

Project on Cybercrime
www.coe.int/cybercrime



Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 4 March 2009 (draft)

Discussion paper (draft)

**Obligations of Internet Service Providers
with regard to child pornography:
legal issues**

prepared by
Marco Gercke (Germany)

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and
Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

This study does not necessarily reflect official positions of the Council of Europe or of the donors funding this project

Content

1	_ Introduction.....	4
1.1	Child pornography and the Internet	4
1.2	Harmonisation of Criminal Law	4
1.2	Discussion about the involvement of Internet Service Providers in the fight against child pornography	5
1.3	Scope of the discussion paper	5
2	_ The reason for an involvement of Internet Service Providers.....	6
2.1	Direct access to information (Hosting Provider)	6
2.2	Ability to control the access to information outside the jurisdiction (Access Provider).....	6
3	_ The dogmatic concept of obligations of ISPs related to child pornography	8
3.1	Structure	8
3.2	Obligations.....	8
3.2.1	Obligor	8
3.2.2	Instruments used to create obligations	8
3.2.3	Directly applicable or require an additional act.....	9
3.2.4	Measures to prevent crimes and measures related to crimes already committed	9
3.3	Consequences of a failure to act in accordance with the obligations.....	9
4	_ Overview of possible obligations of ISPs with regard to child pornography	10
4.1	Preventive measures	10
4.1.1	Hosting Provider	10
4.1.1.1	Registration of the operator of a website	10
4.1.1.2	Analysis of uploaded content	11
4.1.2	Access Provider	12
4.1.2.1	Data Retention.....	12
4.1.2.2	Registration of users.....	13
4.1.2.3	Blocking access to websites with child pornography	14
4.1.2.4	Block the transfer of files containing child pornography	16
4.2	Repressive Measures	17
4.2.1	Hosting Provider	17
4.2.1.1	Removing illegal content (“Notice and takedown”).....	17
4.2.1.2	Supporting investigations	17
4.2.2	Access Provider	18
4.2.2.1	Blocking users that have downloaded child pornography	18
4.2.2.2	Supporting investigations	19
5	_ Conclusion.....	20

1 Introduction

1.1 Child pornography and the Internet

The Internet has become one of the key instruments for the trade and exchange of child pornography images and videos.¹ There are several reasons for this trend towards a digital distribution of child pornography instead of the physical exchange.² One of the main reasons is the fact that the bandwidth available for Internet users has increased dramatically during the past decade in major parts of the world. Pictures and movies placed on a webpage can be accessed and downloaded by millions of users from nearly any place in the world within a very short period of time.³ Another issue that facilitated the process of a digitalisation of the means of exchanging child pornography is the fact that Internet users are feeling less observed while sitting in their homes and downloading material from the Internet. Unless the users made use of means of anonymous communication the impression of a missing traceability is very often wrong.⁴ Most Internet users are simply unaware of the electronic trail they leave while surfing.⁵

1.2 Harmonisation of Criminal Law

In recent years international organisations have increased their activities against child pornography in general and the Internet-related exchange of materials in specific. This includes the harmonisation of legal standards. In addition to broad approaches like the 1989 UN Convention on the Rights of the Child⁶ and the 2003 EU Council Framework Decision on combating the sexual exploitation of children and child pornography⁷ some of the latest approaches include measures that explicitly target Internet-related aspects of the exchange of child pornography. Examples for such approaches are Art. 9 of the 2001 Council of Europe Convention on Cybercrime⁸ and Art. 7 of the 2007 Council of Europe Convention on the

¹ *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>.

² Regarding the methods of distribution, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 10 et seq., available at: <http://www.cops.usdoj.gov/mime/open.pdf?Item=1729>. Regarding the challenges related to anonymous communication see above: Chapter 3.2.m.

³ It was reported that some websites containing child pornography experienced up to a million hits per day. For more information, see: *Jenkins*, "Beyond Tolerance: Child Pornography on the Internet", 2001, New York University Press. *Wortley/Smallbone*, "Child Pornography on the Internet", page 12, available at: <http://www.cops.usdoj.gov/mime/open.pdf?Item=1729>.

⁴ Regarding the challenges related to investigations involving anonymous communication technology see *Gercke*, Herausforderungen bei der Bekämpfung der Internetkriminalität, Multimedia und Recht, 2008, page 294 et seq.; Regarding the impact on tracing offenders see: *Nicoll*, Concealing and Revealing Identity on the Internet in: *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 et seq.

⁵ Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

⁶ UN Convention on the Right of the Child, A/RES/44/25 – available at: <http://www.hrweb.org/legal/child.html>.

⁷ 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.

⁸ Council of Europe Convention on Cybercrime, CETS No: 185, available at: <http://conventions.coe.int>. Regarding the Convention on Cybercrime see: *Sofaer*, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available online: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, page 140 et seq.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review

protection of children against sexual exploitation and sexual abuse.⁹ Legal approaches show a number of remarkable developments – especially with regard to the objects and acts covered. They contain provisions that extend the criminalisation to realistic images that have been created through the use of 3D modelling software.¹⁰ And they tend to criminalise the possession of child pornography in addition to the production and dissemination of child pornography.

