Removing and Blocking Illegal Online Content:

About Controversy, Censorship and Proportionality[1]

Eva Lievens, Karel Demeyer & Jos Dumortier[2]

Introduction

On 13 December 2011, *Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography* was adopted, repealing and updating the 2004 Framework Decision on this topic. The much debated Article 25 of this proposal requires Member States to ensure the prompt *removal* of child pornography websites hosted in their territory and to endeavour to obtain the removal of such websites hosted outside their territory.[3] Additionally it leaves the option for Member States, subject to several safeguards, to *block* access to such websites towards users within their territory.[4] Both these policy choices are very controversial and highly debated, both on the level of the European Union and the individual Member States.

Directive 2011/92/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography

Directive 2011/92/EU on combating the sexual abuse, sexual exploitation of children and child pornography standardises and updates the criminalisation of acts of sexual abuse and exploitation of children (including new phenomena, such as grooming),[5] aims to facilitate the prosecution of offenders and the protection of victims and focuses on prevention and introduces a strategy to deal with online child sexual abuse material (Europa 2011).

The history of the different European legislative instruments and proposals on this matter shows how controversial the policy choice of how to deal with illegal Internet content is. The 2009 Proposal for an updated Council Framework Decision, backed by the Council (Europa 2009) and the Committee of the Regions (2010), added an Article 18 titled 'Blocking access to websites containing child pornography', imposing an obligation on Member States 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*". The Commission's original preference for blocking measures was clarified in the impact assessment which accompanied the 2009 Proposal (European Commission 2010a). Blocking web pages is described as not being the ultimate solution to stop the distribution of child pornography, but, as child pornography dissemination is profit-driven, according to the Commission "*making access more difficult also makes it a less profitable*

[1] This paper is an abridged version of an article accepted for publication in *Policy & Internet*. Please note that the article also contains an extended technical analysis of blocking and removing content. To obtain a draft version, please send an e-mail to eva.lievens@law.kuleuven.be.

[2] Dr. Eva Lievens is a Senior Research Fellow of the Research Fund Flanders at the Interdisciplinary Centre for Law & ICT (KU Leuven). Karel Demeyer is a researcher at the Leuven Institute for Criminology (KU Leuven). Prof. dr. Jos Dumortier is Professor of ICT law and head of the Interdisciplinary Centre for Law & ICT (KU Leuven).

[3] *Removal* entails an intervention at the illegal content *provider*'s side by trying to 'remove' the material from the Internet. Technically, this entails that the content is no longer on a computer system that is 'connected to' or 'part of' the Internet.

[4] *Blocking* intervenes at the illegal content *consumer*'s side and consists of trying to make it technically impossible or very difficult to access the content by filtering Internet users' data connections and blocking their access to the illegal content.

[5] Cf. Recital 19 and Article 6 Directive/2011/92/EU.

business" (European Commission 2009, 34). Moreover, filtering and blocking was "*identified by various stakeholders as a necessary component of the fight against child sexual abuse and exploitation*" (European Commission 2009, 34).

The 2010 Commission Proposal for a Directive of the European Parliament and Council amended this article, adding the obligation for Member States – "*without prejudice to the above*" – to "*take the necessary measures to obtain the removal*" of pages containing child pornography (European Commission 2010a, Article 21).

Although both versions of the article add that with regard to blocking measures adequate safeguards must be taken into account, the debate was fuelled by human right advocates arguing against the introduction of this obligation. After concerns issued by the European Data Protection Supervisor (EDPS) on the legality of blocking operated by private parties (European Data Protection Supervisor 2010) and the opinion of the European Economic and Social Committee (EESC), stating that priority should be given to removing malicious web content at the source (European Economic and Social Committee 2010), the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) drafted an amended proposal. This proposal, agreed upon by the Parliament on 27 October 2011 (European Parliament 2011) and finally adopted in December 2011, inverses the order of the obligations, requiring Member States in Article 25, first, to "*ensure the prompt removal of webpages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory*". In a second paragraph, it does leave Member States the option to "*block access to webpages containing or disseminating child pornography towards the internet users within their territory*" adding that "*these measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress*".

