Title	Blocking child pornography on the internet: European Union developments
Authors(s)	McIntyre, T.J.
Publication date	2010-10-29
Publication information	International Review of Law, Computers and Technology, 24 (3): 209-221
Publisher	Taylor & Francis
Item record/more information	http://hdl.handle.net/10197/10172
Publisher's statement	This is an Accepted Manuscript of an article published by Taylor & Francis in International Review of Law, Computers & Technology on 29 October 2010, available online: http://www.tandfonline.com/10.1080/13600869.2010.522321.
Publisher's version (DOI)	10.1080/13600869.2010.522321

Blocking Child Pornography on the Internet: European Union Developments*

TJ McIntyre[1]

School of Law, University College Dublin, Dublin 4, Ireland

Email: tjmcintyre@ucd.ie

Abstract

Internet blocking has become increasingly common within Europe as a tool to attempt to prevent the distribution of child pornography. However, until recently blocking systems have largely developed independently at a national level. Although there have been European measures against child pornography since 1996 these measures have previously focused on other responses such as the approximation of national laws and the development of hotlines to report illegal content. This, however, is now changing and European Union policy is moving towards greater use of blocking. For example, the Safer Internet Plus Programme has funded the CIRCAMP ('Cospol Internet Related Child Abusive Material Project') police network to promote blocking and the sharing of national blocklists and the Commission is currently proposing legislation which would require all Member States to introduce blocking systems. This article outlines these developments and assesses the implications that they may have for freedom of expression online.

Keywords: child pornography; blocking; freedom of expression

Introduction

The internet has become a significant channel for the distribution of child pornography (or 'child abuse material') but as with other forms of internet content, national responses have often been constrained by territorial limitations. States have found that while they can control what is hosted within their borders, users can turn to material hosted elsewhere, beyond the reach of domestic authorities.[2]

An initial response was to seek increased international cooperation – in particular harmonising national laws and providing for greater sharing of information between law enforcement and industry bodies – with a view to tackling child pornography where it is hosted and reducing the jurisdictions which act as 'safe havens'. This strategy has, however, been only partially successful, and effective international cooperation remains elusive.

---

* This is a post-print version of an article published in (2010) 24(3) *International Review of Law, Computers and Technology* 209-221 and available at http://www.tandfonline.com/doi/abs/10.1080/13600869.2010.522321.

[1] Disclosure: the author is chairman of Digital Rights Ireland, a member organisation of European Digital Rights which is currently lobbying against EU blocking proposals.

[2] For background see Kerry Sheldon and Dennis Howitt, *Sex Offenders and the Internet* (Chichester: Wiley, 2007), chap. 2 and Yaman Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (Aldershot: Ashgate, 2008). For discussion of international cooperation, see in particular Tyler Moore and Richard Clayton, 'The Impact of Incentives on Notice and Take-down' (presented at the Seventh Workshop on the Economics of Information Security (WEIS 2008), Hanover, New Hampshire, 2008), http://weis2008.econinfosec.org/papers/MooreImpact.pdf. It is often argued that the term 'child pornography' is inappropriate and that 'child abuse material' better reflects the harm suffered by children – however, for this article 'child pornography' will be used as reflecting the terminology generally used by European measures.

As a result, European states are increasingly attempting to prevent domestic users from accessing child pornography hosted abroad, by relying on Internet Service Providers (ISPs) to block (or 'filter') access to websites designated by the police or an independent body. These systems have become common within Europe and have been deployed in countries including the United Kingdom, Netherlands and Denmark. They are also currently the subject of controversy in Germany, France and Poland where government plans to introduce blocking have met with substantial resistance from civil liberties groups.[3]

Despite the growth of these systems, until recently they have developed for the most part at a national level with surprisingly little direct European Union involvement. This, however, is now beginning to change. Since 2006 there have been a number of policy initiatives which have moved towards promoting and even requiring EU-wide blocking of illegal content and in particular child pornography.

This article outlines these EU developments and assesses the implications that they may have for freedom of expression.

European Union involvement in blocking

Background

European attempts to stop online child pornography date to 1996 when the Commission adopted the *Communication on Illegal and Harmful Content on the Internet* (COM (96) 487 final) and the *Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services* (COM (96) 483 final), both of which argued that the international nature of the internet would require a coordinated response from Member States.

