concluding that "the possibility of illegal downloads is for some people an introduction to (acquiring a taste for) music": Pyrolyse Bred, « The chinese, champions of illegal music downloads », 24 September 2009, http://pyrolysebred.baywords.com/index.php/2009/09/24/the-chinese-champions-of-illegal-music-downloads/; "Weltweit laden 44 Prozent der Internet-User illegal Musik aus dem Internet Piraten sind gleichzeitig größte legale Konsumenten – auch in Deutschland", press release, 18 Sept. 2009, http://knowledgecenter.ipsos.de/docdetail.aspx?c=1043&sid=67F6B1C4-CC4A-4636-A948-1860CB7A00B1&did=2df20c44-f4c4-4e37-a746-e785070a02da and Nil Sanyas, "Quel est le reel champion du piratage : enfin la réponse!", PC Inpact, 21 Sept. 2009, http://www.pcinpact.com/actu/news/53141-reel-champion-piratage-reponse-ipsos.htm; see also the French data protection Authority's deliberation n° 2008-101 of 29 April 2008, avis n°08008030, giving the Authority's opinion on the French draft law called « creation and Internet », available at this address: http://www.laquadrature.net/wiki/HADOPI_avis_CNIL, or within the report of the "Quadrature du Net", « Hadopi, "riposte graduée" : une réponse inefficace, inapplicable et dangereuse à un faux problème », 9 February 2009, available at this address: http://www.laquadrature.net/files/LaQuadratureduNet-Riposte-Graduee_reponse-inefficace-inapplicable-

An Internet blocking measure in the interest of the music and movie sector whose intent is to prevent persons from exchanging protected music or video files without the consent of the rights owners can be seen as proportionate under the third criterion we retained for assessing proportionality, since such an exchange is not acceptable nor proportionate behaviour. However, this conclusion on proportionality has to be considered relative to other impacts such a measure can have. The measure can be susceptible to additionally prevent the same persons from access files that are legitimate and are protected by the freedom of expression or the right for private life.

Finally it seems that the protection of IPR can be addressed "*in some other, less restrictive way*". For instance, the IPR industry is allowed, in France, to collect data related to infringements to their rights, especially on the P2P network, in the aim of bringing the cases before a court.[605]

dangereuse-a-un-faux-probleme.pdf, p. 23. In this opinion, the French Data Protection Authority "*notices that the only arguments evoked by the government in order to justify the creation of the mechanism confided to the HADOPI* (i.e. the administrative authority that was in charge of the user's sanction within the framework of the French "creation and Internet" draft law) *are the result of the noticing of a decrease of the cultural industries' turnover. In this respect, (the authority) deplores that the draft law is not accompanied by a study that clearly demonstrates that files exchanges through P2P networks are the determining factor of a sale decrease, in a sector that, furthermore, is in complete transformation, notably because of the development of new distribution modes of the spirit works at the numerical format".* (Introductory observations). See also Jean Cedras, « le téléchargement illicite d'oeuvres protégées par le droit d'auteur », Rapport à Monsieur le Ministre de la Culture et de la communication (« illicit download of creations protected by copyright », report to the French Minister of Culture and communication), April 2007, available at : *www.odebi.org/docs/RapportCedras.pdf or* http://www.laquadrature.net/files/rapport_cedras.pdf, n° 6, pages 9 and 10.

[605] See article 9, 4 of the law n° 78-17 of 6 January 1978. See also for instance the Constitutional Council Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, §§ 25-27, decision available in English at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf.

7.6.3 Web or P2P blocking of illegal content …

7.6.3.1 … in the aim of protecting the victim's image

A web or P2P blocking measure set up in the aim of protecting the victim's image aims to prevent people from seeing the image of the victim suffering the crime. This effect seems proportionate, on the condition that the public interest would not be more appropriately served by more direct knowledge of the existence of such crimes, which is also a right protected by Article 10 of the ECHR.[606] However, this proportionality seems acceptable 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 since a child pornography image, for instance, can also display a crime scene without permitting recognition of the victim,[607] for example in cases where the victims face or other identifiable information is not present. Proportionality would also have to be assessed on the basis of the effectiveness of the blocking efforts and risk of circumvention.

As regards the "*basis for believing that"* the victims interest are "*in peril*", the victims interests[608] might also be vindicated 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. This is the position adopted by the German association of victims against internet blocking, which argues, for example, that action against illegal websites is a far bigger priority than blocking, particularly as blocking risks reducing the public perception of the problem.[609]This issue requires further debate taking guidance from the European Court of Human Rights.

As regards the "*proportionality of the very behaviour which is being restricted*" criterion, the blocking measure aims to prevent people from seeing the victims of a crime. The proportionality of this behaviour can be analysed in the light of the interest of the public of identifying such a 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
- the desire to not view such images

The proportionality of these behaviours is therefore relative, as long as the blocking measure is not preventing people from seeing legal contents, which would limit the very proportionate behaviour to receive information, protected by the right to freedom of expression.

Finally, as regards the issue to know if the blocking aim can be "*satisfactorily addressed in some other, less restrictive, way*", it seems to totally depend on the international cooperation and other countries' willingness to preserve the victim interests, since the crime and the victim are no longer visible if and when the content is removed from the hosting provider's server.

7.6.3.2 … in the aim of protecting morals, or in the aim of protecting the interests of sensitive people

A web or P2P blocking measure in the aim of protecting morality or in the interest of protecting sensitive people will first have as a general effect to prevent people from

---

[606] See above section 6.3.2.2.
[607] Beside the fact that the victim could not be recognisable, French law criminalise for instance child pornography even when the crime is not real but drawn.
[608] See section 6.3.3.2.
[609] See http://mogis.wordpress.com/ (last visited 4 September, 2009)

accidentally accessing allegedly immoral or shocking material such as child pornography. Such a 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 a result, the general effect could be a depreciation of the right to freedom of expression, while criminals would still access to immoral or shocking contents. It seems that such a situation would not be very proportionate.