Removal and Blocking from a Technical Perspective

Blocking Web Pages

Several technical measures can be used by or imposed upon third parties by governments to block access to webpages[6] containing or disseminating child pornography towards the Internet users within their territory, at several 'Internet Points of Control' (Zittrain 2003). However, all blocking techniques that are currently being used (such as (TCP/)IP packet header filtering,[7] DNS 'tampering' or 'poisoning',[8] web proxy and hybrid proxy and IP packet filtering,[9] or dynamic Blocking techniques[10]) can be circumvented, for instance by the use of a third party proxy server[11] that is not subject to the blocking regime; especially in combination with the use of encryption, so that the web addresses of the requested content and the content itself are unreadable. This can be compared to a situation where calling certain phone numbers is made impossible in a country. A citizen could easily call an accomplice abroad and ask her or him to dial the blocked number and connect the call. In order for the blocking methods to work efficiently, governments would also have to obtain the blocking of the third party proxy servers, which might also be used for legitimate purposes (e.g. anonymity).

[6] It is important to stress that every version of the proposal for Directive 2011/92/EU only ever discussed the restriction of access to 'web pages' disseminating child sexual abuse material. Although the 'web' (i.e. all Internet traffic using the HTTP(S) protocol, not only the content requested by and viewed in web browsers) is the most known and popular application of the Internet, it is only one of the applications that may be used to disseminate illegal material (Greenfield, Rickwood and Tran 2001; Akdeniz 2010). Consequently, blocking only web pages – even if this would be fully effective (*infra*) – will not put a stop to the distribution of this type of content.

[7] Blocking specific IP addresses/port numbers.

[8] Blocking specific domain names.

[9] Blocking specific web pages/files.

[10] On the basis of content.

[11] There are several other ways to circumvent these blocking techniques. Using a proxy server is a very easy and popular way.

Using a proxy server sounds quite technically challenging but is made very easy by several free or paying services on the Internet (McNamee 2010). All a user has to do to circumvent the blocking is to surf to such a website and fill in the address of the blocked website. The service will send the request through a proxy server and return the requested webpage. In addition, freely available services[12] make it possible to use the Internet with all the data traffic from and to one's computer being encrypted, enabling users to anonymously browse the web without being tracked. These technologies are easy to deploy[13] and use, and are promoted and used for instance by human rights advocates, activists and journalists.

The above mentioned techniques attempt to block 'specific' website domains, websites or files identified to carry illegal content. These are identified by their source (IP-address, domain name or URL) which is on a 'blacklist'. A major problem with this approach is that when such a blacklist is reverse engineered or leaks onto the Internet (and experiences in countries already using blacklists prove this does occur)[14], it provides people with malicious intent looking for these specific kinds of illegal data with a highly targeted list of resources. At the same time, because this system only blocks specific pieces of content previously marked as illegal, this method could be considered as ineffective, given the vast amount of data available on the Internet. This can result in a false sense of safety and the illusion that the problem of online child sexual abuse is being tackled. On the other hand, depending on the technique used, blocking could also be over-inclusive by not only blocking the illegal content but also content (and other services) from the same web server, served from the same IP-address or using (parts of) the same keywords describing the illegal content.

Automated blocking techniques have other shortcomings as they leave no scope for argument or exercise of discretion which leads to an all-or-nothing approach which may not comply with principles of proportionality (*infra*) (McIntyre and Scott 2008). For instance, technical solutions might not be able to distinguish child pornography from non-abuse pictures depicting child nudity (e.g. a photo of a child taking a bath shared in a family photo album, or a piece of art like the Pulitzer Prize winning photograph of Kim Phúc).

On top of this, the different blocking techniques also have a high implementation cost. In an impact analysis assessing Internet blocking to combat terrorism, the European Commission expressed concern with regards to the cost of implementing blocking and filtering systems by ISPs and concluded that the implementation of such a system would have a direct economic impact not only on ISPs but also on consumers (Akdeniz 2010).