Both documents, however, recommended a relatively limited European role. Three factors were central to this conclusion. The first was that Member States took very different approaches towards the acceptability of content: even in relation to child pornography national laws differed substantially. This practical difficulty was matched by a second related concern – to ensure that the doctrine of subsidiarity was respected, so that decisions about content would be made at a national level. Third, the Commission stressed the fact that legislative competence in this area was limited.

The response was to differentiate between *illegal* and *harmful* content, and to deal with each separately. As regards content considered *harmful* to children (which required subjective assessment) the Commission recommended the use of (parental or school) filtering software, encouraging content providers to adopt codes of conduct, and supporting national awareness actions for parents and teachers.

In respect of *illegal* content – particularly child pornography – the Commission identified a number of areas where national laws were broadly similar, and urged Member States to harmonise laws in those areas, to co-operate in the enforcement of

[3] For an overview see Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds.), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), 279-366).

existing laws, to establish minimum European standards on criminal content, to clarify the liability of internet service providers, and to encourage self-regulation.

This approach left control of illegal content to Member States and to self-regulation by industry, with responsibility to be allocated at a national level and the European role being facilitative rather than prescriptive. As such, it did not take a stance either for or against blocking or other technical measures but rather left these to the individual Member States.

This approach was subsequently refined from 1999 onwards with the adoption of a series of Safer Internet Programmes funding internet safety initiatives. The first programme ran from 1999 to 2005 and in relation to child pornography its most significant contribution was to fund a series of national hotlines, providing a contact point for users to report illegal content online and for internet service providers (ISP) to be notified of illegal content hosted on their servers. This indirectly facilitated some national blocking schemes – in the UK, for example, the Internet Watch Foundation ('IWF') was able to piggyback on the hotline mechanism to generate its blocklist – but without directly promoting them.

These developments were paralleled in 2000 by the Electronic Commerce Directive (2000/31/EC) which again neither required nor promoted blocking but was drafted to leave it available as a policy option for Member States. This can be seen in particular in Article 12(3) which provides a mere conduit immunity for ISPs but leaves open 'the possibility for a court or administrative authority [to require] the service provider to terminate or prevent an infringement'.

Interestingly, there was one European initiative at around this time which departed from the consensus and did promote blocking – the 2000 Council Decision to Combat Child Pornography on the Internet (2000/375/JHA) recommended that Member States should encourage 'technical means to prevent the distribution of child pornography material'.

However this recommendation did not gain traction. In 2002 the European Parliament unanimously adopted a report on the protection of minors which rejected the use of blocking on the basis that it was largely ineffective, would result in overblocking and represented a threat to freedom of expression. Similarly, the 2004 Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography (2004/68/JHA) made no mention of blocking as a response.[4]

Policy changes towards blocking

The overall European position during this period therefore left blocking as a policy option to Member States but did not promote it directly. However this began to change from 2006 onwards when a number of developments took place which collectively marked a shift in policy towards promoting blocking of child pornography.

[4] See Joris Evers, 'European Parliament says no to Web site blocking,' *Computerworld*, April 12, 2002, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=70115.

The most significant was the publication in 2006 of the Final Evaluation of the 2003-2004 Safer Internet Programme (COM (2006) 663 final). The evaluation, following a survey of stakeholders, argued that blocking had become an essential tool to prevent access to child pornography, and recommended that action should be taken at the European level and a Europe-wide black list of known illegal sites put in place.

This recommendation was accepted by the Commission, which decided that the next Safer Internet Programme would include support for blocking generally and specifically 'activities by hotlines which lead to joint lists of illegal content ... particularly child sexual abuse images'.

Why was this result reached? Although the evaluation document itself does not contain much detail, a number of factors appear to have influenced this outcome.

During the period up to 2006 the number of websites offering child pornography increased significantly. According to the IWF the number of domains hosting child pornography increased from 1,894 in 2004 to 3,077 in 2006. This growth fuelled demands for blocking and also, it has been argued, a moral panic which precluded any critical scrutiny of these demands.[5]

Also, by 2006 national blocking systems had become established in a number of Member States. The experience of those countries fed into European policy making by providing a proof of concept which hitherto had been lacking. (Indeed, two of the members of the evaluation's expert panel – John Carr (UK) and Annethe Ahlenius (Sweden) – had been involved in the introduction of blocking in their respective jurisdictions.) The national systems also appeared to demonstrate (particularly the Cleanfeed system introduced in the UK by British Telecom and the IWF) that more targeted forms of blocking were technologically possible, addressing complaints about overblocking.