As regards the "*proportionality of the very behaviour which is being restricted*", the blocking measure aims here to prevent people from seeing contents that are either contrary to the notion of morality in their country, or dangerous for their sensitivity. The first of these approaches seems not to be proportionate, notably as we have seen that the European Court considers "*that morals must be accorded whatever protection a States considers appropriate*"[610], under the reservation that protecting people from accessing some defined content for morals purposes might not correspond to the democratic conception of freedom to access information, at least in liberal democracies[611]. Regarding the second issue, the issue of proportionality does not have a real meaning, as people are requesting to be prevented from their freedom to see some contents that can hurt their sensitivity. However, the blocking measure will also prevent non sensitive people from accessing the same contents. As regards, the exclusive aim to protect sensitivity, the measure seems not, in that case, being proportionate. Any proportionality test would also need to assess the statistical likelihood of accidental access to such material.

As regards the issue to know if the interest of morality is in peril by access to pre-determined illegal content, we can consider that this true, as long as the country's notion of morality prohibits such specific contents. The mental health of sensitive persons can be endangered by the existence of content that can hurt them.

Finally, as regards the issue to know if the protection of morals "*can be satisfactorily addressed in some other, less restrictive, way",* we could say that some alternative measures as end-user based filters would be more relevant.

- Firstly, we have shown that people who want to access immoral or illegal contents can always by-pass web-filters, as long as the content is still online, and that P2P blocking would lead to the encryption of P2P communications, preventing therefore any blocking attempt save at the origin or the end of the communication, i.e. on the end-user's machine.
- Secondly, sensitive persons that should be protected from disturbing content are certainly not hurt on the same way when viewing similar content, and should on the other hand be protected against disturbing content, even content that is only harmful but not illegal. The issue of what is disturbing to individuals is very subjective and much legal content could be considered disturbing and harmful by individuals whose sensibilities do not lead to direct government intervention.

The same conclusion has to be reached as regards protection of children's health and children's education, which would reasonably seem to require the ability for children's to have access to useful information for their development and education towards a responsible life,[612] while parents are entitled to give them the education they believe is the best.[613] The protection of both of these categories of people seems to require end-user tools only, which allow a total individualisation of the protection while being less restrictive in terms of preservation of freedoms, since the filter will apply to the concerned person only.

[610] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et seq., quotation p. 30. See above, in our section "the proportionality criteria".
[611] See above, 6.3.2
[612] See section 6.6.2.2.
[613] See section 6.6.2.2.

7.6.3.3 … in the aim of crime prevention

A web or P2P blocking measure in the aim of crime prevention should aim to prevent people from committing or supporting crime by buying, downloading or selling illegal content (or after having accessed illegal content if it is the case that people become paedophiles as a result of viewing images). However, currently, it is not really possible to know if such an aim would be reached by a blocking measure since no study gives the evidence of such an expected effect.[614] If a study would give this evidence, this effect of blocking could then be seen as *legitimate*, if it is the case that blocking would be effective enough to deter such people from accessing the illegal images via other protocols or via circumvention measures.

However, its *proportionality* would depend on the percentage of the population who would cease to commit crime after being prevented access to illegal content balanced against the restrictions on civil liberties that would be caused by the blocking measure. If this percentage were low the limitation of others' freedoms, in other words the general effect of the measure on other freedoms, would have to be low, in order for the measure to be considered proportionate. This can be the case if it can be demonstrated that a large number of criminals (who already represent just a small fraction of the whole population) would continue to commit this crime. This might be because they bypassed the blocking measure or because they would commit this crime regardless of the blocking measure,

This general effect of the measure could not, for instance, be a significant reduction of the freedom of expression or the freedom of private life of every citizen, by the blocking of legal files or legal web pages that are the subject of the exercise or the mean to exercise one of these freedoms, or by an increase of the cost to access the Internet or a decrease of the general quality of the Internet access, because of the expensiveness of the technical measures to implement to ensure the non blocking of legal contents.

As regards the *peril suffered* by the crime prevention, we can say that it is real. There is unfortunately no evidence that a blocking measure would lead to reduce this crime, while it could at the same time restrict some legitimate and proportionate behaviour.

The behaviour which is being restricted is that of contributing to crime by accessing illegal content. However, the reporting illegal contents and demands for the government to give more resources to fight against crime would also be restricted, as well as the people's right to know the remaining level of existence of illegal content on the Internet especially if the government does not accompany the blocking measure by a regular update of the reality of the situation. Moreover, as soon as the blocking measure leads to block legal content, the behaviour that is being restricted is the right to access legal information, which is protected by the freedom of expression.

Finally, as regards the issue of knowing if crime prevention could be satisfactorily *addressed in some other less restrictive way,* it appears that some investigation tools do already exist that empower investigators to track down on the one hand criminal authors and their victims and on the other hand people regularly accessing child pornography. These tools and systems could be further perfected, and their development in the respect of rights and freedoms would seem more relevant to pursue the crime prevention aim than a blocking measure.

There are also initiatives such as the "European Financial Coalition (EFC) to fight child abuse images distribution on the Internet", which the EU Commission has financially supported, and which seems, in principle, to be a good means to contribute towards the disruption of the commercial child pornography business.[615] It would also be beneficial if state reports to the

[614] See above, section 6.3.3.2.

[615] See "The EU Commission will finance the European Financial Coalition (EFC) to fight child abuse images distribution on the Internet", press release, 3 March 2009, available at this address: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/342&format=HTML&aged=0&language=EN&guiLanguage=en.