Removing Web Pages

Another option, introduced at first as a possibility by the Commission in the 2010 proposal but now made the standard policy in the final text of the Directive, is the removal of content. Enforcement difficulties may arise when attempting to remove web pages at the source (Zittrain 2003): it is necessary to know where the different copies of the data are located on the Internet, who is responsible for the service offering the data, who is responsible for the data itself, and which jurisdiction applies (depending, for instance, on the physical location of the storage media, the place where the responsible resides, etc.).

However, notwithstanding the difficulties, it is possible to successfully remove illegal data from the Internet (McNamee 2010). In a 2008 study, Moore and Clayton concluded that the most important factor to success is the incentive to remove (even more important than the technology used by the criminal); for instance, financial institutions seemed to be relatively successful at removing phishing websites while it took on average 150 times longer to remove child pornography (Moore and Clayton 2009).In addition, in an analysis of websites on a leaked Swedish blocking blacklist, digital rights advocates found that they could have websites carrying child pornography, which had been on Scandinavian Internet blocking blacklists for years, removed in very

[12] Such as The Onion Router (TOR), http://www.torproject.org/.

[13] E.g. video tutorials for the installation and use of TOR are available at http://www.torproject.org/docs/documentation.html.en.

[14] Cfr Australia: Moses (2009); Denmark: Meloni (2008); Thailand: Van Buren (2008); Finland: Wikileaks (2008); Norway: Wikileaks (2009).

short time (Freude 2010). This could prompt the question whether law enforcement has until now been sufficiently committed to obtaining the removal of illegal content at the source.

Removal and blocking from a legal perspective

Although any attempt to enhance the protection of children's rights[15] can only be welcomed, the policy choices of removing and particularly blocking child pornography web pages has also proven to be controversial from a legal point of view.

Restrictions on the Free Flow of Information

Although the fundamental rights impact analysis in the impact assessment that accompanied the 2009 Proposal acknowledged the possible interference of the measures with the right to freedom of expression (for instance by occasionally blocking legitimate content too) and stated that the measures therefore must be subject to law and that the proportionality must be guaranteed by a series of safeguards, it was argued that this policy option "*has a positive impact on fundamental rights, as it aims to promote and advance the right to protection of children as laid down in Article 24 of the EU Charter [of Fundamental Rights]"* (European Commission 2009, 38). There are, however, a number of remarks that can be made in this context.

Article 10 of the European Convention on Human Rights (ECHR),[16] which guarantees the right to freedom of expression, provides the possibility to restrict the distribution of certain content, since one of the core characteristics of this article is that this is not an absolute freedom. Certain 'expressions'[17] or content are considered so reprehensible that restrictions may be justified. However, within the legal framework, such restrictions need to fulfil three conditions: they need to be prescribed by law, they need to achieve a certain goal of public interest, and they must be necessary in a democratic society.[18]

First, restrictions need to be prescribed by law. This means that restrictions must be adequately foreseeable, i.e., they must be phrased with sufficient precision so that individuals are able to anticipate the consequences which a given action may cause. In this respect, Recital 47 of Directive 2011/92/EU states that

> *"measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as* ***legislative, non-legislative, judicial or other****. In that context, this Directive is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States". [emphasis added]*

This has undoubtedly been inspired by the wish of certain Member States to maintain the systems they have put in place to fight online child pornography. Although it is thus explicitly stated that the actions should not necessarily be prescribed by law, in order to fulfil the above-mentioned requirement, the recital adds that

> *"Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability to users and service providers".*

[15] Cf. for instance, the United Nations Convention on the Rights of the Child, or Article 24 §2 EU Charter of Fundamental Rights: "*In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*".

[16] Recital 47 of Directive 2011/92/EU explicitly mentions that developments with regard to Article 25 must "*take account of the rights of the end users and comply with existing legal and judicial procedures and the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union*".

[17] Recital 46 of the Directive goes as far as stating that "*Child pornography [...] is a specific type of content which cannot be construed as the expression of an opinion*".

[18] Cf. e.g. European Economic and Social Committee (2010, point 5.1).