Prior concerns about limited legislative competence and differing national laws were also of less importance. The 2004 Framework Decision had substantially aligned national laws, reducing the risk that European action would be inappropriate. In any event, issues of legislative competence were, arguably, less significant when national systems had demonstrated that blocking could be implemented on a self-regulatory and non-legislative basis.

Consequently, it seems that 2006 saw a significant turning point where the factors outlined above promoted the adoption of a new, pro-blocking approach. This reflects the wider international experience described by Villeneuve, who argues that blocking has been 'legitimised' internationally by:

> three interlocking developments: a model of implementation in which the role of the state is reduced, the delinking of filtering and free speech concerns through technological developments, and a reframing of the effectiveness of filtering.[6]

---

[5] For statistics see Internet Watch Foundation, '2006 Annual Report,' 2007, 8. In relation to the 'moral panic' see Mark O'Brien, 'The Witchfinder-General and the Will-o'-the-Wisp: The myth and reality of Internet control,' *Information & Communications Technology Law* 15, no. 3 (October 2006): 259-273.

[6] Nart Villeneuve, 'Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online,' in *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), 62.

European blocking initiatives

From 2006 onwards, therefore, we can identify a number of policy initiatives supported by the EU which promoted blocking. One of the first was the CIRCAMP ('Cospol Internet Related Child Abusive Material Project') Action Plan adopted by the European Police Chief Task Force in 2006. This project, funded under the Safer Internet Plus Programme, assists participating countries in establishing national blocking systems.

This trend was continued in May 2007 with the Commission document 'Towards a general policy on the fight against cyber crime' (COM (2007) 267 final) which argued that:

> A growing number of illegal content sites are accessible in Europe, covering child sexual abuse material, incitement to terrorist acts, illegal glorification of violence, terrorism, racism and xenophobia. Law enforcement action against such sites is extremely difficult, as site owners and administrators are often situated in countries other than the target country, and often outside the EU. The sites can be moved very quickly, also outside the territory of the EU, and the definition of illegality varies considerably from one state to another.

In response that document advocated a policy of promoting 'public-private agreements aiming at the EU-wide blocking of sites containing illegal content, especially child sexual abuse material.'

In March 2009 this approach took a substantial step further when the Commission put forward a Proposal for a Framework Decision on Combating the Sexual Abuse of Children (COM (2009)135 final) which would for the first time require Member States to block access to material online. With the entry into force of the Lisbon Treaty this has now been replaced with a Proposal for a Directive which would require the same result (COM (2010) 94 final).

Assessing European blocking initiatives

The effectiveness of internet blocking is hotly contested. Some advocates, such as Reidenberg, claim that blocking and other technological enforcement mechanisms are necessary to ensure that democratically chosen laws are not negated – others, however, have argued that in practice national blocking systems are ineffective. For example, in a recent study Stol et al. present a strong case that the Dutch child pornography blocking system was adopted without adequate research and with little clarity as to the goal to be achieved, reflecting what they term a 'naive faith in technology'. Indeed, civil rights groups have gone further and argued that blocking is a counter-productive distraction, which according to McNamee offers only 'an illusion of action, reducing pressure for effective policies to be implemented and for the international community to tackle the issue head on.'[7]

---

[7] See Joel R. Reidenberg, 'States and Internet Enforcement,' *University of Ottawa Law & Technology Journal* 1 (2004): 213; Wouter Stol et al., 'Governmental filtering of websites: The Dutch case,' *Computer Law & Security Review* 25 (2009): 251-262; Joe McNamee, 'Pointless action on child pornography,' *The Guardian*, March 29, 2010, http://www.guardian.co.uk/commentisfree/2010/mar/29/blocking-child-abuse-websites-eu.