UN Child Rights Secretariat contained, as a standard section, details of efforts made by the reporting state undertaken in compliance with Article 34 of the Convention. Similarly, NGOs should also always include an appraisal of compliance with Article 34 in their shadow reports. Increased public focus on the efforts for and barriers to international cooperation to have child abuse material taken offline at source appears likely to produce positive results.

7.6.4 Blocking a person in the aim of crime repression and prevention

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 from accessing telephone and TV services.[616] Such an effect is really severe as it completely deprives a person of his or her freedom of receiving and communicating electronic information and of his or her freedom to exercise his or her private and family life, and his or her freedom to correspond, on the electronic world.[617] Therefore, such a sanction is really severe, and can only be proportionate if it is justified as regards the crime that was committed and the aim pursued through its repression, indeed even its prevention.

As regards *the peril suffered* by the crime repression or prevention, we can say, like in the previous sub section, that such a peril is real. And it is clear that a blocking measure taken against a person would lead to reduce this peril, since it will be more difficult for the user to commit an offence by using the Internet.

As regards the behaviour which is being restricted, it is simply and entirely a right to access the Internet, which is "*a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society*"[618] protected by the right to freedom of expression, even when it is not currently considered as a fundamental right in itself.[619]

However, this useful and self-development behaviour is not compatible with an intention to access the Internet in order to commit an offence or a crime. It would be more proportionate in response to these offences and crimes to pursue another aim other than blocking complete Internet access.

Finally, as regards the issue to know if the repression and the prevention of crime could be satisfactorily *addressed in some other less restrictive ways*, the answer will certainly depend on the crime in question, since we know that society has already developed a whole range of sanctions against crimes and other misdemeanours.

[616] Triple play offers allow accessing Internet, phone and television. An interruption of the offer, without distinction between services, would lead to interrupt all these services at the same time.
[617] See sections 6.6.1 and 6.6.2.
[618] European Parliament resolution of 10 April 2008 on cultural industries in Europe, 2007/2153(INI), § 23, accessible at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN. See above section 6.3.2.2.
[619] See above section 6.3.2.2.

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

The basic consequences that an Internet blocking measure can present in terms of interference with freedoms have already been highlighted. However, other 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. Indeed it even facilitates the reporting to the authorities of a message that contains some keywords or images that indicate a presumption of illegality, or of the user who sent or received such a content[620].

A web or a P2P blocking measure could also allow the service provider or the entity that operates the blocking mechanism to retain data related to the content of the communications sent, received or accessed, with or without data enabling the identification of the sender, the receiver or the web-user. The scanning of P2P files could also allow, similar to our example related to spam blocking, the reporting of potentially illegal content to the authorities, with or without the identification data related to the user.

Those initiatives would cause further disproportionate interference in the right of private life or in the right to the freedom of expression.

The proportionality of each measure which interferes with some freedoms has indeed 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 latter[621].

- The proportionality of a spam blocking measure will be generally assessed within the framework of a pursued aim which is the protection of the user's freedom to correspond and the ISP's right to defend its own service against threats.
- The proportionality of an IPR infringement blocking measure will be generally assessed within the framework of the pursued aim of protecting IPR owners' interests.
- The proportionality of a child pornography blocking measure could be only assessed in the aim of protecting morals, children's rights or the sensibilities of individuals.

In all these cases, the implemented measure cannot permit an aim to be pursued other than the one within which the blocking measure has been assessed and authorised. Therefore, a spam blocking measure or an IPR infringement blocking measure can not be used, for instance, to detect crime[622].

As regards Internet blocking measures that would be implemented with the aim of crime repression or prevention, their proportionality would have to be assessed as regards the general effect produced by their technical characteristics, which should be limited to what is strictly necessary to reach the pressing social need that motivated them. For instance, child pornography blocking that would be implemented in the aim of preventing some people from becoming paedophiles and disrupt the commercial business of child pornography could not lead to monitoring some people's internet access, unless such a monitoring also corresponds to a pressing social need in the aim to fight crime, taken into account at the occasion of the assessment of proportionality.

---

[620] Ref 5.4.3

[621] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et seq., quotation p. 24.

[622] The finality of the interference is also a criterion of the legitimacy of interferences in the right to protection of personal data: see Directive 95/46/EC.

In any case, the general effect of this kind of measure cannot directly lead to deprive a freedom. However, monitoring each communication to retain personal data in relation to a content seen, sent or received, or to report each crime or a type of crime to the authorities, extinguishes the right to the confidentiality of private life and disrupts the right to freedom of private life[623]. The non-proportionality of such a restriction was unequivocally declared by the European Court of Human Rights in its *Klass* judgment: "*As concerns the fixing of the conditions under which (a) system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion (…). Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate*"[624]. A similar statement was also made by European Court of Justice Advocate General Kokott in relation to case C-275/06 (the "Promusicae" case) where she stated in paragraph 82 that "there is reason to doubt, whether the storing of personal data of all users – quasi on stock – is compatible with fundamental rights, in particular as this is done without any concrete suspicion."

Such non-proportionality was also criticised by the Article 29 Data Protection Working Group, in its "opinion on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism": "*the routine, comprehensive storage of all traffic data, user and participant data proposed in the draft decision would make surveillance that is authorised in exceptional circumstances the rule. This would clearly be disproportionate. The draft framework would apply, not only to some people who would be monitored in application with specific laws, but to all natural persons who use electronic communications. Additionally all the communications sent or received would be covered. Not everything that might prove to be useful for law enforcement is desirable or can be considered as a necessary measure in a democratic society, particularly if this leads to the systematic recording of all electronic communications. The framework decision has not provided any persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combating crime or protecting national security*".[625]

In conclusion, each time an Internet blocking measure is allowed some guarantees must be undertaken to prevent this blocking measure from being used in a way that would further endanger freedoms. This is the case even if the measure pursues a legitimate aim and its basic function does not block other freedoms in a disproportionate way, The measure can still present one of the risks outlined in 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 essential to the functioning of the blocking mechanism.