It remains to be seen how Member States will implement this requirement in practice, and how they will ensure that removal or blocking procedures are foreseeable and transparent.

Second, restrictions need to achieve a certain goal of public interest. *In casu*, this condition will not pose difficulties; measures taken to address child pornography will fall under the prevention of crime, or the protection of health or morals. In this context we can refer to the case KU v Finland, dealing with an advertisement of a sexual nature on an Internet dating site concerning a minor, in which the European Court of Human Rights stated that

> "*Although 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, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others*".[19]

Third, the measures taken need to be necessary in a democratic society, which entails the existence of a "*pressing social need*". Even though a margin of appreciation is left to the Member States, the European Court of Human Rights will evaluate whether the concrete measure was "*proportionate to the legitimate aims pursued*", and whether the reasons for justification presented by the national authorities are "*relevant and sufficient*".

Proportionality is a very important guiding principle when assessing restrictions on fundamental rights. The drawbacks of blocking methods as shown by the technical description (*supra*), such as the over-inclusiveness and significant ineffectiveness of blocking may lead to significant concerns about the proportionality of blocking content. Although it is easy to argue that child pornography is so reprehensible that the end justifies any means, and therefore blocking content is acceptable despite its proven inefficiency, it is important to take into account the effect this may have on the free flow of information. This is why it is very important that Article 25 states that

> "*the measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress*".

However, we can only hope that these requirements are effectively taken into account when establishing concrete measures, so that the potential negative side-effects on legitimate online content are minimised to the greatest possible extent.

The E-Commerce Directive and Liability of Intermediaries: Towards Private Censorship?

The issue of blocking content is closely linked to the liability of intermediaries as laid down in the *E-Commerce directive*.[20] The *E-Commerce Directive* stipulates a horizontal and conditional exemption from (penal and civil) liability for certain service providers for a wide range (Barcelo and Koelman 2000) of illegal information (copyright infringement, libel and defamation, child pornography, xenophobia, etc.) provided by a recipient of the service. The exemptions from liability established in this directive, however, are only applicable to cases where the activity of the information society service provider is limited to a mere technical functionality, i.e. the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission

[19] European Court of Human Rights. KU v Finland. No. 2872/02. 2 December 2008: para. 49.

[20] 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). *OJ* 17 July 2000, *L* 178: 1.

more efficient.[21] This activity has to be of a mere technical, automatic and passive nature, which entails that the Internet service provider has neither knowledge of nor control over the information which is transmitted or stored.[22] Three types of provision of information society services can, under certain conditions, claim this exemption: mere conduit (Article 12), caching (Article 13) and hosting (Article 14).

Article 14 E-Commerce Directive: Exemption for Hosting Providers. Article 14 of the *E-Commerce Directive* states that where an information society service is provided, and consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

> "*(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.* "[23]

The exemption depends on the level of knowledge and the legal actions with which the service provider is being confronted. It has been argued that hosting providers have been unfairly burdened with the difficult task of judging themselves when content is illegal or a complaint is credible before undertaking action and expeditiously removing the information or disabling access to it (Barcelo and Koelman 2000; Ide and Strowel 2000; Montéro 2001). Identifying child sexual abuse imagery may not be straightforward or obvious, particularly where teenagers are depicted. Hence, to expect private actors, such as ISPs, to decide on the illegality of such images is, in our view, a dangerous precedent. Especially if liability is linked to these decisions (and it is a difficult question to answer who is to be held liable for data uploaded on the Internet by end-users, especially on so-called "User Generated Content" platforms) (Valcke and Lenaerts 2010), this may lead to a chilling effect on freedom of expression: in order not to be found liable,[24] providers might remove content which is perfectly legal (Lievens 2010). This possibility could have a serious impact on the right to freedom of expression. It can be rightfully argued that the guarding of constitutional rights should not be left to private companies, not only because they may lack legal knowledge to judge whether an infringement has taken place, especially when the material is not evidently illegal (Barcelo and Koelman 2000; Montéro 2001), but also because such decisions must be taken in the public (and not a private) interest and must adhere to important procedural safeguards, such as transparency and the right to appeal (The organization for security and co-operation in Europe and Reporters sans Frontières 2005).

