THE UNIVERSITY
of EDINBURGH

Internet Blocking Law and Governance in the United Kingdom: An Examination of the Cleanfeed System

TJ McIntyre

Doctor of Philosophy
University of Edinburgh
2013

Abstract

This thesis examines the legal and governance issues presented by internet blocking ("filtering") systems through the use of the United Kingdom's Cleanfeed system as a national case study. The Cleanfeed system – which aims to block access to child abuse images – has been influential both domestically and internationally but has been the subject of relatively little sustained scrutiny in the literature. Using a mixed doctrinal and empirical methodology this work discusses the evolution of Cleanfeed and considers the way in which government pressure has led to a private body without any express legislative basis (the Internet Watch Foundation) being given the power to control what UK internet users can view.

The thesis argues that the Cleanfeed system sits at the intersection of three distinct trends – the use of architectural regulation, regulation through intermediaries and self-regulation – which individually and collectively present significant risks for freedom of expression and good governance online. It goes on to identify and examine the fundamental rights norms and governance standards which should apply to internet blocking and tests the system against them, arguing in particular that Cleanfeed fails to meet the requirements developed by the European Court of Human Rights under Articles 6 and 10 ECHR. It considers the extent to which Cleanfeed might be made amenable to these principles through the use of judicial review or actions under the Human Rights Act 1998 and concludes that the diffuse structure of the system and the limited availability of horizontal effect against private bodies will leave significant aspects beyond the effective reach of the courts.

This work also assesses claims that the Cleanfeed system is a proof of concept which should be extended so as to block other material considered objectionable (such as websites which "glorify terrorism"). It argues that the peculiar features of the system mean that it represents a best case scenario and does not support blocking of other types of content which are significantly more problematic. The thesis concludes by considering proposals for reform of the Cleanfeed system and the extent to which greater public law oversight might undermine the desirable features associated with self-regulation.

Declaration

This thesis is my own work and has not been submitted for any other degree or professional qualification.

Some portions – particularly chapter 2, section 6 – are drawn from material published as 'Blocking Child Pornography on the Internet: European Union Developments' *International Review of Law, Computers & Technology* 24, no. 3 (2010): 209 and 'Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems', in *Research Handbook on Governance of the Internet*, ed. Ian Brown (Cheltenham: Edward Elgar, 2013). Chapters 4 and 5 develop arguments previously outlined in 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).

The law is stated as of 10 December 2013.

Acknowledgements

I owe a particular debt of gratitude to my colleague Prof. Colin Scott for sparking my interest in the topic and for his assistance with the funding and research leave which made it possible. My supervisors, Prof. Charlotte Waelde, Dr. Abbe Brown and Navraj Singh Ghaleigh, were unstinting in their advice and encouragement and I have benefitted greatly from their guidance. Special thanks are owed to my parents and in particular to my father who gave me an interest in computers and technology. Most of all, I must thank my wife Clodagh and my son Marcus for their forbearance throughout.

Table of contents

Table of figures

Chapter 1 – Introduction

1. Background

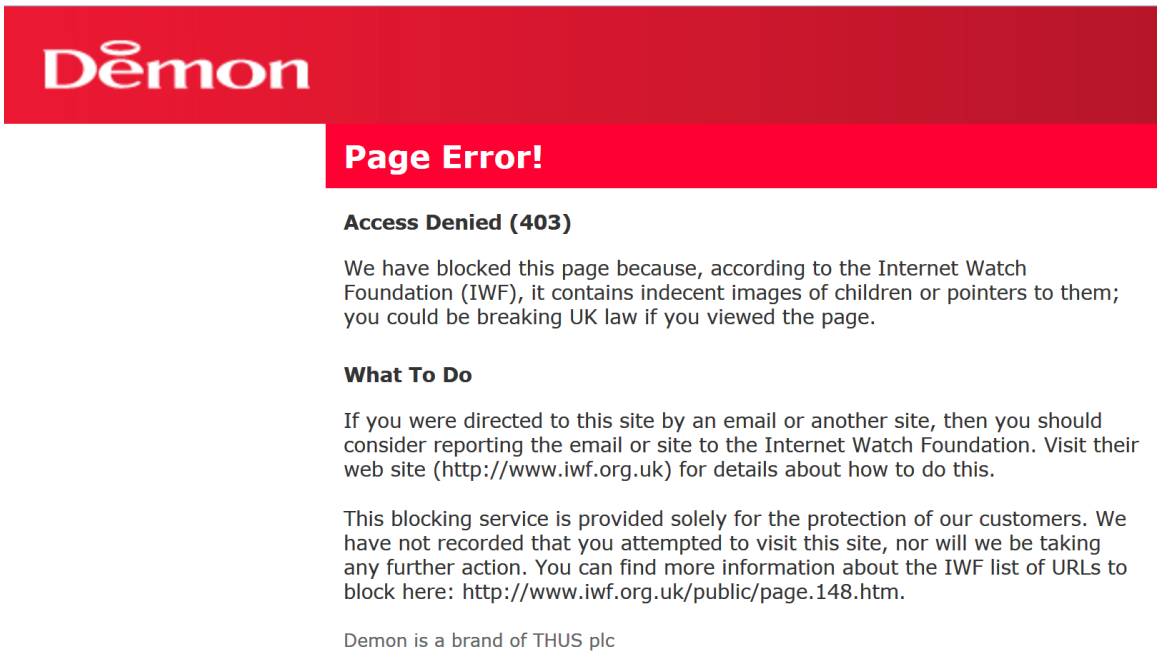

Figure 1 - Demon Internet splash page, http://iwfwebfilter.thus.net/error/blocked.html[1]

