

BILETA 2008, Glasgow Caledonian University, 27-28 March 2008

Intermediaries, Invisibility and the Rule of Law

TJ McIntyre

Lecturer in Law, University College Dublin

Email: tjmcintyre@ucd.ie

Abstract

The growth of the Internet has been matched by a corresponding growth in Internet regulation. Various strategies have been adopted by regulators – domestic law has been matched by international agreements, litigation has been complemented by legislation, and various forms of self- and co-regulation have proliferated, often in an attempt to fend off more direct state intervention.

One of the most significant aspects of this regulation has been an increasing focus on the intermediary rather than the end-user. For example, defamation plaintiffs have taken to targeting hosts, the music industry has aimed at peer to peer networks, and governments worldwide have compelled ISPs to filter user access to objectionable materials. In each case, the intermediary may take on the role of a gatekeeper to control the actions of their users.

It may well be that certain type of activities can only effectively be regulated by enlisting intermediaries. However, the regulatory regimes which result give rise to some concern.

The way in which intermediaries may be required to take on a gatekeeper function is often opaque – particularly where governments threaten intermediaries with legislation should they fail to adopt voluntary self-regulation, or where the threat of litigation compels intermediaries to change their practices. The result may be that rules governing the behaviour of internet users are being created outside the legislative process and with little public scrutiny. The content of the rules applied by intermediaries and the manner in which those rules are imposed may also be unclear. For example, in the case of internet filtering site owners may not be notified that their site has been blacklisted, nor given an opportunity to appeal against that determination. In addition, the incentives which intermediaries face suggest that their application of these rules may be systematically biased towards more speech restrictive outcomes. Finally, the actions of private sector intermediaries may be insulated from any judicial review, even where they are implementing what are in effect rules devised and mandated by governments.

One recently introduced form of “regulation by intermediary” – the UK “Cleanfeed” system for blocking child pornography – offers an opportunity to consider to what extent these concerns are implicated.

Introduction: From cyber-libertarianism to cyber-paternalism

One of the earliest promises of the internet was that it would lead to disintermediation.¹ By cutting out the middlemen, so the argument went, the Internet would not only cut the cost of distributing information and empower the citizen, but also eliminate or at least minimise the mechanisms controlling or preventing access to information.² No longer would the ability to reach a mass audience be mediated through the newspaper editor or television producer – instead, anyone with a PC and internet connection could potentially be heard worldwide.

This was matched by the argument, most famously expressed by Johnson and Post, that the structure of the internet was inherently resistant to censorship, so that attempts by states to control online activities would easily be circumvented by regulatory arbitrage.³

Together, these two arguments provided the underpinning for the cyber-libertarian view which was not that the internet would not be governed, but rather that internet governance would be non-geographic and decentralised, characterised by schemes drawn up and administered by internet users themselves rather than imposed by governmental and hierarchical controls. This view reached its zenith in John Perry Barlow's 1996 Declaration of Independence of Cyberspace⁴:

“Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions...

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.”

This cyber-libertarian utopia didn't prove to be an entirely accurate prediction. The cyber-paternalists, writing in response, identified several reasons why.⁵ Two are particularly important.

¹ See, for example, R. Gellman, “Disintermediation and the Internet” (1996) 13(1) *Government Information Quarterly* 1.

² A. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World* (New York, 1999). For an interesting counterpoint see Clarke, R., “Freedom of Information? The Internet as Harbinger of the New Dark Ages” (1999) 4(11) *First Monday*, available at http://firstmonday.org/issues/issue4_11/clarke/. Clarke suggests that disintermediation may ultimately restrict the freedom of information by encouraging a shift from copyright to contractual restrictions on the use of information, with a possible knock on effect of undermining anonymous and pseudonymous access.

³ D. Johnson, and D. Post, “Law and Borders – The Rise of Law in Cyberspace” (1996) 48 *Stanford Law Review* 1367 (1996).

⁴ Available at <http://homes.eff.org/~barlow/Declaration-Final.html>.

⁵ The cyber-libertarian and cyber-paternalist debate is summarised in Murray, “The regulatory edge of the Internet” (2003) 11(1) *International Journal of Information Technology* 87.

The first, most associated with Lessig, stresses the role of code or architecture as a means of regulation.⁶ He notes that while the first generation of the internet may have been structured in such a way as to provide for anonymous speech, decentralised distribution and the use of encryption, there is no guarantee that this structure will remain. Already, he argues, the architecture is being remade under the influence of governments in a way which will reinstate control.⁷

The second, articulated by Boyle⁸ and Swire⁹, rejects the argument that the decentralised and international nature of the internet makes it difficult or impossible to regulate the conduct of users who may be anonymous or whose location might be uncertain. Instead, they argue, regulators can simply resort to indirect enforcement, targeting intermediaries rather than end users, “elephants” rather than “mice”. For example, Boyle suggested that the state might target ISPs, pressuring or requiring them to “prevent copyright infringement through technical surveillance, tagging and so on”.¹⁰

This argument relies on the fact that the promise of disintermediation was somewhat oversold – while the internet has certainly resulted in some disintermediation, it has also involved the creation of entirely new intermediaries, who often enjoy greater technical and legal capacity to control the actions of their users. For example, as compared with the post office an ISP or webmail provider will enjoy a greater technical capability to screen communications, and may be exempt from older laws prohibiting this. Consequently, the ISP, search engine, hosting provider and others have become the new “Internet points of control”.¹¹ In the most recent example of this trend, software authors have been targeted as a new class of intermediary, with regulators seeking to compel them to build in mechanisms of control which would allow networked software to be remotely rewritten or even to disable other software on a user’s PC.¹²

Implications of intermediaries and architecture

These two tactics – a focus on intermediaries and regulation by architecture – have undoubted pluses. They have been endorsed by those who see them as essential for maintaining effective government by the state and, more specifically, replicating offline powers in the online world. Reidenberg, for example, argues that:

“The failure of a democratic state to use these powers to enforce policies and decisions adopted by the democracy is, in effect, an abdication of the responsibilities of the state.”¹³

⁶ L. Lessig, *Code and Other Laws of Cyberspace* (Cambridge: MA, 1999).