1.2 Discussion about the involvement of Internet Service Providers in the fight against child pornography

Internet Service Provider (ISP) play an important role in almost every data exchange process taking place in the Internet. Due to the structure of the Internet the transmission of data requires the service of a number of providers.¹¹ The offenders can use the network infrastructure of the Access Providers to log-on to connect to the Internet and download child pornography and those who want to offer child pornography can rent storage capacities from a Hosting Provider to make child pornography available to other users.

Ever since activities of offenders shifted to the Internet, the question as to whether ISPs need be involved in the fight against child pornography as been discussed. Concepts for such an involvement cover a wide range of issues, from a liability for crimes committed by the ISP's client to obligations to block access to child pornography websites.¹²

1.3 Scope of the discussion paper

The discussion of obligations of ISP with regard to child pornography is to a large extent solely focusing on specific obligations and related solutions. The present discussion paper is following a different approach. It analyses the underlying structure of obligations of ISP with regard to child pornography on the Internet. It is not a study that intends to conclusively analyse the topic but to point out issues for further discussion.

The majority of issues related to this discussion – especially aspects related to the blocking of child pornography¹³ – are linked to technical aspects of data transfer processes and

International 2008, page 7 et seq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1 – available at: <http://elr.ils.edu/issues/v23-issue1/aldesco.pdf>; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005 – available at: <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf>; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 et seq; Adoption of Convention on Cybercrime, International Journal of International Law, Vol 95, No.4, 2001, page 889 et seq.

⁹ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: <http://conventions.coe.int>.

¹⁰ Based on the National Juvenile Online Victimization Study, only 3% of the arrested internet-related child pornography possessors had morphed pictures. *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.

¹¹ Regarding the network architecture and the consequences with regard to the involvement of service providers see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003 – available at: <http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html>.

¹² See below: Chapter 4.1.2.

¹³ For an overview about the technical aspects of blocking child pornography see: *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 50 et seq.; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filtern van kinderporno op internet, 2008, page 10 et seq.; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrveruegungen.pdf;

detection of suspicious content. The discussion paper highlights the importance of these technical aspects without going into detail.

The discussion paper is based on the broad definition of the term "Service Provider" of Art. 1 c) Convention on Cybercrime.¹⁴ This definition covers a wide range of categories of providers such as Access Provider and Hosting Provider.¹⁵

2 The reason for an involvement of Internet Service Providers

There are different reasons why a role of ISPs in preventing the exchange of child pornography as well as the investigation of child pornography cases is intensively discussed.

2.1 Direct access to information (Hosting Provider)

The ISPs in general control the infrastructure related to their service. Hosting providers for example enable user to store information on storage capacities linked to the network. Unless information is encrypted the Hosting Provider has in general access to the clients data stored on his server. With this direct access he has a greater ability to identify illegal content than police or specialized agencies as his access is neither depending on the results of public search engines nor is it limited by access restriction systems implemented by the client (such as passwords).

Hosting Providers cannot only play an important role in the identification but also in hindering access to illegal content such as child pornography stored on their computer systems without removing the content itself and thereby altering potential digital evidence.

2.2 Ability to control the access to information outside the jurisdiction (Access Provider)

National approaches to criminalize Internet-related acts that are going beyond international standards face a number of problems. With regard to traditional crimes the decision of one or a few countries to criminalize a certain conduct can influence the ability of offenders to act in these countries without risking to be prosecuted. However, when it comes to Internet-related offences the ability of a single country to influence the offender's ability to act is much smaller as the offender can, in general, act from any place with a connection to the network.¹⁶ If he acts from a country that does not criminalize a certain conduct, international investigations as well as extradition requests will very often fail as a consequence of the requirement of dual-criminality.¹⁷ One of the key aims of international legal approaches is,

¹⁴ "service provider" means:

- i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service;

¹⁵ Regarding the differentiation between different types of Internet Service Providers based on the focus of their service see: *Clark*, Networks, IP and the Internet, 2003, page 27 et seq.; *Smith*, Internet Law and Regulation, 2007, page 4 et seq.; *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime – Toward common best-of-breed guidelines?, 2008, Chapter 2.3.

¹⁶ See: *Gercke*, National, Regional and International Legal Approaches in the Fight Against Cybercrime, Computer Law Review International, 2009, page 12.

¹⁷ 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

therefore, to prevent the creation of safe havens by ensuring the implementation of global standards.¹⁸

With regard to national requirements that are going beyond international standards, supplementary regulatory measures may be put in place for ISPs. One example is the establishment of obligations of ISPs to block access to content made available on servers located outside the country.¹⁹ This approach can be considered as an attempt to “re-territorialise the Internet”. It is up to a certain point comparable to the traditional border-control approach as the blocking of content stored outside the country hinders users in the country to download the content. As with regard to borders, such blocking approaches can currently be circumvented for example by using tunnel connects or anonymous communication services like TOR²⁰ that hinder the ISP from getting access to the URL request. The current discussion about “IP-tracing” within the ITU Study Group 17 highlights the increasing demand for more accurate procedures.²¹ Depending on the type of content blocked such an approach may conflict with human rights provisions, and especially the freedom of expression.²²

Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). 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>; *Schjølberg/Hubbard*, “Harmonizing National Legal Approaches on Cybercrime”, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; Plachta, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 et seq, available at: http://www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

¹⁸ The issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: “States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies”. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: “There must be no safe havens for those who abuse information technologies”.