In this context, the Council of Europe stated in its *Human Rights Guidelines for Internet Service Providers* that ISPs which provide access services, hosting, applications or content, should not be "*expected to advice on what content or behaviours are illegal and/or harmful*" (Council of Europe 2008, paras 16 and 24). For reasons of legal certainty and European harmonisation, it would have been useful if this document would have put forward a number of indicators to take into account when judging the admissibility and (il)legitimate nature of a request for takedown.

In 2010 the European Commission drafted a number of informal recommendations (European Commission 2010b) for the clarification of notice and take down procedures[25] for web pages carrying potentially illegal content based on the definitions of not only the *Framework Decision on Combating Sexual Exploitation of Children and Child Pornography of 2004* but also the *Framework Decision on Combating*

[21] Recital 42 E-Commerce Directive.
[22] Recital 42 E-Commerce Directive.
[23] Article 14 para. 1 E-Commerce Directive.
[24] E.g. Donadio (2010) regarding the conviction of Google executives by an Italian Court for content posted on its services.
[25] The scope of the recommendation is well defined as the document states that "*the recommendations are intended to clarify notice and take down procedures. They do not refer to filtering or blocking methods*".

Certain Forms and Expressions of Racism and Xenophobia[26] or the *Framework Decision 2002/475/JHA on Combating Terrorism*[27]. These recommendations are problematic in our view.

First of all, these unofficial[28] recommendations might induce non-transparent, private forms of censorship as ISPs are requested to decide themselves whether content, reported by citizens, is legal or illegal and whether it should be taken down. As we have mentioned above, such methods may be problematic from a human rights point of view.

Secondly, these recommendations not only envisage the removal of child pornography by private parties, but also other kinds of possibly illegal content. Even more so than in cases of child pornography, it might prove to be very dangerous for the protection of the right to freedom of expression to have private parties decide what is e.g. xenophobic, racist etc. The fact that these different criminal behaviours are tackled in the same document is seen by digital rights advocates as an underhanded way to shape policy, by abusing the atrocious nature of child abuse to justify harsh measures compromising human rights, which are then also applied to other types of illegal content (McNamee 2010). This kind of 'mission creep' can also be recognised for instance in different cases where website blocking lists, which were initially set up only to block child pornography, when leaked, seem to contain addresses of websites bearing no images of abused children but other content that is unwanted by the government or other parties (such as copyright holders), but not described by law.[29] Increasingly; blocking is being advocated as the solution for addressing various types of problematic content. For instance in The Netherlands, policymakers have proposed to broaden the use of the blocking systems which were initially only designed to combat child sexual abuse, to gambling websites (Rijksoverheid 2010). In the United Kingdom, ISPs have been ordered to block Newzbin2, a usenet search engine that is claimed to be used heavily by copyright infringers (Lee 2011), as well as the Pirate Bay, a file-sharing site (BBC News 2012). Whereas illegal acts must of course be punished if they occur, as more and more types of content are considered to be worth blocking in order to attempt to stop these kinds of acts, not only the chilling effect may increase but the free flow of information on the Internet may be limited to an undesirable extent.

Article 15 E-Commerce Directive: No General Obligation to Monitor. Notwithstanding Article 14, Article 15 *E-Commerce Directive* confirms that ISPs do not have a general obligation to monitor. It is considered an impossible task for ISPs to monitor all information which is being stored or transmitted to search for illegal activities. Yet, Article 15 does not mean that an ISP cannot voluntarily perform spontaneous acts of (editorial) control, or use filters, etc., for example, because it wants to protects its image or promote its services as being 'child-friendly'. In these circumstances, however, again, private censorship is lurking behind the corner (Montéro 2001), and the ISP runs the risk of losing its exemption when an active instead of a passive role is assumed.