New means of communication have long presented challenges for those who would control the exchange of information. Whether we look at the production of sedition or blasphemy on printing presses in the 1580s[2] or the distribution of pornography via floppy disk in the early 1990s[3] a similar pattern emerges: technology lowers the barriers limiting dissemination of material considered objectionable and enables it to reach a wider audience. The growth of the internet has led to a culmination of this trend, giving the individual worldwide reach.

[1] Accessed 16 May 2011.
[2] See e.g. Lyman Ray Patterson, *Copyright in Historical Perspective* (Vanderbilt University Press, 1968), chap. 6.
[3] House of Commons, Home Affairs Committee, *First Report on Computer Pornography* (London: HMSO, 1994).

Regulatory responses to the challenge of controlling online content have varied. In some cases – racist publications for example – the focus has been on the producers or distributors, so that material may be legal to possess but not to distribute.[4] In other cases – notably child abuse images (CAI)[5] – the recipient has also been targeted, so that mere possession is criminalised.[6] These efforts have, however, often proved unsuccessful, due to the international, decentralised and often anonymous nature of the internet.[7] Consequently, there has been a move towards enforcement by intermediaries[8] – such as Internet Service Providers (ISPs) and search engines – by encouraging or requiring them to block access to particular material.[9] This is most associated with states such as China where blocking is used to suppress political speech; however, in the last decade blocking has also become more common in democracies, usually as part of attempts to limit the availability of CAI.[10] Numerous governments have therefore settled on blocking as their primary solution towards preventing such images from being distributed.[11]

The United Kingdom has been at the forefront of this trend. Since 2004 an industry-funded body – the Internet Watch Foundation (IWF) – has worked with ISPs to identify and block access to web pages hosted abroad which contain CAI. This was first implemented by British Telecom (BT) on a voluntary basis but following Home Office threats of legislation almost all UK ISPs have followed BT's lead and now filter user

[4] Yaman Akdeniz, 'Governing Racist Content on the Internet: National and International Responses', *University of New Brunswick Law Journal* 56 (2007): 103.
[5] The use of terms such as "child abuse images" in preference to "child pornography" is discussed in the Appendix.
[6] Yaman Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (Aldershot: Ashgate, 2008), pt. 1.
[7] Peter P. Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet', *The International Lawyer* 32 (1998): 991.
[8] Jonathan Zittrain, 'Internet Points of Control', *Boston College Law Review* 44 (2003): 653; Jonathan Zittrain, 'A History of Online Gatekeeping', *Harvard Journal of Law and Technology* 19, no. 2 (2006): 253.
[9] Ronald Deibert et al., eds., *Access Denied* (Cambridge, MA: MIT Press, 2008).
[10] Yana Breindl, *Internet Content Regulation in Liberal Democracies: A Literature Review*, DH Forschungsverbund – Working Papers Zu Digital Humanities 2 (Göttingen: Göttingen Centre for Digital Humanities, 2013), http://www.gcdh.de/files/1113/6549/2342/YBreindl_Literature_Review_Mar2013_final.pdf.
[11] 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).

connections against an IWF supplied blacklist. This scheme is generally known as "Cleanfeed" – a title which was originally used internally by BT[12] but is now more commonly used as shorthand for the entire national system.[13]

The Cleanfeed system has, however, proved extremely controversial. The manner in which it was introduced – following government pressure, in close conjunction with the Home Office, Metropolitan Police and Crown Prosecution Service (CPS) but without any legislative basis – coupled with the way in which it delegates determinations of legality to a private body has led to claims that it threatens freedom of expression.[14] Similarly, the system has been challenged on grounds of transparency and fair procedures. The IWF does not generally notify site owners either before or after material is blocked, and most ISPs have implemented blocking in such a way that users are presented with a deceptive error message rather than being informed that material has been blacklisted.[15] There have also been fears of function creep, not least as copyright litigants have succeeded in persuading the courts that they should be entitled to piggyback on ISPs' blocking systems to block filesharing sites also.[16]

2. Aims and original contribution

While these individual issues with Cleanfeed are interesting in their own right, from the wider perspective of this thesis the system is significant in the way in which it brings together a series of wider trends in internet governance and offers us the chance to evaluate those trends in a national context. At the most abstract level, it illustrates the debate between cyber-libertarians and cyber-paternalists as to whether the internet is

[12] Philip Hunter, 'BT's Bold Pioneering Child Porn Block Wins Plaudits amid Internet Censorship Concerns', *Computer Fraud & Security* 2004, no. 9 (2004): 4.
[13] The use of the term "Cleanfeed" is discussed in more detail in Appendix 1.
[14] Lilian Edwards, 'From Child Porn to China, in One Cleanfeed', *SCRIPT-Ed* 3, no. 3 (September 2006).
[15] Tim Richardson, 'ISPA Seeks Analysis of BT's "Cleanfeed" Stats', *The Register*, 21 July 2004, http://www.theregister.co.uk/2004/07/21/ispa_bt_cleanfeed/.
[16] See e.g. Darren Meale, 'NewzBin2: The First Section 97A Injunction against an ISP', *Journal of Intellectual Property Law & Practice* 6, no. 12 (2011): 854.