Leaving aside the issue of effectiveness, however, there is a substantial consensus that blocking systems present particular challenges for fundamental rights – that they are prone to overblocking of legal content, inherently opaque and (especially when implemented on a non-legislative basis) capable of evading constitutional norms associated with the regulation of speech. Consequently, even advocates of blocking have generally conceded that for a system to be legitimate it must be introduced and operated in a manner which addresses these concerns.[8]

The process-oriented analysis taken by Bambauer is representative. He argues that four metrics should be used to evaluate any particular system:[9]

> Openness: does the state admit to filtering the Internet and describe clearly its rationale for the blocking? ...
> Transparency: is the censoring state clear about what material is filtered, and is it specific about the criteria that determine blocking? ...
> Narrowness: how closely does the empirical data about what a state actually blocks match that country's description of its censorship practices? ...
> Accountability: to what degree can citizens influence policymaking on what is censored? What measures or structures push officials to respond to their constituents? What recourse is available to content owners who contend they have been blocked erroneously?

A similar approach was adopted by the Council of Europe in 2008, when the Committee of Ministers issued a Recommendation on measures to promote respect for freedom of expression and information with regard to internet filters (CM/Rec(2008)6). That document identified the threats which filtering or blocking may pose to freedom of expression and recommended that this technology should be used only when it is necessary and effective to achieve a particular goal and subject to a number of safeguards:

> Users' awareness, understanding of and ability to effectively use Internet filters are key factors which enable them to fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information, and to participate actively in democratic processes…
>
> Users must be informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering the content they access is subject to…
>
> Users should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies…
>
> [States should] guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and

[8] On this point see e.g. TJ McIntyre and Colin Scott, 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility,' in *Regulating Technologies*, ed. Roger Brownsword and Karen Yeung (Oxford: Hart Publishing, 2008); Ian Brown, 'Internet filtering – be careful what you ask for,' in *Freedom and Prejudice: Approaches to Media and Culture*, ed Süheyla Kirca Schroeder and LuEtt Hanson (Istanbul: Bahcesehir University Press); Lilian Edwards, 'Pornography, Censorship and the Internet,' in *Law and the Internet*, ed. Lilian Edwards and Charlotte Waelde, 3rd ed. (Oxford: Hart Publishing, 2009).

[9] Derek Bambauer, 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering,' *SSRN eLibrary* (2008): 12-24, http://ssrn.com/paper=1143582.

> impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;
>
> [States should] provide for effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where users and/or authors of content claim that content has been blocked unreasonably.

If we take these approaches as our starting point, how might EU initiatives fare when examined more closely? In the following sections the CIRCAMP blocking project and the proposed Framework Decision/Directive will be assessed against these norms.

CIRCAMP

The CIRCAMP project involves law enforcement agencies from 16 countries as well as INTERPOL and EUROPOL, is led by Norway and the UK and aims to facilitate member countries in introducing a type of blocking termed the Child Sexual Abuse Anti Distribution Filter ('CSAADF'). At the time of writing, six (Denmark, Finland, Italy, Malta, Norway and Sweden) have done so. The CSAADF, which is based on Norwegian practice, operates as follows:

> The police are responsible for confirming the illegality of the domain and to provide the addresses containing child abuse material. The Internet Service Providers (ISP) implements the access blocking in their networks, utilizing existing technology, personnel and equipment. All domains are downloaded by the police, seized, traced, looked up, saved and rechecked at predetermined intervals. Only police officers handle illegal material, as it is considered evidence of a crime, and shared between the participating law enforcement agencies.[10]

As this description suggests, the system is police-led – each national police force is responsible for the decision that material is illegal in their jurisdiction and should be blocked. (There is no EU-wide blocklist, though CIRCAMP is working on developing an international 'worst-of' list for material which would be illegal in almost all jurisdictions.) In this it differs substantially from other national schemes such as the UK IWF model which are industry-led and where material is assessed by a body which is – formally at least – independent of the state.

Legislative basis

Whether or not there is legislation permitting or requiring a blocking system to be put in place is a matter for the individual state. For the most part the states which have implemented this system have not legislated for it and rely on voluntary agreements between the police and ISPs – although these 'voluntary' agreements have generally been in response to substantial state pressure.