Recent Case-Law of the European Court of Justice on Blocking Systems. Recently, the European Court of Justice has shed some light on the scope of Articles 14 and 15 of the *E-Commerce Directive*, in two cases in which a Belgian copyright management association (SABAM) had summoned an Internet service provider (Scarlet) and a social networking platform (Netlog), both classified as hosting providers, to install a filtering/blocking system in order to prevent the unlawful use of musical and audiovisual work. In the Netlog case the Court stated that to

[26] Council Framework Decision 2008/913/JHA of 28 November 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law. *OJ* 6 December, *L* 328: 55.
[27] Council Framework Decision of 13 June 2002 on Combating Terrorism. *OJ* 22 June, *L* 164: 3.
[28] This document "*was written by the Commission and distributed to participants in the consultation (Member States, industry and EDRi). It was not officially published anywhere by the Commission. It was a suggestion by the Commission regarding what industry could 'volunteer' to do, rather than a formal policy document" (answer of an EDRi spokesman on a question we asked about the status of the document).*
[29] E.g. BBC News 2009 and Corner 2010.

> "*oblige [Scarlet/Netlog] to actively monitor almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights. It follows that an injunction would require the hosting service provider to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31*".[30]

In addition, in both cases the Court found that, aside from potentially infringing the operators' freedom to conduct business and the customers' right to privacy,[31] such an injunction to block could also

> "*potentially undermine freedom of information since that system might not distinguish adequately between unlawful and lawful content, with the result that it could lead to the blocking of lawful communications*".[32]

Of course, it should be emphasised that the 'illegal content' that was the target of the proposed filtering system by SABAM were copyright infringements. It can be imagined that the conclusion of the Court would be different when it would examine a case related to child pornography. However, the arguments are interesting to consider, especially since our technical analysis also showed that most blocking or filtering systems function on a very indiscriminate basis and are often over-inclusive.

Conclusion

Comparing the first proposal made by the Commission in 2009 and the final Article 25 of Directive 2011/92/EU it is very clear that, due to the vigorous debate throughout the different stages of the legislative process, important changes have been adopted and that the wording has been carefully considered.

Two crucial points can be made regarding Article 25.

Firstly we are delighted to see that the final text requires Member States to emphasise the *removal* of content and, hence, to focus on identifying perpetrators and punishing them, instead of investing substantial efforts in largely fruitless and ineffective attempts to block content. Whereas blocking is a costly operation which is still easily circumventable, removal of the content, while possibly also not feasible in certain circumstances, will ensure that child sexual abuse images do not further circulate, and, hence, that the risk of repetitive re-victimisation is reduced. Additionally, in the course of trying to remove content, law enforcement must find out where it is hosted and get in contact with the hosting party where the perpetrator store the content (and might have left traces). Doing so, the law enforcer in charge will intuitively be closer on the heels of the perpetrator already, unlike in the case of blocking methods which are deployed close to the end users, where the law enforcers have to contact the end users' ISP's. Finally, even if the blocking tools were to be successful, for now they still only target web content, while numerous other technologies, such as peer-to-peer networks, are available where criminal activity could flee to for the distribution of imagery.

Second, if policymakers in member states do decide that, notwithstanding the disadvantages, *blocking* content remains an option to pursue, crucial questions that need to be asked are, first, who decides on the illegality of content that needs to be blocked, and, second, who blocks the content, and in what manner.

Leaving the discretion for the blocking of web content to private parties (for instance ISPs) might be considered problematic. We have pointed to the problems regarding the identification of illegal content by private parties. Both the resulting chilling effect (especially if ISPs would be found legally liable) as well as the

[30] European Court of Justice. Scarlet v SABAM. C-70/10. 24 November 2011: para. 40; European Court of Justice. SABAM v Netlog. C-360-10. 16 February 2012: para. 38.

[31] With regard to a potential infringement on the right to protection of users' personal data, the ECJ stated that "*the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified*": Scarlet v SABAM: para. 51.