⁷ L. Lessig, *Code Version 2.0* (New York, 2006), at 236-237.

⁸ J. Boyle, “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors” (1997) 66 *University of Cincinnati Law Review* 177.

⁹ P. Swire, “Of Elephants, Mice, and Privacy: International Choice of Law and the Internet” (August 1998). Available at SSRN: <http://ssrn.com/abstract=121277>.

¹⁰ J. Boyle, “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors” (1997) 66 *University of Cincinnati Law Review* 177 at 197.

¹¹ J. Zittrain, “Internet Points of Control” (2003) 43 *Boston College Law Review* 1.

¹² J. Zittrain, “A History of Online Gatekeeping” (2006) 19(2) *Harvard Journal of Law and Technology* 253; J. Zittrain, *The Future of the Internet – And How to Stop It* (New Haven, 2008).

¹³ J. Reidenberg, “States and Internet Enforcement” (2003) *University of Ottawa Law and Technology Journal* 213 at 216.

Zittrain makes a similar point:

“[G]overnment mandated destination-based filtering stands the greatest chance of approximating the legal and practical frameworks by which sovereigns currently sanction illegal content apart from the Internet.”¹⁴

Moves towards internet regulation implemented by intermediaries also often take the form of self-regulation.¹⁵ As such, they may offer many of the attractions of self-regulation for regulators and regulated alike, with (amongst other things) the possibility of minimising enforcement costs, achieving a flexible and “light touch” regulatory regime and (for the industry) warding off more intrusive government regulation.¹⁶

However, there have also been concerns that these tactics may go too far. In particular, rather than simply replicating the norms of the offline world, intermediary and technology based regulation (notably internet filtering¹⁷) may enable governments to avoid the constitutional and institutional constraints which would otherwise restrict their actions.¹⁸

Transparency in introducing regulation

The first area of concern relates to situations in which intermediaries may be compelled by the state to take on a gatekeeper function.¹⁹ Where that function affects a fundamental right – such as freedom of expression or privacy – one might hope that this would be done by primary legislation following a full public debate, or at a minimum following an open public debate in a way which makes clear what restrictions are imposed. This would, for example, be required by article 10 of the European Convention on Human Rights which provides that restrictions on the exercise of the right to freedom of expression should be “prescribed by law” – a phrase which the European Court of Human Rights has held requires that the law must be adequately accessible to the citizen, and formulated with sufficient precision to enable the citizen to regulate his conduct.²⁰

¹⁴ J. Zittrain, “Internet Points of Control” (2003) 43 *Boston College Law Review* 1.

¹⁵ For examples and discussion of the difficulty of defining “self regulation” in the context of the internet, see B. Koops, M. Lips, S. Nouwt, C. Prins and M. Schellekens, “Should self-regulation be the starting point?” in B. Koops, M. Lips, C. Prins and M. Schellekens (eds.), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (The Hague, 2006); M. Price and S. Verhulst, *Self Regulation and the Internet* (The Hague, 2005) Ch. 1; and D. Tambini, D. Leonardi and C. Marsden, *Codifying Cyberspace: Communications self-regulation in the age of Internet convergence* (London, 2008) Chs. 2 and 6.

¹⁶ These advantages are discussed in B. Koops, M. Lips, S. Nouwt, C. Prins and M. Schellekens, “Should self-regulation be the starting point?” in B. Koops, M. Lips, C. Prins and M. Schellekens (eds.), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (The Hague, 2006).

¹⁷ T.J. McIntyre and C. Scott, “Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility” in R. Brownsword and K. Yeung (eds.), *Regulating Technologies* (Oxford, 2008). Though filtering need not necessarily be implemented by intermediaries – as where a user runs a spam filter on their own machine – in practice it generally is.

¹⁸ See e.g. M. Price and S. Verhulst, *Self Regulation and the Internet* (The Hague, 2005) Ch. 1; D. Tambini, D. Leonardi and C. Marsden, *Codifying Cyberspace: Communications self-regulation in the age of Internet convergence* (London, 2008), Ch. 11.

¹⁹ This will include what Price and Verhulst have described as “mandated” or “coerced” self-regulation: M. Price and S. Verhulst, *Self Regulation and the Internet* (The Hague, 2005) at 11-13.

²⁰ *Sunday Times v. The United Kingdom* (1979) 2 EHRR 245.