---

[10] The discussion of CIRCAMP is based for the most part on material from the CIRCAMP website itself, and all quotes are taken from that site. See in particular: 'CIRCAMP overview,' *CIRCAMP*, n.d., http://circamp.eu/index.php?option=com_content&view=article&id=11:circamp-overview&catid=1:project&Itemid=2 and 'CIRCAMP fact sheet english,' *CIRCAMP*, n.d., http://circamp.eu/index.php?option=com_content&view=article&id=15:circamp-fact-sheet-english&catid=1:project&Itemid=2. EUROPOL's involvement is described at 'Funnel Web Introduction,' *EUROPOL*, n.d., http://www.europol.europa.eu/index.asp?page=FunnelIntro&language=. For funding details see 'Projects: CIRCAMP,' *Europa - Information Society*, May 15, 2009, http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2007-TN-140701.

This approach, although common in most national implementations of blocking, presents difficult questions of freedom of expression. Where blocking is carried out by ISPs on a non-legislative basis in response to government pressure then this is likely to violate Article 10 of the European Convention on Human Rights (EHCR). Article 10 requires restrictions on the right to freedom of expression to be 'prescribed by law' – which requires a legal basis which is adequately accessible to the citizen. In the case of industry-led approaches it might be argued that no direct state action is involved and therefore Article 10 is not implicated: this argument cannot be made, however, in relation to the CIRCAMP police-led systems.

Indeed, the European Commission itself has recently made precisely this point, stating in the Impact Assessment for the proposed Framework Decision that filtering systems which lack a legislative basis are likely to breach Article 10:

> [E]ncouragement of self regulation by ISPs to block access to Internet pages containing child pornography would involve interference in the right to freedom of expression in Article 10 ECHR (Article 11 of the EU Charter). In accordance with the ECHR, again, as interpreted by the European Court of Human Rights in Strasbourg, to respect fundamental rights such interference needs to be prescribed by law and be necessary in a democratic society for important interests, such as the prevention of crime... More problematic may be the compliance with the requirement that the interference in this fundamental right must be 'prescribed by law', which implies that a valid legal basis in domestic law must exist. This may not always be present in a system based exclusively on self-regulation, and therefore this measure risks to amount to a non legitimate interference with fundamental rights. (at 30)

It is somewhat ironic, therefore, that the Commission is via CIRCAMP funding a project the implementation of which it has elsewhere described as possibly incompatible with the ECHR.

DNS blocking

A significant feature of the CSAADF is that it promotes DNS based blocking rather than more accurate URL based blocking. This appeals to industry as being comparatively cheap and easy to implement but also causes substantial collateral damage in the form of overblocking.

For example, if a single offending image is hosted at the (fictional) address http://www.example.com/users/johndoe/abuseimage.jpg then hybrid URL blocking should block that individual image while DNS blocking will instead block access to everything hosted at http://www.example.com/ – which may and often will include very large quantities of material entirely unconnected with the image or user. In addition, experience shows that the implementation of DNS blocking can result in other side effects such as the redirection of email.[11]

For these reasons DNS blocking has generally been rejected by most commentators. The CIRCAMP project, on the other hand, makes a virtue of this overblocking by

[11] This is discussed in the context of German judicial blocking orders by Maximilian Dornseif, 'Government mandated blocking of foreign Web content,' in *Security, E-Learning, E-Services: Proceedings of the 17 EDFN-Arbeitstagung über Kommunikationsnetze*, ed. J von Knop, W Haverkamp, and E Jessen, Lecture Notes in Informatics (Dusseldorf: Gesellschaft für Informatik, 2003), http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf.

treating it as a means of incentivising the domain owner to police their domain, and states that this will 'motivate content providers to actively make an effort to avoid files with child sexual abuse on their systems/services'.

It is, however, difficult to see how this intentional overblocking – which will almost certainly impact on innocent users – can be reconciled with the requirement under Article 10 that an interference with freedom of expression should be proportionate. Also, by aiming to motivate hosts to actively police content on their servers it raises questions as to whether it is compatible with either the letter or the spirit of article 15 of the Electronic Commerce Directive which prevents Member States from imposing a general obligation to monitor on providers.