inherently resistant to censorship[17] or can be subjected to regulation by appropriate technological responses.[18] By automating the enforcement of the criminal law it embodies Lessig's concept of "code as law" and enables us to assess his concerns about the opacity of code as a means of regulation.[19] Likewise, by focusing on intermediaries rather than producers or recipients it reflects the practical advantages Zittrain has described in the use of "internet points of control"[20] and also the threats to freedom of expression Kreimer has identified in respect of "censorship by proxy".[21] Insofar as it relies on industry self-regulation[22] – lacking legislative underpinning – it may offer a flexibility and responsiveness absent from traditional forms of regulation[23] while at the same time raising the legitimacy and accountability concerns associated with "self"-regulation which impacts on the rights of others.[24] Finally, by offering a means of enforcing national law online it illustrates Reidenberg's argument that there is a democratic imperative for states to meet their responsibilities online as well as offline; an imperative he claims is best met by re-engineering the internet infrastructure to facilitate enforcement.[25]

The Cleanfeed system is therefore a particularly useful case study to consider these discussions about internet governance and the extent to which they have been reflected in the UK experience. To date, however, there has been relatively little research into

[17] David R. Johnson and David G. Post, 'Law and Borders - The Rise of Law in Cyberspace', *Stanford Law Review* 48 (1996): 1367.
[18] James Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors', *University of Cincinnati Law Review* 177 (1997): 186.
[19] Lawrence Lessig, *Code: And Other Laws of Cyberspace* (New York, N.Y: Basic Books, 1999).
[20] Zittrain, 'Internet Points of Control'.
[21] Seth Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', *University of Pennsylvania Law Review* 155 (2006): 11.
[22] Jeanne Pia Mifsud Bonnici, *Self-Regulation in Cyberspace*, Information Technology & Law Series 16 (The Hague: TMC Asser Press, 2008); Damian Tambini, Danilo Leonardi, and Christopher Marsden, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (London: Routledge, 2008).
[23] Monroe Edwin Price and Stefaan Verhulst, *Self-Regulation and the Internet* (The Hague: Kluwer Law International, 2005), 1.
[24] See e.g. Anthony Ogus, 'Rethinking Self-Regulation', *Oxford Journal of Legal Studies* 15, no. 1 (1995): 97–108; Michael D. Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment', *Virginia Journal of Law and Technology* 8 (2003): 6.
[25] Joel R. Reidenberg, 'States and Internet Enforcement', *University of Ottawa Law & Technology Journal* 1 (2004): 213.

either its development or operation.[26] The legal and regulatory issues it raises have been considered by a number of authors but usually only in an abbreviated form and in the context of a wider examination of internet governance.[27] In particular, there has been little work done on the way in which public law norms and fundamental rights might be implicated by Cleanfeed.[28] To date it appears that only Laidlaw and the current author have considered these points in detail.[29]

This thesis addresses this gap in the literature and provides an original contribution by describing how the Cleanfeed system has developed, using it to test the claims which have been made regarding filtering as a means of internet governance and assessing the implications which this type of state-directed "self-regulation" may have for constitutional values and fundamental rights in a UK context. In doing so it provides the first detailed examination of the domestic legal rules which govern self-regulatory filtering and considers whether – as is often claimed – such a system may undermine

[26] Leaving aside the technical implementation of the system, as to which see Richard Clayton, 'Anonymity and Traceability in Cyberspace' (PhD, University of Cambridge, 2005), chap. 7, http://www.cl.cam.ac.uk/~rnc1/thesis.pdf.

[27] See in particular Christopher Marsden, Steve Simmons, and Jonathan Cave, *Options for and Effectiveness of Internet Self- and Co-Regulation Inception Report* (RAND Europe, 30 April 2007), http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/inception_final.pdf; Christopher Marsden et al., *Options for and Effectiveness of Internet Self- and Co-Regulation Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet* (RAND Europe, 27 June 2007); Jonathan Cave, Christopher Marsden, and Steve Simmons, *Options for and Effectiveness of Internet Self- and Co-Regulation* (Santa Monica: RAND, 2008), http://www.rand.org/pubs/technical_reports/TR566/; Tambini, Leonardi, and Marsden, *Codifying Cyberspace*.

[28] These points are considered in the following works, but generally not as their focus: Tambini, Leonardi, and Marsden, *Codifying Cyberspace*, chap. 11; Daithi Mac Sithigh, 'Datafin to Virgin Killer: Self-Regulation and Public Law', 2009, http://ssrn.com/paper=1374846; Christopher Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge: Cambridge University Press, 2011), chap. 2; Christopher Marsden, 'Internet Co-Regulation and Constitutionalism: Towards European Judicial Review', *International Review of Law, Computers & Technology* 26, no. 2–3 (2012): 211.