Some gatekeeper functions do address these considerations – for example, the ill-fated 2002 Pennsylvania law requiring ISPs to block access to child pornography was passed as primary legislation at the state level.²¹ Deibert and Villeneuve, however, have found that more often internet gatekeeping is being implemented in an opaque way and without legislative underpinning:

“as the practice of Internet content filtering and surveillance is largely new territory, the rules by which states implement such controls are poorly defined, not well known among the general public, and very rarely subject to open debate ... as it stands now such decisions are typically taken behind closed doors through administrative fiat”.²²

A well known example (one cited approvingly by Reidenberg²³) is the way in which then New York Attorney General Eliot Spitzer tackled online gambling – by threatening payment intermediaries (banks issuing credit cards and PayPal) with criminal prosecutions unless they agreed to refuse all transactions identified as associated with Internet gaming – whether or not the customer was located in New York State, and despite the strong argument that there was no breach of the law in simply providing general purpose credit. It may well be the case that the potential reputational damage of being prosecuted – irrespective of the outcome – cowed the intermediaries.²⁴ While certainly effective, we might question the legitimacy of this tactic – particularly since it pre-empted the legislative process, as Congress was then considering various proposals which would for the first time have introduced a clear legislative basis for prohibiting payment intermediaries from processing payments.²⁵

A more topical example is the recent attempt by the music industry (via litigation in Belgium²⁶ and now Ireland²⁷) to compel ISPs to screen users’ connections to prevent the illegal downloading and sharing of music via peer to peer systems. (This of course follows the ruling in *Grokster* which may impose such a duty on software authors also.²⁸) Whether or not one agrees that this is necessary or desirable, it is striking that policy in this area is in effect being made by litigation rather than the legislative process, particularly as this might be seen as undermining the legislative balance struck by the Electronic Commerce Directive²⁹ which prevents the imposition of a general duty to monitor. In addition, there is a risk that the privacy interests of users (who are not party to these actions) will be neglected as ISP defendants will, understandably, focus on defending their own commercial interests.

²¹ Outlined in J. Zittrain, “Internet Points of Control” (2003) 43 *Boston College Law Review* 1.

²² R. Deibert and N. Villeneuve, “Firewalls and Power: An Overview of Global State Censorship of the Internet” in M. Klang and A. Murray (eds.), *Human Rights in the Digital Age* (London, 2005) at 123.

²³ J. Reidenberg, “States and Internet Enforcement” (2003) *University of Ottawa Law and Technology Journal* 213.

²⁴ C. Scott, “Innovation in the regulation of online gambling” in J. Black, M. Lodge and M. Thatcher (eds.), *Regulatory Innovation: A Comparative Analysis* (Cheltenham, 2005).

²⁵ For background see J. Gottfried, “The Federal Framework for Internet Gambling” (2004) 10(3) *Richmond Journal of Law and Technology* 26, available at <http://law.richmond.edu/jolt/v10i3/article26.pdf>, at paras. 82-91.

²⁶ *Sabam v. S.A. Tiscali (Scarlet)*, District Court of Brussels, No. 04/8975/A, Decision of 29 June 2007.

²⁷ T.J. McIntyre, “Ireland: Music industry sues ISP, demands filtering” EDRI-gram No. 6.5, 12 March 2008, available at <http://www.edri.org/edrigram/number6.5/ireland-isp-filtering>.

²⁸ P. Samuelson, “Legally Speaking: Did MGM Really Win the Grokster Case?” (2005) 48 *Communications of the Association for Computing Machinery* 19.

²⁹ Directive 2000/31/EC.

Evading public law norms

Another concern is that the delegation of functions to private entities means that public law norms may be undermined. One prominent example from the offline world is the way in which United Kingdom legislation³⁰ has effectively outsourced immigration functions to airlines, thus allowing the United Kingdom to evade its international obligations towards refugees (preventing, for example, refugees from exercising their right to seek asylum even where they have no documentation).³¹

This concern is equally applicable in relation to internet regulation by intermediary. For example, Boyle has suggested that by requiring ISPs to prevent copyrighted material from being transmitted, governments (or the music industry) might achieve:

“freedom from some of the constitutional and other restraints that would burden the state were it to act directly. Intrusions into privacy, automatic scrutiny of e-mail, curtailing of fair use rights so as to make sure that no illicit content was being carried; all of these would occur in the private realm, far from the scrutiny of public law.”³²

Fair procedures

One particular public law norm that may be jeopardised is the right to fair procedures – in particular, the right to be notified and given the opportunity to make submissions before a decision affecting you is made. This is not, it would seem, a facility which has been offered to site owners or users in most internet filtering schemes worldwide, despite the fact that the outcome of filtering may in effect be an “internet death penalty” – at best, the operators of internet filters may provide for review after the fact.³³

On the related issue of the separation of powers, it is often the case that the intermediary simultaneously acts as lawmaker (drawing up standards), judge (deciding on particular cases) and executive (enforcing their decision). When in some jurisdictions, such as Finland, the role of deciding what sites to block is vested in the police³⁴ there is still a notable absence of any judicial or quasi-judicial determination before the decision to block is made or any formal judicial appeal mechanism thereafter.

Transparency in application

³⁰ Commencing with the Immigration (Carriers' Liability) Act 1987.

³¹ A. Ruff, “The Immigration (Carriers' Liability) Act 1987: its Implications for Refugees and Airlines” (1989) 1(4) *International Journal of Refugee Law* 481.

³² J. Boyle, “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors” (1997) 66 *University of Cincinnati Law Review* 177 at 197-198.