¹⁹ 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/edriagram/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, World 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/iapcod/0211xx-isp-study.pdf>. *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 et seq.

²⁰ Regarding technical approaches in tracing back users of Anonymous Communication Servers based on the TOR structure see: *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3.

²¹ With regard to the IP-Tracing discussion within the ITU Study Group 17 see: Study Group 17, TD 4068, 2008; Rutkowski, Basic Information on the ITU-T IP-Traceback and International Caller-ID Capability Initiatives, 2008, available at: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/Rutkowski_IPtraceback_callerID_rev0.pdf.

²² With regard to the human rights aspect see: Council of Europe 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; Joint Declaration of the OSCE

3 The dogmatic concept of obligations of ISPs related to child pornography

3.1 Structure

The discussion of obligations of ISP focuses on different types of obligations such as:

- Hindering users from accessing websites with child pornography
- Preventing the upload of child pornography images
- Preserving traffic data to be able to identify offenders that are making child pornography available or download such material
- Stronger support of LEAs in identifying locations where child pornography is stored.

Structurally, discussions relate to two basic categories:

- Obligations: A significant part of the current discussion focuses on the question in how far ISP have the obligation to prevent crimes or support investigations
- Consequences: The second category is related to the question in how far the failure of the ISP to act in accordance with its obligations leads to consequences and what these consequences are.

3.2 Obligations

Prior to providing an overview of the different obligations that already exist or are under discussion it is possible to further divide between different sub-categories:

3.2.1 Obligor

The approaches towards establishing obligations address different categories of ISP.²³ Considering that different types of service are offered, the specific obligations of Hosting Providers will up to a certain degree be different from the once for Access Providers.

3.2.2 Instruments used to create obligations

There are different instruments that are used to establish obligations of ISP. The three most important tools are:

- Creation by law
- Decree law or administrative acts
- Contracts and other voluntary agreements.

The first and most common way is the development of obligations by law. With regard to the fact that the obligations can go along with the requirement of financial investments by ISPs in the necessary technology and could interfere with the rights of users, a law as basis for the obligation might in some cases be necessary. An example for such an approach is Art.

Representative on Freedom of the Media & Reporters Sans Frontieres on Gauardanteeing Media Freedom on the Internet, 2005, available at: https://www.osce.org/documents/rfm/2005/06/15239_en.pdf.

²³ Regarding the differentiation between different types of Internet Service Providers based on the focus of their service see: *Clark*, Networks, IP and the Internet, 2003, page 27 et seq.; *Smith*, Internet Law and Regulation, 2007, page 4 et seq.

18, paragraph 1b) Convention on Cybercrime that requires an ISP to submit subscriber information in his possession or control in the context of criminal investigations.²⁴

Another approach is the development of obligations by an administrative act or a decree law. An example for such an approach is an Italian Decree that was issued by the Minister of Telecommunication on the 8th of January 2007. This decree does by amending Decree Law No. 38 from the 6 February 2006 oblige ISPs to use filter technology to block the access to websites with child pornography.²⁵

Apart from that obligations can be developed by contract or other voluntary agreements.²⁶ An example is the draft contract between the German Federal Police (Bundeskriminalamt) and ISPs to block websites containing child pornography on the basis of a blacklist provided by the Federal Police.²⁷ Another example is the blocking of child pornography images online by British Telecom ("Cleanfeed").²⁸

3.2.3 Directly applicable or require an additional act

Another possibility to differentiate between obligations is to focus on the way the obligations are created. In general it is possible to differentiate between obligations that are automatically applicable and obligations that require an additional act to come into force – such as a court order.

3.2.4 Measures to prevent crimes and measures related to crimes already committed

It is furthermore possible to divide between obligations aiming to prevent crimes and those related to offences that already have taken place, for example, in relation to the possession of child pornography and even acts prior to the possession.²⁹ Blocking access to child pornography websites and collecting information about users that tried to access such websites by the Access Provider is prevention with regard to the access of the user. With regard to the website itself the Access Provider is unable to prevent the offence of making the material available but might be able to assist LEA in collecting evidence related to this offence.

3.3 Consequences of a failure to act in accordance with the obligations

As diverse as the obligations are the possible consequences of the failure of an ISP to act in accordance with the obligation. They range from administrative fines and contractual penalties to a criminal liability and the loss of the license to operate the service.

²⁴ For more information see below: Chapter 4.2.1.2.

²⁵ With regard to the Decree see: *Lonardo*, Italy: Service Provider's Duty to Block Content, *Computer Law Review International*, 2007, page 89 et seq.

²⁶ See in this regard: *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 204 et seq.; *Horten*, The Telcoms Package and „3 strikes“ – voluntary cooperation to restrict downloads, 2008.

²⁷ The draft version of the contract is available at: <http://www.ccc.de/press/releases/2009/20090213/20090211-vertragsentwurf-bka-isp.pdf>.

²⁸ Regarding the software used to block child pornography see: *Clayton*, Anonymity and traceability in cyberspace, 2005, page 115 et seq.; *Clayton*, Failures in a Hybrid Content Blocking System in: *Privacy Enhancing Technologies*, 2006, page 78 et seq.

²⁹ See in this context for example Art. 20, paragraph 1f) of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), that criminalises the act of „knowingly obtaining access, through information and communication technologies, to child pornography“.