[29] Emily Laidlaw, 'The Responsibilities of Free Speech Regulators: An Analysis of the Internet Watch Foundation', *International Journal of Law and Information Technology* 20, no. 4 (2012): 312; TJ McIntyre, 'Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems', in *Research Handbook on Governance of the Internet*, ed. Ian Brown (Cheltenham: Edward Elgar, 2013).

freedom of expression by enabling indirect state regulation which avoids traditional public law criteria of legitimacy, transparency and accountability.[30]

3. Why choose Cleanfeed as a case study?

(i) Why the national level?

Given the international nature of the internet, the choice of a purely national case study might seem unusual and merits a few words. There is a common assumption that internet regulation should take place at an international level, and equally one might say that any study should presumptively take an international perspective. Against that, however, there is a growing view that discussions of internet governance have neglected the national dimension.[31] Collins, for example, describes as a myth the view that "national governance is unimportant" and argues that the UK has evolved a distinctive (albeit improvised) and well functioning system of internet governance as compared with other jurisdictions such as the US.[32]

Collins' argument has particular weight when we consider the IWF, which is a peculiarly British self-regulatory body. It is unique in a European context as a private entity which determines what material is illegal and should be blocked – in all comparable European systems this role has been reserved to the police.[33] It raises distinct questions as to whether and how the actions of a private "censor" should be attributed to the state – questions which require a close examination of national law. The

[30] See e.g. Dawn C. Nunziato, 'How (not) to Censor: First Amendment Values and Internet Censorship Worldwide', *Georgetown Journal of International Law* 42 (2011): 1123.
[31] See e.g. Corien Prins, 'Should ICT Regulation Be Undertaken at an International Level?', in *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, ed. Bert-Jaap Koops et al., Information Technology and Law 9 (The Hague: T.M.C. Asser Press, 2006).
[32] Richard Collins, 'Three Myths of Internet Governance Considered in the Context of the UK', *Prometheus* 22, no. 3 (2004): 284.
[33] Wouter Stol et al., 'Governmental Filtering of Websites: The Dutch Case', *Computer Law & Security Review* 25 (2009): 251; TJ McIntyre, 'Blocking Child Pornography on the Internet: European Union Developments', *International Review of Law, Computers & Technology* 24, no. 3 (2010): 209; McIntyre, 'Child Abuse Images and Cleanfeeds'.

singular nature of the IWF also highlights a wider point – generalised discussions of internet regulation may fail to consider local conditions in detail and may therefore be out of touch with national legal systems. Consequently, while we cannot neglect the international dimension inherent in any discussion of internet governance, this thesis will focus primarily on the UK.

(ii) Why child abuse images?

The choice of CAI for this case study should also be explained. Why consider this subject matter instead of other types of content where blocking has been tried? The answer is that this area has both led the vanguard in relation to blocking and represents the best argument for it.

Child abuse is a particularly abhorrent crime and there is a substantial degree of international consensus as to the illegality of CAI. Unlike many other types of content which governments seek to control – such as adult pornography or file-sharing sites – the blocking of CAI has until recently generally provoked little public controversy[34] and is less likely to cause the active resistance which has met blocking of filesharing sites. Child abuse images are illegal to possess, not merely to distribute, which provides an additional paternalist rationale that blocking serves the protection of users.[35] Most importantly, there is a strong dignitarian imperative for blocking – that it serves to prevent victims of child abuse from being further victimised and distressed by further viewing of their abuse.[36]

There is also an important practical aspect which has favoured this type of blocking. As compared with other types of content, there are fewer websites to deal with. The IWF

[34] All Party Parliamentary Communications Group, *Can We Keep Our Hands off the Net? Report of an Inquiry by the All Party Parliamentary Communications Group* (London, 2009), 9, www.apcomms.org.uk/uploads/apComms_Final_Report.pdf.
[35] See chapter 2, section 3.
[36] Max Taylor and Ethel Quayle, *Child Pornography: An Internet Crime* (Hove: Brunner-Routledge, 2003), 31; Ian O'Donnell and Claire Milner, *Child Pornography: Crime, Computers and Society* (Cullompton: Willan, 2007), 70–71.

URL list, for example, typically contains about 500-800 URLs at any one time[37] and in 2011 the IWF dealt with a total of 9,550 web pages hosting CAI on a total of 1,561 different domains.[38] In addition, judgments about CAI are significantly easier to make than judgments about other types of content. Whether something "glorifies terrorism" contrary to the UK Terrorism Act 2006 requires a difficult assessment of the context, including how it is likely to be understood by members of the public.[39] By contrast, the evaluation of CAI does not generally present the same difficulty. As a result, the systems required to monitor, blacklist and ultimately block CAI present fewer administrative and technological difficulties.

For these reasons, CAI can be viewed as the best case scenario for filtering and the area therefore merits special attention. If blocking is problematic in this context then it will be all the more problematic in other areas.

4. Structure

Chapter 2 begins by outlining the legal framework which applies to ISP blocking of CAI. It examines the way in which UK law criminalises CAI and considers how this interacts with the obligations and immunities of ISPs and how these have shaped the deployment of blocking systems. It assesses the legal risks which "voluntary" blocking systems pose for ISPs and how they have mitigated these risks, and concludes by considering the way in which European Union law has influenced the growth of blocking.