Moreover, a judge must be allowed each time to assess the proportionality of each a specific blocking measure on each occasion.

---

[623] This right needs to be exercise in privacy to be real. See section 6.6.1.

[624] *Klass and others v. Germany*, application n° 5029/71, judgment of 6 September 1978, Series A, n° 28, § 49, accessible at: http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=klass&sessionid=27675613&skin=hudoc-en.

[625] Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism", adopted on 9 November 2004, WP99, quotation page 4, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf, p. 4.

7.8 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 the national judges. The national courts are also entitled to make a judgment on complaint regarding 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.

Therefore, each blocking measure put in place on the initiative of an ISP can be challenged before a court - at least in ECHR party countries.

However, if having the right to challenge before a court a decision that limited one's freedoms is a fundamental right[626], it supposes that this limitation has already been put in place and that the citizen had already to suffer from its effects. For this reason, in some situations it remains important 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.

7.8.1 The assessment and declaration of the illegality

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[627], only a judge should have the competence to declare a piece of content, a situation or an action as illegal. This exclusive power, provided for by the domestic legal system, implies that this piece of content, this situation or this action has to be qualified as "potentially" illegal until a judge has been enabled to give a decision on that illegality issue.

With regards to illegal contents to be blocked, another approach which would allow a government or indeed even a private entity to decide what is or not illegal and therefore what people have the right to see or not see would be unacceptable in a democratic country[628], except when internet users can control the filter put in place[629].

---

[626] Article 6 of the ECHR; Article 14 of the ICCPR.

[627] Larry Diamond, "Defining and Developing Democracy", in Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, the democracy sourcebook, p. 35: "Specifically, liberal democracies has the following components: (…) executive power is constrained, constitutionally and in facts, by the autonomous power of other government institutions (such as an independent judiciary, parliament and other mechanisms of horizontal accountability)".

[628] See for instance Council of Europe, Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, May 13, 2005, available at this address: https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)56&Sector=secCM&Language=lanEnglish&Ver=final&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75: "*Member states should maintain and enhance legal and practical measures to prevent state and private censorship. At the same time, member states should ensure compliance with the Additional Protocol to the Convention on Cybercrime and other relevant conventions which criminalise acts of a racist and xenophobic nature committed through computer systems. In that context, member states should promote frameworks for self- and co-regulation by private sector actors (such as the ICT industry, Internet service providers, software manufacturers, content providers and the International Chamber of Commerce). Such frameworks would ensure the protection of freedom of expression and communication*"; "*Member states should promote, through appropriate means, interoperable technical standards in the digital environment, including those for digital broadcasting, that allow citizens the widest possible access to content*"; the Joint declaration by UN commission of human rights, OSCE and OAS, December 21, 2005: www.article19.org/pdfs/standards/three-mandates-dec-2005.pdf: "*Filtering systems which are not end-user controlled – whether imposed by a government or commercial service provider – are a form of prior-censorship and cannot be justified. The distribution of filtering system products designed for end-users should be allowed only where these products provide clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive*".

[629] See for instance the Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, accessible at https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75: "*In co-operation with the*

Moreover, declaring specific content as illegal implies recognising at least the material existence of a crime, even if there is no legal proceedings initiated against its perpetrator and even if this perpetrator could be considered as innocent within the framework of a specific trial. The declaration of illegality is therefore a first step that could lead to a criminal accusation. Further, this first declaration of illegality could be taken into account by the Court that could in a second step declare the liability of the content's owner, without analysing this question again. In any cases, blocking is a deprivation of the right to distribute a specific content. As a consequence of all these observations, it would be appropriate and compliant with the ECHR to apply to such a declaration the same obligations as would be the case with the procedures of other criminal accusations.

As regards criminal accusations, the European Court of Human Rights requires the respect of the guarantees provided by article 6 of the ECHR, related to a fair trial, especially the existence of an independent and impartial tribunal. The wide conception of the Court of the meaning of "criminal matters" drives it to apply this principle also to administrative authorities that would be allowed by a national law to pronounce some sanctions[630]. Therefore, a person that would have committed an action that could be qualified as criminal has to be judged by an independent and impartial tribunal, which, in Europe, is usually a court of law. The declaration of its liability will allow the judge to pronounce an appropriate sanction.

---

private sector and civil society, member states should ensure that users are made aware of activated filters and, where appropriate, are able to activate and deactivate them and be assisted in varying the level of filtering in operation (…)"; "*In this context, civil society should be encouraged to raise users' awareness of the potential benefits and dangers of filters. This should include promoting the importance and significance of free and unhindered access to the Internet so that every individual user may fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information and the right to private life, as well as to effectively participate in public life and democratic processes*".

[630] Some countries, as France, use to transfer some powers of the judge to some ad hoc independent administrative authorities. This transfer of power has to respect some conditions, in addition to the respect of the guarantees of a fair trial. On this discussion, see Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux", 4 June 2009, Juriscom.net, pages 2 *et seq*., available at this address: http://www.juriscom.net/uni/visu.php?ID=1133. See also Jean-François Brisson, « Les pouvoirs de sanction des autorités de régulation: les voies d'une juridictionnalisation » ; AJDA 1999, p. 847.