Procedural safeguards

How does the system fare in relation to procedural safeguards? On the positive side, the CSAADF system does build in important elements of transparency and accountability – in particular, it ensures that users who try to view a page are notified via a 'stop page' that access has been blocked, why, and how this might be challenged, including links to national legislation and contact information to complain about the blocking. This stop page is also intended to serve the effect of deterring some users and reminding them that the internet is being policed.

Although there does not appear to be any system in place to notify content owners that they have been blocked, there is a mechanism – run by EUROPOL – which operates as a single point of contact allowing owners of domains to request a revision of the block in all participating states. This mechanism is, however, available only to the registrant of the blocked domain. Consequently other affected parties – such as users or the authors of blocked material – will only be able to complain by contacting each national police force individually.

One significant concern is that the national review mechanisms envisaged by CIRCAMP are internal to the police only. There is no requirement for any independent or judicial review of the decision to block. However, in light of the Council of Europe Recommendation it would seem that if a national system does not provide for a review by 'an independent and impartial tribunal or regulatory body' then it may be incompatible with Article 6 of the ECHR.

Blocking of domestic sites

Another concern with the CIRCAMP model is that it appears to depart from the fundamental rationale for blocking – that it is necessary to deal with sites which are beyond the reach of national law – by allowing for the blocking of domestic sites also. This has been particularly controversial in Finland where a critic of the blocking system has found his own website blocked (for linking to sites which he claims have been wrongfully blocklisted) despite the fact that his site is hosted locally and a criminal investigation resulted in no charges against him. It is hard to see how the use

of blocking can be justified in a situation such as this where the national criminal justice system can act.[12]

Effectiveness

The CIRCAMP / CSAADF project is intended to block access to child pornography, minimise the re-victimisation of children, stop the illegal distribution of files, reduce harm to the general population and limit the market for new child pornography material. Unfortunately it seems likely that it will achieve these goals only to a limited degree.

The CSAADF applies to distribution of child pornography via the web only. Other forms of online distribution – via USENET, IRC, p2p, shared webmail accounts, Freenet, instant messaging, email, etc. are left unaffected. Consequently, even if it were entirely technically successful the system could at best affect only one particular channel of communication – albeit the most publicly visible and easily accessible channel. Even in relation to the web, however, the DNS system used is straightforward to evade and indeed has been described by critics as the easiest form of blocking to circumvent.

CIRCAMP itself acknowledges that the blocking can be evaded, but argues in response that the block will still be effective for 'those not technically skilled enough', that it may have a deterrent effect on those encountering a block page and that it will prevent accidental viewing of child pornography. This reflects a common fallback argument that blocking – even if easily evaded – can stop the casual offender, help to 'save men from themselves' and prevent a latent interest in child pornography from being developed further.

While this argument is certainly plausible there does not seem to be any research demonstrating that this is in fact the case or that accidental exposure to child pornography is a significant problem. Some studies suggest that viewing of online child pornography may create or reinforce a sexual interest in children – however these studies generally focus on deliberate viewing and consider accidental exposure only tangentially if at all. There is little research on the extent of accidental exposure, but if reports to national hotlines are used as a rough proxy then it would appear to be falling. The Irish hotline, for example, has stated in its 2010 Annual Report that 'Internet users are encountering illegal content on the Internet less often than in the previous two years'. Also, perhaps more significantly, the weaker nature of this justification and its inherent admission that blocking is at best only partially effective makes it more difficult to argue that this form of blocking (and the collateral damage it entails) is a necessary and proportionate response.[13]

---

[12] Dan Goodin, 'Finland censors anti-censorship site,' *The Register*, February 18, 2008, http://www.theregister.co.uk/2008/02/18/finnish_policy_censor_activist/; Matti Nikki, 'Lapsiporno.info and Finnish censorship,' *Lapisporno.info*, July 20, 2009, http://lapsiporno.info/english-2008-02-15.html.

[13] On the 'latent interest' point see e.g. Barry Collins, 'Charity: child abuse filters save men from themselves,' *PC Pro*, February 23, 2009, http://www.pcpro.co.uk/news/248117/charity-child-abuse-filters-save-men-from-themselves/print. On the ease of evading DNS systems see Cormac Callanan et al., *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublin: Aconite Internet Solutions, 2009), 126. For studies on exposure to child pornography and subsequent offending see in particular Michael Bourke and Andres Hernandez, 'The 'Butner Study' Redux: A Report of the

Impact of the Telecoms Package?