³³ N. Villeneuve, “The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace” (2006) 11(1) *First Monday*. Available at http://firstmonday.org/issues/issue11_1/villeneuve/index.html; R. Deibert and N. Villeneuve, “Firewalls and Power: An Overview of Global State Censorship of the Internet” in M. Klang and A. Murray (eds.), *Human Rights in the Digital Age* (London, 2005) p. 114.

³⁴ See <http://www.ffi.org/blog/kai-2008-02-18.html> which outlines the role of the Finnish National Bureau of Investigation in drawing up a secret list of foreign sites found to be distributing child pornography.

Another public law norm which may suffer is the principle of decisions being made in a manner which is based on accessible norms and those decisions being presumptively public. In the case of actions by intermediaries, users may not be aware that a gatekeeping role has been adopted, much less that any particular action has been taken. For example, in the case of internet filtering, users may be entirely unaware that an ISP has adopted any filtering system³⁵, much less that a particular site has been blacklisted. Even if a user finds their access to a particular site blocked, it is common for filtering systems to deceive users, by presenting error pages rather than specifying that a site has been deliberately blocked.³⁶ According to Villeneuve, this is often “an attempt to deflect criticism, allowing the authorities to claim that they are not censoring Internet content”.³⁷ This is exacerbated by a tendency on the part of commercial providers of filters to claim that their criteria for filtering, blacklist and technical details of the operation of their software are commercially sensitive and thus should not be disclosed – to the point where they have sometimes threatened researchers with litigation.³⁸

Intermediaries and incentives

Another concern is that the incentives faced by intermediaries may lead them to make decisions in a way which is systematically biased towards a particular outcome. It is clear, for example, that the imposition of knowledge based liability has led to a takedown first, ask questions later (or not at all) approach from hosts in Europe – something that was neatly exemplified by Ahlert’s “mystery shopper” project³⁹:

“This consisted of a complaint to an ISP about alleged copyright infringement on a website that actually contained perfectly legal material. One website was set up with one of the most established US ISPs, and another with a major UK-based ISP. The identity of the person who uploaded the site was fictitious.

For symbolic reasons, the material uploaded was chapter two of *On Liberty*, in which Mill discussed the freedom of the press and the dangers of censorship. This content is clearly in the public domain, because it was published in 1869, and subsequently its posting does not constitute any form of copyright infringement.

The US ISP followed up on the dubious complaint, made on behalf of the chairman of the non-existent John Stuart Mill Heritage Foundation, with detailed questions. But the UK ISP took the site down almost immediately, effectively censoring legal content without investigation.”

In relation to internet filtering, if intermediaries face potential liability for failing to block certain content, this suggests that the effect similarly will be to encourage systematic overblocking of material – particularly where the intermediary faces no cost for such errors. Kreimer notes that in the case of “proxy censors” their dominant

³⁵ A point made by L. Lessig, *Code and Other Laws of Cyberspace* (Cambridge: MA, 1999) where he refers to “truth in blocking” as a desirable characteristic.

³⁶ R. Deibert and N. Villeneuve, “Firewalls and Power: An Overview of Global State Censorship of the Internet” in M. Klang and A. Murray (eds.), *Human Rights in the Digital Age* (London, 2005) at 119.

³⁷ N. Villeneuve, “The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace” (2006) 11(1) *First Monday*. Available at http://firstmonday.org/issues/issue11_1/villeneuve/index.html

³⁸ B. Fitzgerald, “Note: *Edelman v. N2H2* – At the Crossroads of Copyright and Filtering Technology” (2004) 69 *Brooklyn Law Review* 1471.

³⁹ C. Ahlert, “How *Liberty* was lost on the internet” *spiked* 1 June 2004, available at <http://www.spiked-online.com/Articles/0000000CA553.htm>.

incentive is “to protect themselves from sanctions, rather than to protect the target from censorship”.⁴⁰

There is, of course, also the possibility that intermediaries will simply use the regulatory function vested in them in a way which serves their own interests. For example, there have been numerous cases where the makers of filtering software have blocked sites critical of their software⁴¹, while in Canada the ISP Telus achieved notoriety recently when it blocked subscriber access to a site supporting a strike by its employees.⁴²

Proportionality

Filtering software in particular has often been said to lack proportionality – for example, it is common for certain technical implementations to block entire domains or even entirely unrelated sites due to offending material on a single page.⁴³ For example, the current Finnish system of blocking child pornography appears to operate by means of DNS blacklisting in a way which will also prevent access to other sites hosted on a shared server.⁴⁴ This echoes the problems revealed in *Centre for Democracy & Technology v. Pappert*⁴⁵ where the Pennsylvania law ultimately caused more than 1,190,000 innocent web sites to be blocked by ISPs even though they had been required to block fewer than 400 child pornography web sites.

These problems are commonly due to slapdash technical implementations and can to some extent be mitigated by solutions that block at the full URL level rather than the IP or DNS level, or in the case of content based filtering by solutions which employ smarter algorithms to identify blocked content.

However, even where technical approaches make more granular blocking possible, there may still remain the problem that while technology is capable of applying rule based metrics, it falls down when asked to apply standard based assessments (such as whether a particular use of copyrighted material amounts to fair use or fair dealing).⁴⁶ Consequently, technical solutions are most appropriate where legality (as in the case of child pornography) is more likely to be a binary (yes/no) matter – applying

⁴⁰ S. Kreimer, “Censorship by Proxy: The First Amendment, Internet Intermediaries and the Problem of the Weakest Link” (2006) 155 *University of Pennsylvania Law Review* 11.