7.8.2 The proportionality of the response to an illegal situation or action, or to an interference to other's private rights

The proportionality of an Internet blocking measure is generally difficult to assess, because it mainly depends on the particular 'legitimate aim' to preserve within each factual situation, on the usefulness of the measure to reach that aim in a particular circumstance, and on the blocking characteristics and their impact on other rights and freedoms. For instance, when a specific kind of blocking of an illegal website would only lead to blocking illegal contents, assessed as such by a judge, without blocking legal ones or an email domain, while the disruption caused by the measure are compensated for by its usefulness, a judge can consider a blocking measure as being the adequate response to address to the illegal situation. On the contrary, the non-existence of some or all of these requirements could lead one to consider the measure as non-proportionate. As the judge is the authority that has the professional ability and skills to assess the proportionality of a measure, when it relates to achieving a balance between freedoms[631], only the judge should have the power to assess the proportionality of a blocking measure, in response to a crime, an offence or an infringement.

The provision of resorting to a judge is sometimes a requirement to assess the proportionality of an interference, for the European Court of Human Rights. It pays indeed "*close attention (…) to the width of powers whereby restrictions on rights and freedoms are imposed*". "*Objections are likely to be raised where they are not subjected to close supervision and there is, therefore, much scope for possible abuse*". For instance, the European Court condemned search powers "*where these could be exercised without the need for a judicial warrant and were seen as subject to restrictions appearing too lax and full of loopholes; the police could decide upon the expediency, number, length and scale of searches and seizures and the interference with the applicant's right to respect for his private life could not be regarded as strictly proportionate to the legitimate aim of tackling tax evasion*"[632].

In consequence, since blocking might cause significant restrictions to the exercise of the right to freedom of expression and of the right for private life, the European Court could consider the resort of a judge, to decide on the setting up and of the extent of a blocking measure, as required.

As regards an Internet blocking measure that would not be directed against a content but against a person, for the purpose of sanction one of his or her actions for an offence or a crime, we can reach the same conclusion. Such a measure would be a very severe sanction, since it would lead to deprive this person of his or her entire right to communicate online and to exercise his or her right of private life in the electronic world, while the right to access the Internet is considered as fundamental in democracy[633]. Therefore, in such a situation as well, only the judge has the professional ability and should have the legitimacy to pronounce such a sanction, after having verified that it was proportionate to the crime being repressed. The European Parliament pronounced itself in that sense[634], as well as the Committee of Ministers

---

[631] See for instance Véra Morales, « La protection juridictionnelle des droits fondamentaux : révélation d'une entente conceptuelle », VI° Congrès français de droit constitutionnel, Atelier n°2 : « Le renouveau du droit constitutionnel par les droits fondamentaux », Montpellier, 9, 10 and 11 June 2005, accessible at the following address: http://www.droitconstitutionnel.org/congresmtp/textes2/MORALES.

[632] Jeremy McBride, "Proportionality and the European Convention on Human Rights", in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et seq., quotations p. 27.

[633] See above section 6.3.3.2.

[634] See for instance "No agreement on reform of telecom legislation", Information society, press release, 6 May 2009, available at this address: http://www.europarl.europa.eu/news/expert/infopress_page/058-55086-124-05-19-909-20090505IPR55085-04-05-2009-2009-true/default_en.htm: "*A user's Internet access cannot be restricted without prior ruling by the judicial authorities, insists the European Parliament reinstating one of its first-reading amendments*".

of the Council of Europe[635] and, as regards the "*purpose of protecting holders of copyright and related rights*", the French Constitutional Council[636].

[635] Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, III, accessible at https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75: "*Notwithstanding the importance of empowering users to use and control filters as mentioned above, and noting the wider public service value of the Internet, public actors on all levels (such as administrations, libraries and educational institutions) which introduce filters or use them when delivering services to the public, should ensure full respect for all users' right to freedom of expression and information and their right to private life and secrecy of correspondence*"; "*In this context, member states should (…) : ii. guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights*".

[636] See Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 16, decision available in English at this address: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf: "*The powers to impose penalties created by the challenged provisions vest the Committee for the protection of copyright, which is not a court of law, with the power to restrict or deny access to the internet by access holders and those persons whom the latter allow to access the internet. The powers vested in this administrative authority are not limited to a specific category of persons but extend to the entire population. The powers of this Committee may thus lead to restricting the right of any person to exercise his right to express himself and communicate freely, in particular from his own home. In these conditions, in view of the freedom guaranteed by Article 11 of the Declaration of 1789, Parliament was not at liberty, irrespective of the guarantees accompanying the imposition of penalties, to vest an administrative authority with such powers for the purpose of protecting holders of copyright and related rights*"

7.8.3 Role of the Internet Service Provider

The Ministers responsible for Media and New Communication Services of the Council of Europe did the same, as regards the interruption of an internet access but also as regards any action on the Internet that could question fundamental rights stating "*the cooperation of Internet Service Providers for content control, either in the field of copyright enforcement or in other areas, is problematic in terms of respect of freedom of expression and access to information. Only a judge should be able to decide whether to cut or not Internet access or to ask for a specific action on the Internet in full respect of fundamental rights and freedoms*"[637].

[637] 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services, "A new notion of media?" 21 April 2009, MCM(2009)021, p.5, accessible at: http://www.ministerialconference.is/media/images/MCM_2009_021.pdf.

7.8.4 Conclusion

As a result of the above, 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.

The latter is indeed a choice of each country, even if we have seen that blocking for moral purposes does not seems to be acceptable within a liberal democracy.[638]

Spam blocking has a particular statute, since its proportionality is generally accepted and since it responds to the demand of the very people who are impacted by the measure, in other words the email service users.

[638] See section 6.3.2

7.9 Conditions under which Internet blocking could be acceptable

Blocking attempts limit some fundamental rights and freedoms. The legitimacy of blocking, at least in liberal democracies which respect human rights and fundamental freedoms, is therefore dependent on respect of certain conditions in order to determine such legitimacy.