[32] Scarlet v SABAM: paras 49-52; SABAM v Netlog: paras 47-50.

technical over-inclusiveness and indiscriminate nature of blocking techniques could lead to a significant, possibly disproportional, limitation of the fundamental freedom of expression. Following the Council of Europe (2008), as well as the European Data Protection Supervisor (2010), we believe that private parties should not be expected to decide which content or behaviours are illegal and/or harmful. We believe that this task belongs to - or at least needs to be surveyed by - the judicial power in a democratic society.

As for the question of how blocking should be organised, in our view the procedures should be clearly defined and transparent, truly adhering to the necessary safeguards laid down in Article 25. Only in this manner the negative side-effects on the free flow of legitimate information will be minimised.

References

Rijksoverheid. Adviescommissie Kansspelen via Internet. 2010. *Legalisatie van Kansspelen via Internet*. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/08/23/rapport-kiv.html (August 16, 2012) [in Dutch].

Akdeniz, Yaman. 2010. "To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression." *Computer Law & Security Review* 26 (May): 260-273.

Barcelo, Rosa-Juliá and Kamiel Koelman. 2000. "Intermediary Liability in the E-Commerce Directive: So Far So Good, but It's Not Enough." *Computer Law & Security Report* 4: 231-239.

BBC News. 2009. "Thais Block 'Anti-Royal Websites." 6 January. http://news.bbc.co.uk/2/hi/asia-pacific/7813269.stm (August 16, 2012).

BBC News. 2012. "The Pirate Bay Must Be Blocked by UK ISPs, Court Rules." April 30. http://www.bbc.co.uk/news/technology-17894176 (August 16, 2012)

Callanan, Cormac, Marco Gercke, Estelle De Marco and Hein Dreis-Ziekenheiner. 2009. "Internet Blocking, Balancing Cybercrime Responses in Democratic Societies." http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf (August 16, 2012).

Corner, Stuart. 2010. "EFA Fights ACMA over 'Take Down' Notice." *ITWire*. April 20. http://www.itwire.com/it-policy-news/regulation/38423-efa-fights-acma-over-take-down-notice (August 16, 2012).

Council of Europe. 2008. *Human Rights Guidelines for Internet Service Providers – Developed by the Council of Europe in Co-operation with the European Internet Service Providers Association (EuroISPA)*. http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf (August 16, 2012).

Donadio, Rachel. 2010. "Larger Threat is Seen in Google Case." *The New York Times*. February 24. http://www.nytimes.com/2010/02/25/technology/companies/25google.html (August 16, 2012).

Europa. 2009. Press Release "2936th Council Meeting Justice and Home Affairs Luxembourg." http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/09/83&format=HTML&aged=1&language=EN&guiLanguage=en (August 16, 2012).

Europa. 2011. Press Release "European Parliament Supports Stronger Legislation Against Child Sexual Abuse." http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1255&format=HTML&aged=0&language=EN&guiLanguage=en (August 16, 2012).

European Union. Committee of the Regions. 2010. *Opinion on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography and Combating Trafficking in Human Beings, and Protecting Victims. OJ* 29 May, C 141: 50.

European Union. European Commission. 2009. *Commission Staff Working Document – Accompanying Document to the Proposal for a Council Framework Decision on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA – Impact Assessment*. SEC (2009) 355.

European Union. European Commission. 2010a. *Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Sexual Abuse Imagery repealing Framework Decision 2004/68/JHA*. COM (2010) 94 final.

European Union. European Commission. 2010b. *Draft Recommendations for Public Private Cooperation to Counter the Dissemination of Illegal Content Within the European Union*. http://www.edri.org/files/Draft_Recommendations.pdf (August 16, 2012).

European Union. European Data Protection Supervisor. 2010. *Opinion on the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA. OJ* 30 November, *C* 323: 6

European Union. European Economic and Social Committee. 2010. *Opinion on the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA. OJ* 15 February, *C* 48: 138.

European Union. European Parliament. 2011. *Legislative Resolution on the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework*

Decision 2004/68/JHA. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2011-0468#top (August 16, 2012).

Freude, Alvar. 2010. "Analysis of a Representative Example of European Blacklists." *AK Zensur*. http://ak-zensur.de/2010/09/29/analysis-blacklists.pdf (August 16, 2012).