4 Overview of possible obligations of ISPs with regard to child pornography

The following chapter provides an overview of possible obligations related to child pornography that are either already contained in international instruments and national laws or are currently discussed. With regard to the structure the following chapter distinguishes between Access Provider and Hosting Provider as well as between preventive measures and obligations arising after an offences has been committed.

4.1 Preventive measures

While in the past discussions on the obligations of ISP concentrated on the role of ISP in criminal investigations the focus has shifted. Current debates focus to a large extent on involving ISPs in preventing crimes related to child pornography in the Internet. One example is the discussion of the introduction of a mandatory filtering obligation in Australia.³⁰ A similar discussion is currently taking place in Germany.³¹

Although this discussion is often linked to combating child pornography in the Internet there are other offences possibly entailing obligations of ISPs. One example is copyright violations. The question if ISPs shall obliged to hinder users from up-loading or downloading copyright protected material through file-sharing systems was controversially discussed during the debate on the EU Telecoms reform.³² After criticism of such obligations by the European Parliament³³ the Commission decided not to include such obligations in the legislative text presented in November 2008.³⁴ The debate was recently reopened in connection with new legislative initiatives on reform of the E-Commerce Directive.

4.1.1 Hosting Provider

4.1.1.1 Registration of the operator of a website

One concern with regard to the exchange of illegal content in general and child pornography in specific³⁵ is the fact that offenders can use free webspace to make such material available.³⁶ Even if the illegal content on such websites is detected the identification of the offender who made it available is difficult as services that are offered free of charge do in general not verify registration information even if they require a formal registration.³⁷ An

³⁰ See: *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Moses*, Web censorship plan heads towards a dead end, *The Sydney Morning Herald*, 26.02.2009, available at: <http://www.smh.com.au/articles/2009/02/26/1235237810486.html?page=fullpage#contentSwap1>.

³¹ See for example: *Germany to Crack Down on Internet Child Pornography*, 20.11.2008, available at: <http://www.dw-world.de/dw/article/0,2144,3808419,00.html>.

³² *Horten*, The Telecoms Package and „3 strikes“ – voluntary cooperation to restrict downloads, 2008.

³³ Vote of the European Parliament on 24th of September 2008.

³⁴ 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.

³⁵ See *Moore/Clacton*, The Impact of Incentives on Notice and Take-down, page 6 et seq., available at: <http://weis2008.econinfosec.org/papers/MooreImpact.pdf>.

³⁶ *Moore* and *Clayton* point out that with the phishing attacks they analysed 17% of the spoofed websites were located on webspace available free of charge. See *Moore/Clayton*, Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing, available at: <http://www.cl.cam.ac.uk/~rnc1/fc09evil.pdf>.

³⁷ Regarding the impact of free webspace on criminal investigations see: *Schwarz*, „A Case of Identity: A Gaping Hole in the Chain of Evidence of Cyber-Crime, *Boston University Journal of Science and*

obligation of ISP to register users and verify the registration information could improve the ability of LEAs to identify the publisher of child pornography images.

But there are concerns related to such an approach. The requirement of an effective verification procedure would raise the costs for the operator of the service and could make free services in general more difficult to run. This would especially influence those who can not afford paid services. Taking into account the idea of a global non-discriminatory access to the Internet raises concerns related to such restrictions.³⁸ Art.4 of the Council of Europe Declaration on Freedom of Communication on the Internet³⁹ points out that barriers to the participation of individuals in the information society should be removed. The explanatory notes to the Draft Declaration⁴⁰ points out that this does especially refer to mandatory registration obligations.⁴¹

4.1.1.2 Analysis of uploaded content

Files uploaded to be available on a website are in general stored on the Host Providers servers. As mentioned above, the Hosting Provider has in general access to the clients' data stored on his server. With this direct access he has a greater ability to identify illegal content than police or specialized agencies as his access is neither depending on the results of public search engines nor is it limited by access restriction systems implemented by the client (such as passwords). An obligation of the Hosting Provider to monitor the content that is uploaded combined with an obligation to report illegal content could increase the ability of LEAs to investigate in cases related to illegal content.

There are four general concerns related to this approach. The first is concerning the cost of such measure. As is the case with registration obligations, the requirement of content-checking procedures would go along with additional costs for the industry. This could have a negative effect on the availability of free services.⁴² The second concern is related to aspects of the technical ability to implement such procedures without influencing the general nature of the service. Especially for larger Hosting Provider with several Terabyte of files being uploaded every day it is in general impossible to run manual analyses of every file uploaded. It is very likely that even automated technical solutions such as hash-value bases searches for known child pornography images⁴³ or a keyword search⁴⁴ would negatively influence the upload speed. Before implementing such obligations further technical research is required. In any case, such obligation would only apply to Hosting Providers. Taking into account that

Technology Law, Vol. 9, Issue 1; *Evers*, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005 – available at: <http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm>.

³⁸ See in this context: *Kertcher/Margalit*, Challenges to Authorities, Burdens of Legitimation: The Printing Press and the Internet, *Yale Journal of Law & Technology*, 2005-2006, page 25; *Nunziato*, The Death of the Public Forum in Cybespace, *Berkeley Technology Law Journal*, Vol 20, page 1162.