Chapter 3 sets out the history of the Cleanfeed system and outlines its operation. It begins by tracing the origins of the IWF and the way in which government pressure

[37] Internet Watch Foundation, 'FAQs Regarding the IWF's Facilitation of the Blocking Initiative', 2011, http://www.iwf.org.uk/services/blocking/blocking-faqs.
[38] Internet Watch Foundation, '2011 Annual Report', 2012, 11, https://www.iwf.org.uk/assets/media/annual-reports/annual%20med%20res.pdf.
[39] David Banisar, *Speaking of Terror* (Strasbourg: Council of Europe, 2008), 21, http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

forced industry to adopt both the IWF itself and later Cleanfeed. It then describes the evolution of IWF policy towards blocking before focusing on the 2008 blocking of Wikipedia and the lessons to be drawn from that incident. Finally it evaluates proposals to expand the remit of the IWF and Cleanfeed and considers what impact these might have.

Chapters 4 and 5 contextualise the Cleanfeed system within a wider literature on internet regulation. These chapters first set out the cyber-libertarian/cyber-paternalist debate on the feasibility and legitimacy of internet regulation and then focus on three regulatory approaches associated with cyber-paternalist thinking – the use of architectural regulation ("code as law"), regulation through intermediaries and self-regulation. The chapters consider the advantages and risks which have been predicted for each approach before going on to assess to what extent the Cleanfeed system bears out or challenges these predictions. The Cleanfeed system is argued to be particularly problematic insofar as it sits at the intersection of these three approaches, compounding the concerns regarding transparency and accountability which each approach would individually present.

Chapter 6 examines in more detail the issues which arise from the self-regulatory nature of Cleanfeed by asking whether it evades judicial oversight or whether aspects of it might be subject to public law norms and compliance with fundamental rights. Two particular approaches are considered. First, we examine whether the IWF might have public status for the purposes of judicial review, an action under the Human Rights Act 1998 or as an "emanation of the state" under European Union law. Second, we evaluate to what extent the state might face a positive obligation under the ECHR to protect freedom of expression against actions of private entities such as ISPs. The chapter concludes that public law norms and fundamental rights will be enforceable against the Cleanfeed system under both approaches – however, due to the diffuse nature of the system this will be in a haphazard manner at best.

Chapter 7 moves on to consider the type of norms which might be enforced against Cleanfeed. First, it surveys the literature to identify fundamental rights approaches and governance standards which should apply to internet filtering generally. It then examines the way in which English law already regulates internet filtering in other contexts – for example, in court orders blocking websites accused of facilitating filesharing. Finally, it applies the ECHR to the Cleanfeed system to assess to what extent the ECHR already embodies standards capable of regulating internet filtering and to determine whether Cleanfeed would comply with those standards. The chapter argues that the manner in which the Cleanfeed system implements blocking would not meet the emerging jurisprudence of the ECtHR in relation to internet filtering, but that ultimately the structural problems with the Cleanfeed system can only be partially addressed by any approach which focuses on individual rights or the use of litigation.

In conclusion, chapter 8 considers proposals for the reform of the Cleanfeed system and in particular whether there is a risk that putting the system on a legislative basis might undermine the alternative accountability mechanisms and constraints imposed by self-regulation. It then identifies the way in which the perceived success of Cleanfeed has led to a fascination on the part of successive governments with the use of blocking as a regulatory tool and argues that – correctly understood – the Cleanfeed system is deeply problematic in its own right while its unique context does not support the argument that blocking should be extended to other types of content.

Chapter 2 – Legal Framework

1. Introduction

A challenging aspect of research into the Cleanfeed system is the range of legal issues which it presents. In addition to the headline public law and fundamental rights points (which will be considered in chapters 6 and 7) there are a number of less visible but equally important areas of law which have shaped the actions of the IWF, ISPs and the state but have not received the same attention.

The underlying status of the images to be blocked is one such area. While it might seem obvious that an examination of filtering should begin with an analysis of the legality of the blocked material, much of the literature has proceeded on the crude basis that filtering systems can be analysed as blocking the generic category of "child pornography" without any real examination of the types of content involved.[1] When this is done it becomes apparent that there are a number of distinct offences subsumed under that general heading which are treated quite differently by the IWF and Cleanfeed.

Similarly, to understand how the system has developed we must consider the legal constraints on the behaviour of the state and ISPs in implementing filtering. Here there is an extensive literature as to whether ISPs can be *compelled* to block but very little addressing the legal risks faced by ISPs who adopt filtering systems without a legal obligation.[2] It is therefore necessary to consider the issues faced by ISPs and the IWF in operating a voluntary blocking system – for example, their potential exposure to

[1] See e.g. Hunter, 'BT's Bold Pioneering Child Porn Block Wins Plaudits amid Internet Censorship Concerns'; Ronald J. Mann and Seth R. Belzley, 'The Promise of Internet Intermediary Liability', *William and Mary Law Review* 47 (2005): 239; Sylvia Kierkegaard, 'To Block or Not to Block – European Child Porno Law in Question', *Computer Law & Security Review* 27, no. 6 (2011): 573.