Greenfield, Paul, Peter Rickwood and Huu Cuong Tran. 2001. "Effectiveness of Internet Filtering Software Products." *CSIRO Mathematical and Information Sciences*. http://pandora.nla.gov.au/pan/53049/20051005-0000/www.aba.gov.au/newspubs/documents/filtereffectiveness.pdf (August 16, 2012).

Ide, Nicolas and Alain Strowel. 2000. "Responsabilité des Intermédiaires: Actualités Législatives et Jurisprudentielles." http://www.droit-technologie.org/2_1.asp?dossier_id=32&motcle=ide+strowel&mode=motamot (August 16, 2012) [in French].

Lee, Timothy B. 2011. "British Telecom Ordered to Blacklist Usenet Search Engine." *Ars Technica*. July 28. http://arstechnica.com/tech-policy/2011/07/british-telecom-ordered-to-blacklist-usenet-search-engine/ (August 16, 2012).

Lievens, Eva. 2010. *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments*. Leiden/Boston: Martinus Nijhoff Publishers.

McIntyre, T.J. and Colin D. Scott. 2008. "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility." In *Regulating Technologies*, ed. Roger Brownsword and Karen Yeung. Oxford: Hart Publishing.

McNamee, Joe. 2010. "Internet Blocking - Crimes Should Be Punished and Not Hidden." *European Digital Rights*. http://www.edri.org/files/blocking_booklet.pdf (August 16, 2012).

Meloni, Michael. 2008. "Denmark's Net Censorship Blacklist Published on WikiLeaks." http://www.somebodythinkofthechildren.com/denmark-net-censorship-blacklist/ (August 16, 2012).

Montéro, Etienne. 2001. "La Responsabilité des Prestataires Intermédiaires sur les Réseaux." In *Le Commerce Electronique Européen sur les Rails?*, ed. Etienne Montéro. Brussel: Bruylant [in French].

Moore, Tyler and Richard Clayton. 2009. "The Impact of Incentives on Notice and Take-down." In *Managing Information Risk and the Economics of Security*, ed. M. Eric Johnson. New York: Springer.

Moses, Asher. 2009. "Leaked Australian Blacklist Reveals Banned Sites." *The Sydney Morning Herald*. March 19. http://www.smh.com.au/articles/2009/03/19/1237054961100.html (August 16, 2012).

Murdoch, Steven J. and Ross Anderson. 2008. "Tools and Technology of Internet Filtering." In *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Deibert, Ronald, John Palfrey, Rafal Rohozinski and Jonathan Zittrain. Cambridge: MIT Press.

The Organization for Security and Co-operation in Europe and Reporters sans Frontières. 2005. "Joint Declaration on Guaranteeing Media Freedom on the Internet." https://www.osce.org/documents/rfm/2005/06/15239_en.pdf (August 16, 2012).

Valcke, Peggy and Marieke Lenaerts. 2010. "Who's Author, Editor and Publisher in User-Generated Content? Applying Traditional Media Concepts to UGC Providers." *International Review of Law, Computers & Technology* 24 (1): 119-131.

Van Buren, Chris. 2008. "Thai Website Blacklist Leaked." *Internet & Democracy Blog*. December 29. https://blogs.law.harvard.edu/idblog/2008/12/29/thai-website-blacklist-leaked/ (August 16, 2012).

Wikileaks. 2008. "797 Domains on Finnish Internet Censorship List, Including Censorship Critic." http://wikileaks.org/wiki/797_domains_on_Finnish_Internet_censorship_list,_including_censorship_critic,_2008 (August 16, 2012).

Wikileaks. 2009. "Norwegian Secret Internet Censorship Blacklist, 3518 Domains." http://www.wikileaks.org/wiki/Norwegian_secret_internet_censorship_blacklist,_3518_domains,_18_Mar_2009 (August 16, 2012).

Zittrain, Jonathan. 2003. "Internet Points of Control." *Boston College Law Review* 44: 653-688.