³⁹ Council of Europe, Committee of Ministers, Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies)

⁴⁰ CM (2003) 67.

⁴¹ This means in practice that public authorities should not issue regulations which complicate the setting-up and running of individual web sites, for example licensing or registration systems or any other requirements having a similar effect.

⁴² See in this context above: Chapter 4.1.1.1.

⁴³ *Gordon/Hosmer/Siedsma/Rebovich*, *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*, 2002, page 57.

⁴⁴ See *Vacca*, *Computer Forensics, Computer Crime Scene Investigation*, 2nd Edition, 2005, page 48; *Lange/Nimsgger*, *Electronic Evidence and Discovery*, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*, 2002, page 63.

there are other ways how files can be exchanged – for example by using file-sharing systems that do not require an upload on a server, the creation of such obligations might only shift the problem to another level. The last aspect of the concerns is related to existing legal standards that might prevent the implementation of such obligation unless existing standards are changed. One example for such legal standard is Art. 15 EU E-Commerce Directive:

Article 15

No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Based on Art. 15 of EU E-Commerce Directive a Hosting Provider shall have no general obligation to monitor information transmitted or stored. As pointed out in Explanation 47, Member States are prevented from imposing a monitoring obligation unless in a specific case.⁴⁵

4.1.2 Access Provider

4.1.2.1 Data Retention

If users that have downloaded child pornography images from a website or from a file-sharing system without using personal information or undertaking financial transactions by using a registered account, the identification of the user in general needs to be based on traffic data such as the IP-address.⁴⁶ Such information that LEAs in general need to trace back and identify the offender are often deleted shortly after the finalisation of the transfer process.⁴⁷ This leaves a time frame for investigations that is smaller than those required by traditional investigation instruments.⁴⁸ A data retention obligation forces the provider of Internet services to save traffic data for a certain period of time.⁴⁹ The implementation of a data retention obligation is an approach to avoid the above mentioned difficulties of getting access to traffic data before they are deleted. An example for such an approach is the EU Directive on Data Retention.⁵⁰

⁴⁵ Directive 2000/31/EC of the European Parliament and 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) – available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.

⁴⁶ *Gordon/Hosmer/Siedsma/Rebovich*, *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*, 2002, page 57; Regarding the different sources that can be used to extract traffic data see: *Marcella/Marcella/Menendez*, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, 2007, page 163 et seq.

⁴⁷ *Gercke*, *Datenschutz und Datensicherheit*, 2003, page 477 et seq.; *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

⁴⁸ *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", *CRi* 2006, 142.

⁴⁹ For an introduction to data retention 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.; *Blanchette/Johnson*, *Data retention and the panoptic society: The social benefits of forgetfulness* – available at: <http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf>.

⁵⁰ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The fact that key information about any communication in the Internet will be covered by the Directive lead to intensive criticism by human rights organisations.⁵¹ It was especially criticised that the fact that users are aware of the data retention could influence their way of using the Internet for legitimate purposes.⁵² This could lead to a review of the Directive and its implementation by constitutional courts.⁵³ In addition, in her conclusion in the case *Productores de Música de España (Promusicae) v. Telefónica de España*⁵⁴ the advisor to the European Court of Justice *Advocate General Juliane Kokott* pointed out that it is questionable whether a data retention obligation can be implemented without a violation of fundamental rights.⁵⁵ Difficulties with regard to the implementation of such regulations were already pointed out by the G8 in 2001.⁵⁶ Such an obligation is not contained in the Convention on Cybercrime. Apart from the legal aspects there are also technical concerns related to data retention obligations. If the offenders are using anonymous communication technology that is based or at least partly operated outside countries with data-retention obligations an investigation based on retained data can be seriously hindered.⁵⁷

4.1.2.2 Registration of users

If the user, who is downloading child pornography images from online sources uses Internet access facilities that do not require an identification with personal information prior to the use of the service it can be difficult for LEAs to later on identify the offender.⁵⁸ A registration obligation could prevent users from abusing the service and enable their identification if they committed a crime. An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7⁵⁹ of the Italian Decree 144⁶⁰ that was in 2005 converted

⁵¹ See for example: Briefing for the Members of the European Parliament on Data Retention – available at: <http://www.edri.org/docs/retentionletterformepps.pdf>; CMBA, Position on Data retention: GILC, Opposition to 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.

⁵² See in this regard: *Pimenidis/Kosta*, The Impact of the Retention of Traffic and Location Data on the Internet user – A critical discussion, *Datenschutz und Datensicherheit (DUD)*, 2008, page 92 et seq.

⁵³ See: Heise News, 13,000 determined to file suit against data retention legislation, 17.11.2007 – available at: <http://www.heise.de/english/newsticker/news/99161/from/rss09>.

⁵⁴ Case C-275/06.

⁵⁵ See: Advocate General Opinion – 18.07.2007 – available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top>. The court does usually but not invariably follow the advisors conclusion.

⁵⁶ In a G8 Meeting in Tokyo experts discussed the advantaged and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

⁵⁷ Regarding the impact on tracing offenders see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, *Digital Anonymity and the Law, Tensions and Dimensions*, 2003, page 99 et seq.