⁴¹ For examples, see The Free Expression Policy Project, *Internet Filters – a Public Policy Report* (New York, 2006), available at <http://www.fepproject.org/policyreports/filters2.pdf>; a Electronic Frontiers Australia press release, “Government approved net filters attempt to silence critics” available at <http://www.efa.org.au/Publish/PR000629.html>; TIME Digital Magazine, “Cybersitter decides to take a time out” 8 August 1997 available at <http://web.archive.org/web/20000830022313/http://www.time.com/time/digital/daily/0,2822,12392,00.html>

⁴² CBC News 24 July 2005. Available at <http://www.cbc.ca/story/canada/national/2005/07/24/telus-sites050724.html>.

⁴³ R. Villeneuve, “The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace” (2006) 11(1) *First Monday*. Available at http://firstmonday.org/issues/issue11_1/villeneuve/index.html

⁴⁴ D. Goodin, “Finland censors anti-censorship site” *The Register* 18 February 2008, available at http://www.theregister.co.uk/2008/02/18/finnish_policy_censor_activist/; EFFi, “Finnish Internet Censorship”, available at <http://www.effi.org/blog/kai-2008-02-18.html>.

⁴⁵ 337 F. Supp 2d. 606 (ED Pa 2004)

⁴⁶ J. Grimmelman, “Regulation by Software” (2005) 114 *Yale Law Journal* 1719.

technical solutions in more nuanced contexts is likely to result in an excessive number of false positives.

Proportionality is also likely to be an issue where, by outsourcing enforcement to intermediaries, governments succeed in externalising the costs of policing their policies. It may well be that, by taking away the discipline imposed by financial or staff constraints, this form of enforcement encourages more blocking than is socially optimum.⁴⁷ It might also be mentioned that where enforcement is carried out by means of code or architecture – and is thereby automatic – the potentially valuable element of discretion in enforcement is lost.⁴⁸

Function creep

One characteristic of many of the filtering systems outlined is that once established there are soon calls for other objectionable material to be brought within their scope. For example, in Sweden there have been calls by the music industry to implement a file sharing filter along the existing child pornography filter.⁴⁹

Regulation in the UK: “Cleanfeed”

The recent introduction in the UK of the so-called “Cleanfeed” system for blocking child pornography presents an opportunity to see to what extent these concerns are implicated.

Background

Cleanfeed has its genesis in the Internet Watch Foundation (IWF) which was founded in 1996 by way of agreement between the government, police and the internet service providers association.⁵⁰ Originally termed the Safety Net Foundation, this body had its origin in warnings by the Metropolitan Police that ISPs faced liability for hosting illicit content – particularly child pornography – unless they established procedures for removing this material. The IWF was established in response to provide a voluntary mechanism to monitor and report illegal material on the UK Internet (including a hotline for members of the public to report material), and to coordinate a notice and takedown procedure in respect of this material.

Although a private, charitable body with no formal state representation on its board, the IWF nevertheless enjoys public funding (by way of the EU Safer Internet Initiative and government grants for specific projects) as well as being funded by the Internet industry in the UK. It also enjoys public recognition as the only private body

⁴⁷ S. Kreimer, “Censorship by Proxy: The First Amendment, Internet Intermediaries and the Problem of the Weakest Link” (2006) 155 *University of Pennsylvania Law Review* 11 at 27.

⁴⁸ L. Tien, “Architectural Regulation and the Evolution of Social Norms” (2003-2004) *Yale Journal of Law and Technology* 1 makes this point.

⁴⁹ See, e.g., <http://www.sonafoundation.org/cases/internet-filter-norway/>.

⁵⁰ See, e.g., <http://www.rogerdarlington.co.uk/iwf.html>. The establishment of the IWF is discussed in detail in Y. Akdeniz, *Internet Child Pornography and the Law* (Aldershot, 2008) ch. 9. The parties to its establishment included LINX, various individual ISPs, the ISPA, the Department of Trade and Industry and the Home Office.

to be recognised as a relevant authority under Section 46 of the Sexual Offences Act 2003 – granting immunity in the carrying out of its functions.⁵¹

In carrying out this hotline function the IWF drew up a database (formally known as the Child Sexual Abuse Content URL List⁵²) of particular URLs which its staff had determined hosted child pornography. That list is said by the IWF to typically contain between 800-1200 URLs at any time. The process whereby the list is drawn up and reviewed was outlined by the IWF at one board meeting as follows:

“Termed the Child Abuse Images URL service or CAI URL service, this is a dynamic system, up-dated daily as new URL’s are added. For inclusion on the list, the web-site must contain images of child abuse image URLs deemed potentially illegal according to UK law. If the potentially illegal images are on the home page then the entire site is included, if they are only found in specific locations within that site, then only those URL’s containing such content are recorded and added.

The IWF has five highly trained analysts, working full-time viewing and classifying images. The analysts undergo a comprehensive in-house training programme as well as attending a training day with police experts.

The IWF uses the classifying system as stipulated by the Sentencing Advisory Panel. This lists 5 levels of abuse from Level 1, erotically posed children etc. through to Level 5. At least two analysts must confirm that an image is Level 1 before it is added to the database. All reports will include the name of both the analysts involved in such a classification.