[2] See e.g. Etienne Montero and Quentin Van Enis, 'Enabling Freedom of Expression in Light of Filtering Measures Imposed on Internet Intermediaries: Squaring the Circle?', *Computer Law & Security Review* 27, no. 1 (February 2011): 21; Katalin Parti and Luisa Marin, 'Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content', *Journal of Contemporary European Research* 9, no. 1 (7 January 2013): 138.

defamation actions in the case of wrongful blocking of an innocent site – in order to understand how these have shaped the development of the Cleanfeed system.

There is also a significant European Union dimension to this area, both at the level of soft law and binding legal rules. Three particular strands must be mentioned – the successive Safer Internet initiatives and child protection measures which since 1996 have helped to promote blocking, the Electronic Commerce Directive of 2000 which limited the obligations which could be placed on ISPs, and the telecommunications framework legislation which limits the actions which can be taken by ISPs.[3]

This chapter will bring together these issues and assess how they interact with each other and the way in which they have promoted and constrained the development of Cleanfeed.

2. Jurisdiction

We will consider the law of England and Wales ("English law"). This reflects the fact that the key players – the IWF, Association of Chief Police Officers (ACPO), CPS, Metropolitan Police and the overwhelming majority of ISPs – are headquartered in that jurisdiction, and the IWF itself follows procedures which are based on that law.[4] While the IWF remit is UK-wide and decisions of the IWF will have effects in Scotland and Northern Ireland, a focus on English law is appropriate.

[3] See e.g. McIntyre, 'Blocking Child Pornography on the Internet'; Karel Demeyer, Eva Lievens, and Jos Dumortier, 'Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective', *Policy & Internet* 4, no. 3–4 (2012): 1.
[4] See e.g. Internet Watch Foundation, 'Newsgroups', 13 November 2008, http://www.iwf.org.uk/corporate/page.49.231.htm.

3. Criminalisation of child abuse images

Although "child pornography" is commonly used to describe certain types of crime English law does not have any general offence of possession or distribution of "child pornography".[5] Instead, as Gillespie points out, offences involving images or other depictions of children may be prosecuted using a variety of crimes which fall under three broad headings: (i) communication offences, (ii) obscenity and (iii) indecent photographs, pseudo-photographs and related offences.[6] To this we can now add a fourth classification: (iv) non-photographic images, added recently by the Coroners and Justice Act 2009. Adopting and adapting Gillespie's classification to reflect the 2009 Act, each of these categories will be considered in turn.

(i) Communications offences

Transmission of CAI will in some circumstances constitute an offence under section 127 of the Communications Act 2003, which prohibits the sending of messages which are "grossly offensive or of an indecent, obscene or menacing character" via a public electronic communications network. Although this section appears intended to deal with harassment, the House of Lords in *DPP v. Collins*[7] has confirmed that it applies whether or not the intended recipient would be offended by the message, and so must be differentiated from the comparable offence under section 1 of the Malicious Communications Act 1988. Instead the purpose of the offence is not merely to protect recipients but more generally to "prohibit the use of a service provided and funded by the public for the benefit of the public for the transmission of communications which contravene the basic standards of our society".[8] Indeed, the offence will apply even

[5] Though there are offences of involving children in pornography. See generally Suzanne Ost, *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge University Press, 2009), 67–68.
[6] Alisdair Gillespie, *Child Exploitation and Communication Technologies* (Lyme Regis: Russell House Publishing, 2008), chap. 3–4.
[7] [2006] UKHL 40.
[8] Para. 7.

where the recipient welcomes the message, and reciprocates with similar messages.[9] A number of cases involving social media have also accepted that it applies to the internet, not merely to traditional telephony.[10]

The implications for the transmission of CAI will be apparent. Where "grossly offensive" or "indecent or obscene" pictures are sent over the internet then an offence under section 127 is likely to have been committed – notwithstanding that the material may have been sent from one collector to another. It should also be noted that *DPP v. Collins*[11] makes it clear that the effect of the section is that the offence is complete once the message is sent – irrespective of whether it is received.[12] Consequently, provided the sender is located within the UK then the location of the recipient is irrelevant.

It is likely that this will be used only as a last resort in relation to child pornography, as it is a summary offence only and carries a maximum term of imprisonment of six months. Nevertheless the vague nature of the offence may create difficulties. While there is no authority on the point, it is possible that ISPs could be prosecuted if they know that material hosted by them falls within the scope of the section as section 127(1) criminalises both a person who "sends" a grossly offensive, etc. message as well as one who "causes any such message to be sent" and there is no requirement that the defendant have any particular intention or purpose in doing so. Consequently ISPs may be called on to assess user content against the uncertain standard of "grossly offensive" or face liability for failure to remove it.

[9] *Per* Lord Bingham, para. 26.
[10] See Lilian Edwards, 'Section 127 of the Communications Act 2003: Threat or Menace?', *Society for Computers and Law*, 9 October 2012, http://www.scl.org/site.aspx?i=ed28102.
[11] [2006] UKHL 40.
[12] *Per* Lord Bingham, para. 8.