⁵⁸ See in this context: *Wortley/Smallbone*, *Child Pornography on the Internet*, U.S. Department of Justice, Office of Community Oriented Policing Services, 2006, page 39

⁵⁹ Based on Art. 7 "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electronic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a license by local authorities and identify persons using the service. For more information see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, *Computer und Recht International*, 2006, page 94 et seq

⁶⁰ Decree 144/2005, 27 July 2005 ("Decreto-legge"). - Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article Privacy and data

into a law (Legge No 155/2005).⁶¹ The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes or universities⁶²) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this services.

It is uncertain if the extent of the improvement of investigations justifies the restriction of access to the Internet by requiring an identification procedure. Free access to Information is widely recognised as an important aspect of the Information Society and is protected by the constitution in a number of countries.⁶³ It is likely that the requirement of identification will affect the use of the Internet - especially in countries where publishers of critical reports on the political situation are facing the risk of sanctions. Apart from that, offenders that want to prevent identification can easily circumvent the identification procedure. They can for example use prepaid phone cards bought abroad that do not require an identification to access the Internet.

4.1.2.3 Blocking access to websites with child pornography

One of the issues that is currently very much in the focus of the discussion about the involvement of ISPs in combating child pornography in the Internet is blocking the access to websites containing child pornography.⁶⁴ As the Access Provider is responsible for forwarding requests of the user for accessing a website, he is from a technical point of view in general able to check if the website requested is on a black 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 proxy servers to hybrid

retention policies in selected countries available at
<http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026>.

⁶¹ For more details see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, *Computer und Recht International*, 2006, page 94 et seq.

⁶² *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, *Computer und Recht International*, 2006, page 95.

⁶³ With regard to the human rights aspect see as well: Council of Europe, Committee of Ministers, Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies)

⁶⁴ 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, Sperrverfügungen im Internet, 2008; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research 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/edriagram/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, *World 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-isp-study.pdf>. *Zittrain*, *Harvard Journal of Law & Technology*, 2006, Vol. 19, No. 2, page 253 et seq.

solutions that combine various approaches.⁶⁵ As pointed out above this approach is especially relevant with regard to content that is stored at a location outside the jurisdiction and can therefore not be removed. Several European countries such as Norway⁶⁶, Sweden⁶⁷, Switzerland⁶⁸ United Kingdom⁶⁹ and Italy⁷⁰ as well as non European countries such as China⁷¹, Iran⁷² and Thailand⁷³ use such an approach.

There are a number of concerns related to the blocking of websites. The first concern is that all technical solutions that are currently available can be circumvented.⁷⁴ As a consequence blocking content shall not substitute efforts to remove the content from the server where it is stored and if necessary develop the necessary legal requirements (such as harmonisation of differing national standards). Such filtering approaches are therefore mainly relevant to prevent accidental access.⁷⁵ The second technical concern is related to the fact, that a number of those technical solutions that are currently discussed go along with the threat of

⁶⁵ For an overview about the technical aspects see: *Sieber/Nolde*, Sperrverfügungen 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*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrveruegungen.pdf; *Pursch/Baer*, Sperrverfügungen 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.

⁶⁶ „Telenor Norge: Telenor 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 pornography sites, T-CY (2006) 04, page 3.

⁶⁷ 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 pornography sites, T-CY (2006) 04, page 3; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008, page 6.

⁶⁸ *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 55; *Schwarzenegger*, Sperrverfügungen gegen Access-Provider in: *Arter/Joerg*, Internet-Recht und Electronic Commerce Law, page 250.

⁶⁹ *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research 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 pornography 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>.

⁷⁰ *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 Research Service, Nov. 2008, page 6 et seq.; *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 54.

⁷¹ *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: <http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrveruegungen.pdf; *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73;

⁷² *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

⁷³ *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, page 55

⁷⁴ *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrveruegungen.pdf

⁷⁵ *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008, page 2.

over-blocking.⁷⁶ If a discussion about child pornography legislation is not possible anymore because the access to such website is blocked due to the term "child pornography" this could in addition to the technical component have a legal implication with regard to the protection of freedom of expression. The importance of those fundamental rights was pointed out by the Council of Europe Recommendation⁷⁷ on measures to promote the respect for freedom of expression and information with regard to Internet filter.⁷⁸ The third major concern is related to the fact, that the technology that is implemented to block child pornography (that is globally recognised as illegal content) can be used to block other content as well. This can happen intentionally as well as accidentally by adding websites to the filter-list that contain legitimate content.⁷⁹

4.1.2.4 Block the transfer of files containing child pornography

Access Providers establish connections to the Internet. Provided that the user does not send or receive encrypted material the Access Provider has at least in some cases the possibility to analyse the content transmitted. 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 images⁸⁰ or a keyword search.⁸¹

The concerns related to the cost side as well as the loss of performance are similar to the concerns related to analysis performed by the Hosting provider.⁸² In addition the same legal concerns need to be taken into consideration. With regard to EU countries such obligations to monitor content transmitted would not be in line with Art. 15 of the EU E-Commerce Directive. Based on Art. 15 of EU E-Commerce Directive an Access Provider shall have no general obligation to monitor information transmitted or stored. With regard to Access Provider a second legal issue needs to be taken into account within the discussion as the content transmitted might be covered by laws protecting the privacy of correspondence⁸³ and telecommunications.⁸⁴

⁷⁶ *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

⁷⁷ 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)

⁷⁸ „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.”