The IWF also has a complaints procedure to allow site owners to make representations if they feel they have been wrongly added to the database. If, on receipt of a complaint, a web-site that has been added to the list has subsequently been found not to contain potentially illegal images, then the URL will be removed from the database. If, however, in the expert opinion of the analysts at the IWF, the content is still potentially illegal under UK law, then the URL will remain on the list. The complainant can then make further representations in which case the matter will be referred to POLIT who will further review the web-site concerned and make their judgement. The police judgement is final.”⁵³

In November 2002 legal advice was received indicating that the IWF could make this list available to members for the purpose of blocking these images to prevent their customers from being inadvertently exposed to them.⁵⁴ In late 2004 this advice was ultimately implemented via a system whereby members and others can access the database under licence (for a size-related fee up to £5,000 per year).⁵⁵ This is not limited to ISPs – Google, for example, has chosen to implement the system in order to filter search results.

It would appear from media reports that this took place following pressure from children’s charity NCH and intervention from the Home Office.⁵⁶ BT then appears to have taken the initiative both in seeking to have this list be made available and also in

⁵¹ See, for example, the “Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003” dated 6 October 2004, available at http://www.iwf.org.uk/documents/20041015_mou_final_oct_2004.pdf, which gives special recognition to the role of the IWF. See generally Internet Watch Foundation, “About the Internet Watch Foundation” available at <http://www.iwf.org.uk/public/page.103.htm>.

⁵² See <http://www.iwf.org.uk/public/page.148.htm>.

⁵³ See <http://www.iwf.org.uk/corporate/page.94.176.htm>.

⁵⁴ See <http://www.iwf.org.uk/corporate/page.49.233.htm>.

⁵⁵ See http://www.theregister.co.uk/2006/12/29/iwf_feature/.

developing a technical system whereby subscriber access to the web could effectively be filtered against the list.⁵⁷ They did this in 2004 via what was internally termed “Cleanfeed” – a two stage filtering process intended to minimise both false positives and slowdown of connections.⁵⁸ The promise of this system was that it appeared to offer a cost effective means of implementing filtering and to limit overblocking by looking at the more granular level of individual URLs rather than domain names.⁵⁹ BT also agreed to make their solution available to other UK ISPs.

(It should be noted that even though the term Cleanfeed appears to have stuck as a generic description for this blocking, the correct name for this technology is the BT Anti Child Abuse Initiative – “Cleanfeed” is a trade mark of the THUS group of companies and is used by them to describe voluntary filtering at an end-user level.⁶⁰)

This technical implementation of the IWF blacklist has attracted some criticism. In particular, some have complained that by tackling only port 80 or http:// traffic it fails to deal with IRC, instant messaging or peer to peer access to child pornography.⁶¹ Moreover, the way in which it is implemented enables an “oracle” attack where users with a moderate degree of technical knowledge will be able to identify what sites are on the blacklist.⁶² More fundamentally, the complaint has been made that it misleads the end user by presenting an error message rather than specifying that a site is blocked.⁶³

Nevertheless, once BT provided a voluntary “proof of concept” there soon followed calls for other ISPs to follow suit – by compulsion if necessary.⁶⁴ For the most part, ISPs agreed to do so, citing commercial and practical rather than constitutional and principled concerns where they did express reluctance.⁶⁵ For the rest, the matter was soon put effectively beyond debate when the Government in 2006 signalled its intention to introduce legislation unless 100% coverage was achieved “voluntarily”.⁶⁶

⁵⁶ M. Bright, “BT puts block on child porn sites” *The Observer* 6 June 2004, available at <http://www.guardian.co.uk/technology/2004/jun/06/childrenservices.childprotection>.

⁵⁷ J. Leyden, “BT’s modest plan to clean up the Net” *The Register* 7 June 2004, available at http://www.theregister.co.uk/2004/06/07/bt_cleanfeed_analysis/.

⁵⁸ M. Bright, “BT puts block on child porn sites” *The Observer* 6 June 2004, available at <http://www.guardian.co.uk/technology/2004/jun/06/childrenservices.childprotection>. See also Hunter, “BT Siteblock” (2004) 9 *Computer Fraud and Security* 4.

⁵⁹ R. Clayton, “Failures in a hybrid content blocking system” <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>.

⁶⁰ See <http://www.cleanfeed.co.uk/>.

⁶¹ W. Grossman, “IWF reforms could pave way for UK net censorship” *The Register* 29 December 2006, available at http://www.theregister.co.uk/2006/12/29/iwf_feature/.

⁶² R. Clayton, “Failures in a hybrid content blocking system”, available at <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>.

⁶³ F. Fisher, “Caught in the web” *The Guardian* 17 January 2008 available at http://commentisfree.guardian.co.uk/frank_fisher/2008/01/caught_in_the_web.html.

⁶⁴ See e.g. “BT sounds web child porn warning”, *BBC News* 7 February 2006, available at <http://news.bbc.co.uk/1/hi/uk/4687904.stm>: “John Carr, an internet adviser to the children’s charity NCH, has welcomed the work being done by BT and other companies. However, he believes the current system of self-regulation is “reaching its outer limits”. He told BBC Radio Five Live that “unless the industry can show pretty quickly that they’re at or close to 100% coverage in Britain, I’m afraid we will be going to talk to our MPs... demanding legislation”.”