(ii) Obscenity[13]

(a) Continued relevance

Obscenity offences were the most important tools available to prosecute CAI prior to the Protection of Children Act 1978 but after that Act the use of obscenity offences fell off.[14] This reflects the advantages for prosecutors of the more specific offences under the 1978 Act which reduced difficulties of proof and provided for greater maximum sentences. Indeed, the current CPS legal guidance on obscene publications sets out a general rule that obscenity offences should not be used in relation to indecent images of children.[15]

Despite this, obscenity offences remain significant. The 1978 Act applies only to images – specifically photographs and pseudo-photographs. Child pornography is however a substantially wider concept which may include audio-recordings of abuse, drawings and even computer generated images or plain text documents. Insofar as these fall outside the 1978 Act, the CPS guidance on indecent photographs of children recommends that prosecutors consider obscenity prosecutions in such situations.[16] Consequently, obscenity offences must be considered in some detail.

---

[13] On obscenity and the internet see generally Ian Walden, *Computer Crimes and Digital Investigations* (Oxford: Oxford University Press, 2007), 131–135; Gavin Sutter, 'Don't Shoot the Messenger? The UK and Online Intermediary Liability', *International Review of Law, Computers & Technology* 17 (2003): 73.
[14] Yaman Akdeniz, 'The Regulation of Pornography and Child Pornography on the Internet', *The Journal of Information Law and Technology* 2, no. 1 (1997), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1.
[15] Crown Prosecution Service, 'Obscene Publications: Legal Guidance', March 2010, http://www.cps.gov.uk/legal/l_to_o/obscene_publications/.
[16] Crown Prosecution Service, 'Indecent Photographs of Children: Legal Guidance', August 2010, http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/.

(b) Offences

The most important offences are those contained in section 2(1) of the Obscene Publications Act 1959 (as amended by the Obscene Publications Act 1964) which provides:

> any person who, whether for gain or not, publishes an obscene article or who has an obscene article for publication for gain (whether gain to himself or gain to another) shall [commit an offence].

These require either publication or the intention to publish – they do not apply to simple possession or even creation of CAI. This limitation was, as we shall see, a key motivation behind the adoption of specific crimes relating to indecent images of children. These offences carry a maximum penalty of five years imprisonment.[17]

(c) Application to electronic files and the internet

The 1959 Act was adopted significantly before the development of the internet. To what extent can it be applied to internet transmissions and the activities of ISPs?

"Articles"

The offence created by the 1959 Act relates to obscene "articles". Consequently an issue arises as to whether electronic files fall within this definition. Under section 1 of the 1959 Act "article" is defined widely to mean:

> any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures.

This definition was extended further by section 2 of the Obscene Publications Act 1964 to cover any items (such as photographic negatives, stencils and moulds) which can be

[17] Increased from three years by section 71 of the Criminal Justice and Immigration Act 2008.

used "either alone or as one of a set, for the reproduction or manufacture therefrom of articles containing or embodying matter to be read, looked at or listened to."

Caselaw has taken an expansive view of the term, and in *Attorney General's Reference (No. 5 of 1980)*[18] the Court of Appeal held that the showing of screen images derived from a video tape amounted to the publication of an obscene article contrary to section 2 of the 1959 Act. Although the court accepted the general principle that it "should be slow to apply the words to a piece of electronic equipment which probably had not been within the contemplation of Parliament" it went on to hold that the words chosen in the legislation were wide enough to embrace any developments in the electronic field. Similarly, in *R. v. Fellows; R. v. Arnold*[19] the Court of Appeal held that a hard disk containing scanned images of children was capable of being an "article" for the purposes of the Obscene Publications Act 1959.

"Publication"

Simple possession of obscene articles is not an offence. To achieve a conviction under section 2(1) of the Obscene Publications Act 1959 it is necessary to show that a person either "publishes an obscene article" or has one "for publication for gain". In 1994 the law in this area was specifically adapted to address electronic publications, and section 1(3) of the 1959 Act now includes transmission of data stored electronically within the concept of publication.[20]

This will cover all forms of internet distribution. Indeed, in *R. v. Fellows; R. v. Arnold*[21] the Court of Appeal held that even prior to 1994 section 1(3) was wide enough to apply to a situation where a person made files available via the internet. This has since been

[18] [1980] 3 All ER 816.
[19] [1997] 2 All ER 548.
[20] See section 168(1) of the Criminal Justice and Public Order Act 1994.
[21] [1997] 2 All ER 548.

confirmed in *R. v. Waddon*[22] where the Court of Appeal accepted that "there is publication... both when images are uploaded and when they are downloaded". Crucially for ISPs, *R. v. Fellows; R. v. Arnold*[23] also held that the making available of files for downloads initiated by others is sufficient – it is not necessary to show that a defendant himself actively initiated a particular transmission of a file.

One to one communications

The scope of "publication" has also been considered in *R. v. GS*[24] which accepted that it could apply even to private text communications online. In that case the defendant was prosecuted on the basis of Internet Relay Chat logs found on his computer. These recorded conversations with another person describing his fantasies about the physical and sexual abuse of children. The prosecution case was that his comments constituted "obscene articles" for the purposes of section 2(1). The trial judge accepted the defence submission that one to one chat online could not amount to publication in the absence of any evidence that the material was shared to some other party – treating this as the equivalent of a private conversation in a physical room. On appeal by the prosecution, however, the Court of Appeal held that "to publish an article to an individual is plainly to publish it within the meaning of the Act".[25]

The significance of this decision lies in the way in which it takes the "public" out of publication – by confirming that the 1959 Act applies even to private conversations it opens the door to the investigation and prosecution of anyone using the internet to discuss sexual fantasies with another if those fantasies meet the malleable standard of obscenity. The decision also resurrects obscenity prosecutions for the purely written word – something which most observers had considered dead following the *Inside Linda*

[22] [2000] All ER (D) 502.
[23] [1997] 2 All ER 548.
[24] [2012] EWCA Crim 398.
[25] Para. 21.