⁷⁹ *Clayton*, Failures in a Hybrid Content Blocking System in: Privacy Enhancing Technologies, 2006, page 78 et seq; *Ayre*, Internet Filtering Options Analysis: An Interim Report, 2006, page 5.

⁸⁰ *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>.

⁸¹ 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.

⁸² See above: Chapter: 4.1.1.2.

⁸³ See in this context: *Rodriguez*, Protecting the secrecy of telecommunications : a comparative study of the European Convention on Human Rights, Germany and United States, 1995. The issue of secrecy of correspondence was also highlighted by the Council of Europe Recommendations on measures to promote the respect for freedom of expression and information with regard to Internet filters: „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

4.2 Repressive Measures

Apart from the prevention of an exchange of child pornography via the Internet, obligations of ISPs may also refer to the termination of a criminal activity that is already taking place and can therefore not be prevented anymore. In addition the involvement of ISPs in criminal proceedings is discussed.

4.2.1 Hosting Provider

4.2.1.1 Removing illegal content ("Notice and takedown")

As mentioned above the Hosting Provider has in general access to the clients data stored on his server. With this direct access he has the ability to remove illegal content or block the access to the content. If the Hosting Provider is obliged to remove child pornography as soon as he becomes aware of it, this can positively influence the availability of such material online. Such an obligation is for example established by Art. 14 EU E-Commerce Directive. Based on Art. 14 a Hosting Provider that obtains concrete knowledge of illegal activities or illegal content can only avoid liability if he immediately removes the illegal information.⁸⁵ The failure to immediately react thus leads to a criminal liability of the Hosting Provider.

There are a number of concerns related to such an obligation. Based on Art. 14 of the directive it is not necessary that a court or a competent authority informs the Provider about illegal content. Even information passed by a regular user can create an obligation to remove the content. The Hosting provider is therefore often in a difficult situation. On the one hand side he needs to react immediately to avoid liability – on the other hand side he has certain obligations with regard to his customers. If he removes legal information that was just at first sight illegal this could lead to claims for indemnity. The fact that a significant number of incidences report to hotlines dealing with child pornography turned out to be not related to illegal material highlights the challenge for ISPs to deal with this obligation.⁸⁶

4.2.1.2 Supporting investigations

In recent years the Council of Europe Cybercrime Convention has become the global standard for cybercrime legislation.⁸⁷ Art. 16 – 21 of the Convention provide a framework for procedural instruments related to Cybercrime investigations. These contain a number of obligations for Hosting Providers such as:

- Art. 16 ("Expedited Preservation"): As pointed out above the identification of a cybercrime offender does very often require the analysis of traffic data.⁸⁸ One of the

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."

⁸⁴ Similar to a traditional voice communication provider that would in most countries not be allowed to monitor conversations and interrupt them if they are linked to criminal activities an Access Provider will not be allowed to intercept any correspondence in order to analyse the content exchanged.

⁸⁵ This procedure is called "notice and takedown"

⁸⁶ See in this respect for example the 2007 Global Internet Trend Report Trends associated with Illegal Content on the Internet based on the experiences of the INHOPE International Network of Internet Hotlines, available at www.inhope.org.

⁸⁷ See Gercke, National, Regional and International Legal Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, page 7 et seq.

⁸⁸ "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or

main challenges for investigation is the fact that traffic data that are relevant for the information are often deleted automatically within a rather short period of time.⁸⁹ Based on Art. 16 Convention on Cybercrime a Hosting Provider is obliged to preserve the relevant data on request.

- Art. 18 ("Production Order"): Art. 18 Convention on Cybercrime enables the competent authorities to order a Hosting Provider to submit traffic and content data as well as subscriber information. The Hosting provider is obliged to follow the order.
- Art. 19, paragraph 4 ("Support of LEA"): Very often the investigators will not be able to identify the exact location with the help of the system administrator that is responsible for the server infrastructure.⁹⁰ But even if they are able to identify the hard drive protection measures might stop them from searching for the relevant data. The drafters of the Convention therefore included an obligation of system administrator and other people, who have knowledge about the location of stored information to assist the law enforcement agencies in Art. 19, paragraph 4.

4.2.2 Access Provider

4.2.2.1 Blocking users that have downloaded child pornography

Access Providers have up to a certain degree the possibility to block clients from using their services. If they add a client to a black list he would not be able to use the Access Providers service in the future to commit crimes. This approach was controversially discussed during the debate on the EU Telecoms reform.⁹¹ After criticism by the European Parliament⁹² the Commission decided not to include such an obligations in the legislative text presented in November 2008.⁹³ In 2008 France introduced a draft law that would oblige ISP to block users that have not stopped violating copyrights from using their service.⁹⁴ This approach was reported to be criticised by the EU Commission.⁹⁵

destination, traffic data regarding these past communications is required", See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155.; Regarding the identification of suspects by IP-based investigations see: *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.

⁸⁹ The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an e-mail, accessing the Internet or downloading a movie) those traffic data that have been generated during the process and that ensure that the process could be carried out are not anymore needed and the storage of the data would increase the cost of operating the service. The cost issue was especially raised within the discussion about data retention legislation in the EU. See for example: E-communications service providers remain seriously concerned with the agreement reached by EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: <http://www.ispai.ie/EUROISPADR.pdf>; See as well: ABA International Guide to Combating Cybercrime, page 59.