There may also be issues presented for CIRCAMP by the new end-user rights created by the Telecoms Reform Package Directive (2009/140/EC). Although adopted with 'three strikes' laws in mind, Laidlaw has suggested that these rights may be wide enough to cover national blocking systems also.[14]

The relevant provision is paragraph 3a which provides:

> Measures taken by Member States regarding end-users' access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons...
>
> Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards... including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency... The right to effective and timely judicial review shall be guaranteed.

On the face of it, a national system which blocks access to particular websites or pages would appear to be a measure 'regarding end-users' access to, or use of, services and applications' which is 'liable to restrict... fundamental rights' and therefore subject to this provision. If this view is correct, then police-led systems such as CIRCAMP (though possibly not industry-led systems, which might not constitute 'measures taken by Member States') would be obliged to introduce a right to be heard in relation to blocking decisions, along with a right to judicial review thereafter.

It seems reasonably clear, however, that this was not an intended result of the Telecoms Package, making this interpretation somewhat speculative and its implications still unclear. It is likely that certainty on this point will only be reached once the Directive comes into force and this point is considered either by the Commission (in the context of infringement proceedings) or the courts.

Proposed Framework Decision / Directive

Legislative or self-regulatory blocking?

Incidence of Hands-on Child Victimization by Child Pornography Offenders,' *Journal of Family Violence* 24, no. 3 (April 1, 2009): 183-191 and Diana E.H. Russell and Natalie J. Purcell, 'Exposure to pornography as a cause of child sexual victimization,' in *Handbook of Children, Culture, and Violence*, ed. Nancy E. Dowd, Dorothy G. Singer, and Robin Fretwell Wilson (London: Sage, 2005), 59–84. Irish statistics are available at Internet Service Providers Association of Ireland, 'Hotline.ie Annual Report 2010: Analysis of 2009 Reports: Trends,' 2010, http://www.hotline.ie/report2010/2009-anlsys/trends.html.

[14] See Emily Laidlaw, 'Internet Freedom Provision subject IWF to ECHR principles?,' *laidlaw.eu*, March 17, 2010, http://www.laidlaw.eu/2010/03/internet-freedom-provision-subject-iwf-to-echr-principles/.

The Commission's March 2009 Proposal for a Framework Decision included in Article 18 a provision requiring Member States to introduce blocking:

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

The reference to 'measures to enable the competent judicial or police authorities' was significant, reflecting the conclusion in the Impact Assessment that self-regulatory systems would not be 'prescribed by law' as required by Article 10 of the ECHR. Consequently the proposed Framework Decision rejected purely self-regulatory systems as an option and required that the decision to order blocking should rest with public bodies.

This, however, met with resistance from some national governments who feared that it would require existing national systems to be placed on a legislative basis, affecting industry-led schemes such as the UK IWF and possibly also non-legislative police-led schemes.[15]

After the Lisbon Treaty came into force (doing away with the framework decision mechanism) it became necessary to recast the proposal as a directive. Significantly, when this was done the relevant provision was amended in light of national resistance by deleting any reference to police or judicial authorities. It now provides in Article 21 that:

> Member States shall take the necessary measures to obtain the blocking of access by Internet users in their territory to Internet pages containing or disseminating child pornography...

The implications of this change are spelled out in the new Recital 13 which makes it clear that Member States no longer have to adopt legislation but can comply by merely 'supporting and stimulating Internet Service Providers on a voluntary basis to develop codes of conduct and guidelines for blocking access to such Internet pages'.

This change is open to criticism, however, in that the fundamental rights concerns expressed in the Impact Assessment appear to have been sidestepped in order to ensure that existing national schemes can continue unchanged.

Significantly, similar criticism has been expressed by the European Data Protection Supervisor in a May 2010 Opinion on the proposed Directive. That Opinion indicated 'strong doubts about the legal certainty of any blocking operated by private parties' together with concerns about 'possible blocklisting of individuals and their possibilities of redress before an independent authority' and the data protection implications of 'the monitoring of individuals by private sector actors... in areas that are in principle under the competence of law enforcement authorities'. Consequently, the view of the Data Protection Supervisor is that self-regulation is not appropriate

[15] Joe McNamee, 'Controversial draft Framework Decision on Child Sexual Exploitation,' *EDRi: European Digital Rights,* October 7, 2009, http://www.edri.org/edrigram/number7.19/draft-framework-decision-child-exploatation.

and that ‘a code of conduct or voluntary guidelines would not bring enough legal certainty in this respect’.