7.9.1 Conditions for Limitations to Fundamental Freedoms

Liberal democracies must respect Fundamental Freedoms and the Court of Human Rights conditions of their limitation

The conditions that have to be respected when limiting freedoms are especially detailed and supervised by the European Court of Human Rights. However, countries that only adhere to the ICCPR should follow this interpretation, at least regarding the right to freedom of expression, to contribute to the harmonisation of International law concepts related to Human Rights.

These conditions, which are described in detail throughout Chapter 7 are listed below into proposed steps to determine the legitimacy of blocking in a democracy that respects Human Rights and Fundamental Freedoms.

7.9.2 Determining blocking legitimacy in a liberal democracy

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

This implies that Internet blocking is implemented to preserve one or several particular legitimate interest(s), in a way to respond to a pressing social need with proportionality, on the basis of a law that would also take into account other specific international provisions that the concerned state respects.

Step 2 Determining rights and freedoms that will be limited

Internet Blocking will always be in interference with the right to freedom of expression, as it intends to reduce the accessibility of some contents or some individuals[639], and might also be in interference with the right to respect for private life[640]. Blocking might moreover limit in a more severe way some freedoms that disabled persons can only exercise thanks to their access to Internet technology and services[641]. It is therefore necessary to determine precisely which right(s) the planned blocking measure will interfere.

Step 3 Example
Determining the extent of the limitation

With regards to a blocking measure that would aim to prevent the access of a particular type of illegal content, such as child pornography, it should be determined in what extent legal contents or email domains might be blocked, which could lead to limit the right to protection of the freedom and of the confidentiality of private life, of family life and of correspondence[1]. It could therefore appear that additional effects might vary, depending on the characteristics of the servers or domains that host the contents to be blocked.

It should also be determined the cost of the measure and its impact on the quality, stability and development's schedule of the networks on which the measure has to be implemented, to further determine the impact of the measure on the right for private life and the right to freedom of expression, which might be reduced by a higher internet access cost, a lower networks' quality for today or tomorrow or a lower possibility to chose between ISP and services, because of the disappearance of some of them.

[639] See section 6.6.2.2
[640] See section 6.6.1
[641] See section 6.6.3

Step 3 Determining the extent of the limitation

The extent of an interference has to be determined taking into account:

- The inherent characteristics of the measure that might lead to limit some freedoms
- The inherent characteristics of the measure that could allow to implement further functionalities that would limit freedoms, even if the pursued aim is not to implement and use such functionalities
- The characteristics and functionalities that are expected from the measure to reach a particular aim

Step 3 Example
Impact of other functionalities – evidence of liability
The impact of other functionalities that a country or a stakeholder would like to append to the blocking measure should also be assessed. The general retention of the IP addresses of users that access blocked websites would be a strong limitation of the right to protection of personal data, which could even not be admitted[642], except within the framework of an investigation provided for by the law and, eventually, supervised by the judge[643]. Such retention would be all the more dangerous since an IP address does not allow to know which person was using the identified internet access to consult a website[644], while some countries begin to criminalise the regular access to online child pornography[645]. The retention of these data and the possibility to give them to the authorities could lead to unjustified investigations, depriving a person from his freedom for some days, leading to the seizure of his computer[646] and damaging his honour and reputation by arresting him in front of his neighbours without serious evidence of liability[647].

Step 4 Determining precisely the pursued aim(s)

A blocking measure that interferes in some conditional freedoms has to pursue one of the legitimate aims restrictively listed into the European Convention on Human Rights or the ICCPR, within the article proclaiming the specific freedom. Details in Section 7.4

A blocking measure generally pursues one or several of the following aims:

- The protection of the rights of others:
- The protection of morals:
- The protection of health:
- The prevention of crime:

[642] See section 6.6.1.3.
[643] See section 7.8.2.
[644] See section 6.6.1.3.
[645] See for instance article 227-23 of the French penal Code. Such provisions, which are considered as useful to investigators who need some further legal instruments to fight against online child pornography, seem however to dangerously go beyond the general principles of penal law in a democracy, which imply that an action can only be sanctioned when committed willingly and that penal law only criminalise actions or blatant omissions that are hurting the society's high values. Usually, seeing a crime is therefore generally not a crime, while not helping to stop the crime or to limit its effect, when feasible, can be one
[646] Without guarantee to get this material back, even in case of innocence.
[647] Beyond the impossibility to deduce from an IP address the liability of an individual for an action committed on the internet, a computer expert seems to have the possibility to make believe that an IP address is at the origin of an action while it is not. See for instance Michael Piatek, Tadayoshi Kohno, Arvind Krishnamurthy, "Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice", technical report, University of Washington Department of Computer Science and Engineering, http://dmca.cs.washington.edu/dmca_hotsec08.pdf, p. 3 (index du site : http://dmca.cs.washington.edu/)

- The repression of crime:

The precise determination of the pursued aim(s) is highly important, since the other conditions of the legitimacy of a blocking measure have to be assessed in regards to this aim.

Step 5 The stated blocking aim has to correspond to a reality

The aims listed above are all legitimate aims in the eyes of the international texts that are protecting freedoms. However, there still remains the issue of the effective possibility, for an Internet blocking measure, to pursue the determined aim.

Step 6 Determining if blocking for the stated aim answers a pressing social need

As soon as the pursued aim of a blocking measure is determined, another issue is to know if there is a pressing social need to reach that aim by a blocking measure that causes the interferences analysed in section 7.6. A positive answer implies that the blocking measure is able to answer that need adequately.

- Does blocking answer a pressing social need when aiming to protect crime?
- Does blocking answer a pressing social need when aiming to protect morals or sensitive persons' health (including children)?
- Does blocking answer a pressing social need when aiming to protect others' rights?

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

The interference in freedoms of an Internet blocking measure must be proportionate to the pursued aim.