⁹⁰ "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

⁹¹ *Horten*, The Telecoms Package and „3 strikes“ – voluntary cooperation to restrict downloads, 2008.

⁹² Vote of the European Parliament on 24th of September 2008.

⁹³ 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.

⁹⁴ 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/.

⁹⁵ 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>.

Several concerns are related to this approach. First of all such a ban could easily be circumvented by using public access points. Apart from that, the ban is linked to an Internet access – not necessary to a specific user. If several users are connecting to the Internet by using a single connection they would all be affected by the measure. This raises concerns with regard to the freedom of access to information services.⁹⁶

4.2.2.2 Supporting investigations

The procedural instruments mentioned in Art. 16 – 21 Convention on Cybercrime do not only apply to Hosting Providers but also to ISPs. In addition to related obligations mentioned above, the obligations of Art. 17, 20 and 21 Convention on Cybercrime are of relevance to ISPs.

- Art. 17 (“Partial Disclosure”): The Convention on Cybercrime does strictly distinguish between the obligation to preserve data and the obligation to submit them to the competent authorities. Without a partial disclosure law enforcement agencies would in some cases not be able to trace back the offender and preserve more relevant data when more than one provider was involved.⁹⁷ Therefore Art. 17 Convention on Cybercrime creates an obligation to disclose certain traffic information.
- Art. 20 (“Collection of Traffic Data”): Traffic data play an important role in cybercrime investigation.⁹⁸ Having access to content data enables law enforcement agencies to analyse the nature of messages or files exchanged and help to trace back the offender. Depending on the way Art. 20 Convention on Cybercrime is implemented by the member states it requires and ISP to collect the traffic data in real time.
- Art. 21 (“Interception of Content Data”): In some cases the collection of traffic data is not sufficient to collect the evidence that is required to convict the suspect. This is especially relevant in those cases where the law enforcement agencies do already know the communication partner and the services used but have no information about the information exchanged. Depending on the way Art. 21 Convention on Cybercrime is implemented by the member states it requires and ISP to intercept the content data in real time.

⁹⁶ With regard to the Freedom of access to the Internet see: Council of Europe, Committee of Ministers, Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies).

⁹⁷ “Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.” See Explanatory Report to the Convention on Cybercrime, No. 167.

⁹⁸ “In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.” See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in Cybercrime investigations see as well: ABA International Guide to Combating Cybercrime, page 125; Gercke, Preservation of User Data, DUD 2002, 577 et seq.

5 Conclusion

As diverse as the obligations are the possible consequences of a failure of an ISP to act. Possible consequences range from administrative fines and contractual penalties to a criminal liability and the loss of the license to operate the service. Especially the question of criminal liability is of relevance to ISPs.

An example of an approach to force ISPs to block access to child pornography images and as a consequence of a failure to act start criminal proceedings are the preliminary proceeding against the CEO of CompuServe Germany in 1996.⁹⁹ The prosecution based its investigation on the fact that pornographic images showing the sexual abuse of children that were stored on servers of CompuServe US were available to customers of CompuServe Germany.¹⁰⁰ As a consequence, the trial against the CEO of CompuServe Germany was based on the assumption that failure of the access providers to block such content leads to a criminal responsibility of the CEO for the content to which they provide users access.¹⁰¹ The approach by the German court was heavily criticized.¹⁰²

Taking into account the importance of the services offered by the ISPs in the information society and technical limitations of ISPs to prevent and stop crimes, several approaches to limit the liability of ISPs have been discussed. One example is reflected in Art. 12 - 15 of the EU E-Commerce directive.¹⁰³

⁹⁹ Regarding the CompuServe case see *Gercke*, The Development of Legislation Related to the Criminal Liability of Internet Service Providers in Germany in: Reich, *Cybercrime & Security, IV., C.*, Booklet IVC.Germany.A-1; Local Court (Amtsgericht) Munich, *Multimedia und Recht (MMR)* 1998, page 432 et seq. with annotation *Sieber*; District Court (Landgericht) Munich, *Neue Juristische Wochenschrift (NJW)* 2000, page 1051 et seq; *Hoeren*, *Neue Juristische Wochenschrift (NJW)* 1998, page 2792 et seq.

¹⁰⁰ *Derksen*, *Neue Juristische Wochenschrift (NJW)* 1997, 1878 et seq.

¹⁰¹ Local Court (Amtsgericht) Munich, *Multimedia und Recht (MMR)* 1998, page 432 et seq. For a summary of cases in the English language see: <http://www.qlinks.net/comdocs/somm.htm>; *Frydman/Rorive*, *Regulating Internet Content through Intermediaries in Europe and the USA*, *Zeitschrift fuer Rechtssoziologie*, 2002, page 52 – available at: http://www.isys.ucl.ac.be/etudes/cours/inf2202/Frydman_&_Rorive_2002.pdf. For the court decision in English see <http://www.kuner.com/data/reg/somm.html>.

¹⁰² *Gercke*, The Development of Legislation Related to the Criminal Liability of Internet Service Providers in Germany in: Reich, *Cybercrime & Security, IV., C.*, Booklet IVC.Germany.A-1.

¹⁰³ Directive 2000/31/EC of the European Parliament and 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) – available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.