⁶⁵ S. Hargrave, “Surfing with a safety net” *The Guardian* 29 June 2006, available at <http://www.guardian.co.uk/technology/2006/jun/29/guardianweeklytechnologysection>

⁶⁶ See, e.g., the comments of Vernon Coaker, Under Secretary of State at the Home Office, speaking in the House of Commons on 15 May 2006 – “We recognise the progress that has been made as a result

As of 31 December 2007 it now appears that all UK broadband providers have adopted filtering against the IWF blacklist – whether or not they use the particular BT Cleanfeed hybrid blocking solution.

Issues arising

To what extent, then, does the “Cleanfeed” system adopted throughout the UK implicate the concerns we raised earlier?

Transparency in introducing regulation

Critics have expressed concern about the way in which the Cleanfeed system has been introduced.⁶⁷ Even though at an individual level the actions of ISPs might be described as voluntary self-regulation, taken together the effect is to subject internet users to a system of state-directed censorship of the internet, with no legislative basis of any description. Indeed, the system adopted again appears to conflict with existing legislation such as the prohibition in the E-Commerce directive of imposing general duties on ISPs to monitor activity on their networks. Edwards, for example, has questioned the rule of law implications⁶⁸:

“This censorship needs no laws to be passed, no court to rule, with the publicity that entails. It only needs the collaboration, forced or otherwise, of ISPs. ISPs are not public bodies; their acts are not subject to judicial review. Nor are they traditional news organisations; their first concern (quite properly) is for their shareholders and their own legal and PR risks, not for values like freedom of expression. Research has shown that most ISPs, asked to remove or block objectionable, but not illegal, content, or face legal pressure, tend to take down first, and worry about human rights afterwards. And even those ISPs who might have fought against censorship will have no choice after 2007.

Does this all sound familiar? It should, because it’s exactly what Google recently faced media outrage over, when they agreed to censor their own search engine to fit the requirements of the Chinese government. Here in the UK, the state itself, not a private company, proposing China-style censorship tools as part of a compulsory package for all ISPs, doesn't seem to have raised many eyebrows.”

Evading public law norms

Suppose that a site owner suffers damage from finding their site wrongfully blacklisted. What remedy might they have? ISPs as private actors do not appear to be

of the industry's commitment and investment so far. However, 90 per cent. of connections is not enough and we are setting a target that by the end of 2007, all ISPs offering broadband internet connectivity to the UK general public put in place technical measures that prevent their customers accessing websites containing illegal images of child abuse identified by the IWF. For new ISPs or services, we would expect them to put in place measures within nine months of offering the service to the public. If it appears that we are not going to meet our target through co-operation, we will review the options for stopping UK residents accessing websites on the IWF list.” Available at <http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm060515/text/60515w0013.htm#06051532001002>.

⁶⁷ W. Grossman, “The Great Firewall of Britain” *net.wars* 24 November 2006, available at http://www.pelicancrossing.net/netwars/2006/11/the_great_firewall_of_britain.html.

⁶⁸ L. Edwards, “From child porn to China in one Cleanfeed” (2006) 3(3) *Script-ed* available at <http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol3-3/editorial.asp>.

subject to judicial review, and in the absence of any contractual relationship it is difficult to see what claim a site owner might have against an ISP.

A stronger case might be made against the IWF itself. Despite its nominally private status, the IWF has accepted that it is “a public body” for the purposes of the European Convention on Human Rights and has undertaken to be governed subject to the Human Rights Act 1998.⁶⁹ Although it is not clear whether this concession would be binding if a judicial review were brought, it might provide the basis for such an action notwithstanding the lack of “any visible means of legal support” for the IWF. (compare *R. v. Panel on Takeovers and Mergers, ex p. Datafin*⁷⁰). Having said that, however, the remedies offered by judicial review are relatively limited and other governance norms which would apply to public bodies (such the Freedom of Information Act 2000) would appear to be lacking. This case would appear to prove the truth of the point made by Akdeniz that:

“When censorship is implemented by government threat in the background, but run by private parties, legal action is nearly impossible, accountability difficult, and the system is not open or democratic.”⁷¹

Fair procedures

The IWF does not notify site owners of an intention to blacklist a URL or even an entire domain, nor does it notify site owners that a decision has been made. While it does offer an internal review (to those who happen to find out that their sites have been blocked) that mechanism does not provide for any appeal to a court – instead, the IWF will make a final determination on the legality of material in consultation with a specialist unit of the Metropolitan Police.⁷² There is no provision for any further or judicial appeal.

Transparency in application

The IWF is in many regards a transparent organisation, with for example policy documents and minutes of all its board meetings available online.

It does not publish the list of blacklisted URLs, arguing (not unreasonably) that to do so would be to provide a roadmap for paedophiles. There appears to be less justification, however, for the practice adopted by BT and other ISPs of serving error pages instead of indicating that a site has been blocked. This deceptive approach has not been followed in other systems blocking child pornography, and the following is an example from Norway:

⁶⁹ Minutes of IWF Board Meeting 25 April 2001, discussed in Y. Akdeniz, *Internet Child Pornography and the Law* (Aldershot, Ashgate, 2008) at 264.

⁷⁰ [1987] 2 WLR 699.

⁷¹ Y. Akdeniz, “Who Watches the Watchmen? The role of filtering software in Internet content regulation” in C. Moller and A. Amouroux (eds.), *The Media Freedom Internet Cookbook* (Vienna, 2004), at 111.

⁷² Internet Watch Foundation, “Child Sexual Abuse Content URL Service: Complaints, Appeals and Correction Procedures” available at: <http://www.iwf.org.uk/public/page.148.341.htm>.