- The overall effect of a particular restriction must be assessed, i.e. to assess the limitations caused to other freedoms, but also to assess the efficiency of the measure to reach the pursued aim.
- A measure that has a low level of efficiency cannot lead to limit, in a more extensive way, the freedoms this measure is interfering with.
- There must be sufficient basis for believing that the interest which is preserved by the Internet blocking measure is in peril.
- The proportionality of the very behaviour which is being restricted has to be assessed, i.e. a limitation will be less or more permissible, depending on the people's legitimacy of having this behaviour as regards the interest that is in danger.
- The less restrictive way to satisfactorily address the pursued aim has to be chosen.

Step 8 Consider the principle that must govern blocking in the lights of the European Court's criteria

As regards Internet blocking, those criteria allow to say that the "usefulness" of the measure to reach a particular aim has to be higher than or equal to the limitation brought to other freedoms.

- The "usefulness" of the measure has to be assessed on the one hand as regard the rate and importance of the peril suffered by the interest to preserve and on the other hand as regards the level of efficiency of the measure to prevent this particular peril, such a prevention having been recognised as a pressing social need.
- The limitation brought to freedoms has to be assessed as regards the importance of the freedoms that will be limited, and the proportionality of the exact behaviour that will be limited, as regards the limits it could bring to the interest

that has to be preserved by blocking. It has also to be assessed as regards the limitations that are not necessary to the pursued aim but that could be brought to freedoms because they are possible by the technology used to block.

This principle must be applied in conjunction with the following criteria

- The limitation of a freedom must be only brought to preserve the particular interest that is in peril and which justified the blocking measure.
- The limitation of a freedom must not "extinguish" the latter but leave "some scope" for its exercise, even if the "usefulness" of the blocking measure is assessed as very high.
- The limitation to freedoms must be the lowest possible, to satisfactorily address the pursued aim, and can never be higher to the "usefulness" of the measure defined.

Step 8: Example

A blocking measure can not be put in place, except if a law provide for provisions that prevent the use of certain functionalities of the mechanism, or that correct certain effects that can be corrected, to make the measure proportionate.

For instance, one of the negative effects of child pornography blocking on the citizen's rights would be the limitation of their right to be informed about the existence and the volume of such a crime on the Internet.

One corrective measure would be to regularly inform citizens about the remaining volume of such contents on the Internet, the means given to investigators and the level of successfulness of the investigations.

Step 9 ***A* law *may be needed to prevent the use of certain functionalities of the blocking mechanism***

Such a law will in most of the case have also to be voted, to insert the intervention of a judge into the blocking disposal. We have indeed seen that a judge was needed in at least two situations:

- The decision to block a particular content can be seen as a declaration of illegality, which can be the first step that could lead to a criminal accusation, and which could be used in a further trial to part-establish the liability of the content's owner. A decision to block content can be seen as a deprivation of the right to distribute that content, such a deprivation shall be provided for by a law, and, in liberal democracies, applied by the judge.
- The proportionality of the measure will need to be assessed in each specific case. Blocking particular content, which is on a particular server, by a particular measure, can cause or not some extended limitations to freedoms. Blocking a person to answer a crime is also a very severe sanction, which has to be assessed by a judge.

Step 10 Providing for blocking within law

A blocking measure that would meet all the necessary criteria must be provided for by the law. The definition of law includes here "*non-written law*", "*enactments of lower rank than statutes*", and sometimes cases-law[648]. Whatever the text will be, this law must be "*adequately accessible*", which means that "*the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case*", and must be "*formulated with sufficient precision to enable the citizen to regulate his conduct*"[649].

Law is necessary

A law is necessary for two main reasons.

The first one is the requirement of the public order clause holds by the European Convention on Human Rights. The European Court of Human Rights begins its analysis of every interference in a conditional freedom[1] by verifying if the interference was "*in accordance with the law*"[1].

The second one is the necessity, for the country that plans to implement blocking:

- To ensure that the blocking measure will not be in contradiction with other rights and obligations provided for in some international provisions it has took the commitment to respect.
- To combine these rights and obligations with the blocking's effects that could be in opposition with them.

[648] European Court of Human Rights case *Kruslin v. France*, judgment of 24 April 1990, Series A, n° 176 A, p. 20, § 29. See above our section

[649] All quotations are coming from the European Court of Human Rights case *Sunday Times v. The United Kingdom*, afore-quoted, § 49.

7.10 Studies Required

During the process of analysing the process of balancing fundamental freedoms several studies were identified as needed in order to enable adequate evaluation of the proportionality requirements. These studies do not preclude the necessity to assess the proportionality of the blocking measure on its own merits in addition to support of studies indicated here. This list is not exhaustive since each particular measure needs to be assessed in its own context and therefore further studies may also be required. The current list includes:

7.10.1 Internet Blocking and Prevention of Paedophilia

To ensure the reality of such a blocking aim, a study related to the prevention of paedophilia should be done that would give evidences that some people become criminals by accessing some internet contents, explaining the "taking action" process and highlighting the percentage of the concerned population. This study would demonstrate that blocking prevents effectively such people to access illegal images, while such an access is effectively the deciding factor that causes them to take illegal action.

This study could therefore identify the several Internet protocols used by the population to protect from becoming paedophile to access child pornography, their expected behaviour in case of blocking, to know for instance if they would renounce or, on the opposite, if they would find the way to access content by other means. This study could also evaluate the risk of taking action of the potential population that would not any more access illegal content, if such an aim appears as reachable.

7.10.2 Disrupting Commercial Child Pornography Business Model

To ensure the reality of such a blocking aim, a study related to the disruption of child pornography business model for commercial child pornography would for instance have to show on the percentage of business done thanks to the websites that are or could be blocked. It should review in which ways these websites are accessible and the impact of these ways on an Internet blocking measure in terms, for instance, of bypassing the measure. It should consider the other Internet protocols that are used to sell materials and the potential transfer rate of content and clients, between the web and those other protocols, in case of web-blocking.