Compatibility with the Interinstitutional Agreement on Better Law Making

As revised, the proposal also appears to conflict with the 2003 Interinstitutional Agreement on Better Law Making. In article 17 of that agreement the institutions undertake not to use self- or co-regulation as a policy instrument where to do so may undermine transparency or the protection of fundamental rights:

> The Commission will ensure that any use of co-regulation or self-regulation is always consistent with Community law and that it meets the criteria of transparency (in particular the publicising of agreements) and representativeness of the parties involved. It must also represent added value for the general interest. These mechanisms will not be applicable where fundamental rights or important political options are at stake or in situations where the rules must be applied in a uniform fashion in all Member States.

In this case, it is clear – as the Commission’s own Impact Assessment acknowledges – that blocking implicates fundamental rights and in particular Article 10 ECHR. Despite this, however, the proposal does not make any reference to the Interinstitutional Agreement or explain why the use of self- or co-regulation is justified in this case.

This is a particularly significant omission when it is clear that some existing national schemes fall well short of meeting basic standards of legitimacy, transparency and compliance with fundamental rights. (Stol et al., for example, have found after a comprehensive review that Dutch blocking practice lacks a specific legal basis and is unlawful.) In light of this, a proposal which encourages reliance on those national schemes does not appear to meet the Commission’s duties under the Interinstitutional Agreement.

Implications for national blocking systems

The rather vague wording used presents some problems in trying to assess this proposal. For example, it is not clear what is meant by ‘internet pages’ – should this be taken to include web pages, individual image files, or Usenet posts? ‘Adequate safeguards’ and the ‘possibility of challenging’ a block are left largely undefined – it is not clear whether, for example, these would include requirements for independent oversight or the right to a judicial or independent review. Similarly, the proposal does not explain what is meant by blocking being ‘limited to what is necessary’ – a standard which if taken literally would fundamentally disrupt many national systems and the CIRCAMP project by requiring the use of URL filtering rather than DNS blocking.

On the other hand, in some jurisdictions even the core elements of the proposal would require a change in national practices. In the UK, for example, some of the safeguards proposed – particularly blocking being limited to what is necessary, users being informed of the reason for a block and content providers being informed of a right to challenge a block – would go substantially beyond what is currently required by the IWF.

Conclusion

This article has reviewed EU developments in relation to blocking of child pornography in light of the requirements for legitimacy identified by Bambauer and the Council of Europe Recommendation on measures to promote respect for freedom of expression and information with regard to internet filters.

Given the increased use of internet blocking systems at national level – and increasing criticisms of such systems – one might hope that interventions at European level would help to promote good governance and respect for fundamental rights in this context. At the moment, however, this hope does not appear to be realised. At a basic level, it is remarkable that the Commission has put forward a proposal to encourage the use of self-regulatory blocking systems which it had previously found to be incompatible with the ECHR. Similarly, while both the CIRCAMP system and the proposed Directive do incorporate some welcome procedural safeguards neither would meet the standards set by the Council of Europe Recommendation. Consequently it seems that current EU developments leave safeguards for fundamental rights to be built in, if at all, at a national level only.

Questions of governance and fundamental rights are not, of course, unique to blocking. It has long been argued that the European policy preference for self-regulation of internet content creates a structural tendency towards unseen and unaccountable censorship, excluding public oversight and accountability.[16] Current EU policies in relation to blocking, however, rather than addressing these criticisms seem set to add to them.

Acknowledgement

I would like to thank Ian Brown and Joe McNamee for their helpful comments. The usual disclaimer applies.

[16] See e.g. Louise Cooke, 'Controlling the Net: European approaches to content and access regulation,' *Journal of Information Science*, 33, no. 3 (2007): 360-376; Yaman Akdeniz, 'To block or not to block: European approaches to content regulation, and implications for freedom of expression,' *Computer Law & Security Review* 26, no. 3 (2010): 262-263.