Stopp!

Nettleseren din har nå forsøkt å kontakte et nettsted som benyttes i forbindelse med distribusjon av overgrepbilder av barn - noe som er straffbart etter norsk straffelovs §204a (tidl. kalt barnepornografi).

Dersom du har innvendinger mot at sidene er sperret, eller mener en slik sperring ikke er korrekt, kan du ta kontakt med Kripas på tlf. 23 20 80 00 eller ved å [sende oss en epost](#).

Det logges ikke noe informasjon om din IP-adresse eller annet som kan identifisere deg når du får opp denne siden. Denne sperringen er utelukkende ment for å forebygge straffbar distribusjon av dokumenterte seksuelle overgrep, og hindre at barn som allerede er avbildet blir ytterligere utnyttet.

Hvis du ønsker mer informasjon, eller ønsker å tipse Kripas, gå til [Kripas tipsmottak](#) eller ring oss på 09989.

Kripas og internettleverandørens samarbeidsprosjekt mot seksuell utnyttning av barn på Internett



The Child Sexual Abuse Anti-Distribution Filter (CSAADF) is part of the COSPOL Internet Related Child Abusive Material Project (CIRCAMP). The project is initiated by the European Chief of Police Task Force - aimed at combating organized criminal groups behind commercial sexual exploitation of children.

Some such notification would appear to be the minimum necessary in order to ensure that there is a feedback mechanism to identify sites which have been wrongly blocked (particularly as there is no other provision for notification).

The lack of transparency in the administration of the Cleanfeed system by BT is also reflected in a dispute as to the effect the system has had. Soon after the introduction of Cleanfeed BT publicly claimed that it succeeded in thwarting over 230,000 attempts to access child pornography over a three week period – a figure which unsurprisingly caught the attention of the media. The ISPA was, however, skeptical of these figures, suggesting that at a very basic level they appeared to confuse visits with hits and pages with images. Moreover, as users might try to reload pages, and some hits might be due to images in spam, the numbers may have little validity.⁷³ Notwithstanding this confusion, the BT figure still appeared to be instrumental in shaping public opinion as to the need for this system.

Intermediaries and incentives; Proportionality

It has emerged that one ISP – Be Unlimited – in order to comply with government demands to implement a filtering system but apparently unwilling or unable to incur the cost associated with a BT-style hybrid blocking system, have done so by simply implementing crude IP address blocking, resulting in collateral damage to what may have been many thousands of innocent sites which happened to share a host with the blacklisted site.⁷⁴ This would appear to confirm the fear expressed earlier that

⁷³ “ISPs want BT to clarify data on attempts to access child abuse sites” *Washington Internet Daily* 23 July 2004.

⁷⁴ S. Lahtinen, “Be Unlimited causes stir in effort of blocking child abuse images” *thinkbroadband.com* 11 October 2007, available at <http://www.thinkbroadband.com/news/3235-be-unlimited-causes-stir-in-effort-of-blocking-child-abuse-images.html>.

intermediaries, faced with difficulties in complying with regulatory demands, will systematically overblock.

Function creep

Fears of function creep appear to have been borne out⁷⁵ recently when the Home Secretary, Jacqui Smith, announced her intention to extend the Cleanfeed system to cover extremist Islamic websites:⁷⁶

“On the threat from the internet, Smith said the government was already working closely with the communications industry to take action against paedophiles, and planned to target extremist websites in the same way. ‘Where there is illegal material on the net, I want it removed,’ she said.

The move comes after details were revealed of an extremist website containing threats against the prime minister and calling for the creation of a ‘British al-Qaida’.

‘If we are ready and wiling to take action to stop the grooming of vulnerable young [people] on social networking sites, then I believe we should also take action against those who groom vulnerable people for the purposes of violent extremism,’ she said.”

Indeed, even before this there was an interesting comment in the IWF board minutes from January 2007⁷⁷ which appeared to indicate that the blacklist was already being used by some IWF members as an intelligence gathering tool, apparently intended to identify users attempting to access child pornography. Would there be public support for such an intelligence led use of the system? In an interesting recent survey on behalf of a children's charity, it was said that 89% of the public would support ISP measures to track access to “paedophile” sites⁷⁸ while in Canada child-safety advocates have similarly expressed support for systems which would require ISPs to identify and report to police users who view child pornography.⁷⁹

Conclusion

The system of filtering of child pornography which has now been adopted by UK ISPs raises some difficult issues of transparency, process and legitimacy, particularly insofar as it appears to blur the public / private boundary and leave the process by which law is made and enforced unclear. This appears to present an ongoing threat to civil liberties insofar as the system – with its reference to a central blacklist – appears to be readily extensible to cover, for example, “extreme” political content.

⁷⁵ F. Fisher, “Caught in the web” *The Guardian* 17 January 2008, available at: http://commentisfree.guardian.co.uk/frank_fisher/2008/01/caught_in_the_web.html.

⁷⁶ H. Mulholland, “Government targets extremist websites” *The Guardian* 17 January 2008, available at: <http://www.guardian.co.uk/politics/2008/jan/17/uksecurity.terrorism>.

⁷⁷ See <http://www.iwf.org.uk/corporate/page.170.htm>.

⁷⁸ <http://publicaffairs.linx.net/news/?p=281>.

⁷⁹ “Toughen ISP rules on child porn, advocate says” *CBC News* 18 January 2008.