7.10.3 Internet Blocking Reducing Child Pornography Exchanges

To ensure the reality of such a blocking aim, a study related to the usefulness of blocking to reduce child pornography exchanges would for instance show on the percentage of child pornography accessed through the protocol that is planned to be monitored, as regards the number of materials distributed by criminal through other protocols, and the impact of such a blocking on the behaviour of people who distribute and access child pornography through the blocked protocol, to know the potential transfer rate of content and lovers of those contents, between the blocked protocol and other ones.

7.10.4 Internet Blocking Protecting Sensitive Persons or Morals

To know if blocking on these aims, would answer a pressing social need, two kind of studies are needed:

A study on the efficiency of blocking to protect sensitive persons from contents which might cause them harm or to protect everyone to contents which are in opposition with morals (remembering that protecting people from accessing some defined content for moral purposes might not correspond to the democratic conception of freedom to access information, at least in liberal democracies). The key issue is to determine the volume of the population to protect, which means the percentage of the population that accidentally finds disturbing contents, or contents in opposition with morals, and the efficiency of blocking to ensure their protection.

This question could be answered by highlighting the volume of the population needed to be protected (which implies to know the percentage of access attempt done by Internet robots or machine), its characteristics, and the impact of the filtering measure on the blocked websites (to know if some of them reappear, in which extent and in which general delay, and if the new websites present the same characteristics of accessibility).

A study to determine if the blocking measure could be considered as really answering **a pressing social need** of protecting health or morals by blocking only *some* kinds of disturbing or immoral contents but not *all* the shocking content available. It seems that, in such a case, the measure could be assessed as irrelevant to reach its aim.

An analysis of the percentage of each disturbing contents that are easily accessible on the Internet would be welcome on that issue. This analysis could emphasis on the main identified disturbing contents (child pornography, murders, rapes, other kind of violence or tortures), but also deal with each content that could heart a specific population, for instance on the basis of the required filtering rules by users of end user filtering tools.

7.10.5 Internet Blocking Protecting Victims Interests

To ensure the **reality of such a blocking aim**, a study needs to be conducted on crime victims' interests which would demonstrate that the protection of such interests implies that one category or each category of individuals can not access to the victims' image within the scene of a crime.

This study would help to analyse the blocking's capability to adequately answer **a pressing social need**. It could for instance analyse the percentage of criminals that would not bypass the measure, and the percentage of people that do not want to access such images but who would, either the content has reappear at another address, the content was not on the list of contents to block, or those people usually bypass filters not to see illegal images, but simply to not being blocked at the occasion of their surf.

7.10.6 Internet Blocking Protects IPR

As regards IPR protection, the existence of a social need could be determined by a study on the reality of the threat that Internet represents for rights owners, which could include notably an analysis of the business model of the music and the movie industry on the Internet, especially the lack of availability of online legal content and the low level of the artists remuneration, an analysis of its perception by the general public and by artists, and of its possible evolution. If such a study would lead to say the IPR protection by blocking is a pressing social need, another study would be to analyse the efficiency of blocking on online IPR infringements. It could notably include an analysis of the expected behaviour of Internet users facing blocking, which could be to encrypt their exchanges or to exchange their files on other protocols or at other addresses or by other means on the protocol were the blocking measure is implemented. It could further include a analysis of the consequences of the latter behaviour on the efficiency of the measure.

Chapter 8 CONCLUSION

This report has covered four main subject areas on the subject of Internet blocking.

Chapter 3 reviewed the meaning of Internet blocking and considered different understandings of what Internet blocking means.

Chapter 4 covered the motivations why society currently believes that Internet blocking attempts might solve some major societal concerns and how other approaches do not appear to be very successful. It reviewed 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. It also provides a list of which countries have already adopted Internet blocking systems. The conclusion of this chapter is that there are substantial frustrations by some countries on the lack of effectiveness of current international cybercrime co-operations and the lack of response by some countries to significant legal issues including child pornography, hate speech or terrorism.

Chapter 5 provides a technical overview of the major Internet blocking systems in use today, explains how these are applied to different Internet services and discusses the impact of these systems and the technical challenges created by these systems. The methods which are used to evade these blocking systems and an analysis of the effectiveness of these systems is included. The chapter concludes that the implementation of an Internet blocking system requires substantial resourcing in terms of financial and human resources. Surprisingly one of the easiest systems to evade is DNS blocking which is a system used by many national blocking systems today. Nearly all systems have a technical impact of the resilience of the Internet and add an extra layer of complexity onto an already complex network. All systems can be bypassed sometimes a small amount of knowledge is required and sometimes some technical knowledge is required. Despite this, there is increasingly available software solutions on the Internet which assist in evading an Internet blocking measure.

Chapter 6 provided an comprehensive overview of Internet Blocking and the Law and provides an extensive review of relevant legal instruments which concern Internet Blocking systems. The key role modern liberal democracies have in their active respect for fundamental freedoms and civil liberties is clearly identified. The review includes national and International instruments and considers what fundamental rights are in opposition to Internet blocking and which fundamental rights support Internet blocking. It also considers the role of Internet Service Providers and the confusing situation they operate with regards to competing and sometimes contradictory legal requirements. This chapter discusses the complexity of these instruments and how they apply to Internet services and Internet blocking initiatives.

Chapter 7 develops the issue of balancing fundamental freedoms when different rights are in conflict and, through an analysis of processes adopted by the European Court of Human Rights provides guidelines on how Internet blocking measures can be developed. The development 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 ECHR guidelines. The chapter examines the legitimate aims of the Internet blocking initiatives and questions the validity of some systems. The chapter concludes with a

sequence of steps which can be followed in order to evaluate Internet blocking proposals for their legitimacy in a democratic society.