Lovelace acquittal in 1976 – thus creating a fresh legal risk for ISPs who had previously been able to focus on images only.[26]

(d) Defining "obscenity"

What do we mean by obscenity? Section 1(1) of the Obscene Publications Act 1959 puts the common law test on a statutory footing by providing that:

> an article shall be deemed to be obscene if its effect... is taken as a whole, such as to tend to deprave or corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

This antiquated[27] definition is inapt when applied to CAI insofar as it focuses on harm to the viewer rather the victim depicted in the image. That said, it does parallel a more modern theme – that blocking prevents accidental or casual viewers from awakening a latent sexual interest and may prevent progression to "contact offences" (real-world offending) against children.[28]

The test of obscenity depends on the likely audience for the material. It will be easier, for example, to demonstrate that material is obscene if it is freely available online and likely to be viewed by children than if it is only available to subscribers to a particular website or mailing list. Consequently determinations of obscenity are a matter of fact to be determined by the jury on a case by case basis and it is not possible to categorically say what types of CAI would fit this definition – whether, for example, simple nude images would be found to be obscene. Nevertheless, it is probably safe to say that the

---

[26] John Sutherland, *Offensive Literature: Decensorship in Britain, 1960-1982* (Rowman & Littlefield, 1983), 135; John Ozimek, 'Girls Aloud Net Obscenity Case Falls at First Hurdle', *The Register*, 29 June 2009, http://www.theregister.co.uk/2009/06/29/obscenity_trial_off/; Jane Ozimek, 'UK Judges Quietly Declare Text Chat Can Be Obscene', *The Register*, 3 August 2012, http://www.theregister.co.uk/2012/08/03/text_talk_legal_status/.

[27] Originating with *R. v. Hicklin* (1868) LR 2 QB 360.

[28] See e.g. John Carr and Zoe Hilton, 'Combating Child Abuse Images on the Internet - International Perspectives', in *Internet Child Abuse: Current Research and Policy*, ed. Julia Davidson and Peter Gottschalk (Abingdon: Routledge, 2011).

types of images which were involved in *R. v. Fellows; R. v. Arnold*[29] (described by the court as "children engaged in various sexual acts or poses") are likely to be found obscene.

Also, material may be obscene notwithstanding that it is published to a willing audience which may be to some extent already "depraved and corrupt". In the leading case on this point, *DPP v. Whyte*[30], the House of Lords held that the 1959 Act "equally protects the less innocent from further corruption, the addict from feeding or increasing his addiction".[31] Consequently, the fact that CAI is only made available to those with a pre-existing interest will not prevent a possible obscenity conviction.[32]

Finally, brief mention should be made of the so-called "aversion argument" – that is, that material is not obscene if its effect is to repulse the viewer. This argument (which was most famously advanced by John Mortimer at the "Oz trial"[33]) would not, however, be likely to be successful in the context of online CAI. As Gillespie notes "[c]hild pornography on the internet is frequently placed there to allow 'like minded individuals' to access, download or replicate... On that basis it is unlikely the aversion argument would succeed".[34]

(e) Defences

A public interest defence in respect of obscenity is provided by section 4(1) of the Obscene Publications Act 1959 where publication is "justified as being for the public good on the ground that it is in the interests of science, literature, art or learning, or of other objects of general concern". Although at first glance this might appear to have little relevance to CAI, it highlights a real risk for ISPs. There have been several

[29] [1997] 2 All ER 548.
[30] [1972] AC 849.
[31] *Per* Lord Wilberforce at 863.
[32] *R. v. Gavin Smith* [2012] EWCA Crim 398.
[33] For background see John Mortimer, 'Return To Oz', *Index on Censorship* 37, no. 3 (2008): 32.
[34] Gillespie, *Child Exploitation and Communication Technologies*, 35.

instances where images of children displayed in prominent galleries have been seized by police for investigation, suggesting that the boundary between art and obscenity or indecency remains uncertain in this context.[35] This boundary is further blurred by the context-sensitive nature of obscenity, so that an image which might not be obscene in the context of a gallery exhibition may present further issues when made available to a wider audience via a website.[36] Consequently an ISP faces the possibility that even mainstream art hosted by it may be the subject of an obscenity investigation – and this risk is all the greater when we go on to consider the legal status of "indecent photographs", in respect of which there is no public interest defence. As we shall see in chapter 3, this legal uncertainty played a significant part in encouraging the setting up of the IWF.[37]

(iii) Indecent photographs, pseudo-photographs and tracings of children

(a) Background

Prior to 1978 CAI were generally prosecuted as a form of obscenity. The Protection of Children Act 1978 changed this by providing for new offences relating to "indecent photographs" of children.[38] As originally adopted, the 1978 Act criminalised the making and distribution of photographs, but subsequent amendments have also criminalised mere possession[39] and extended the scope of the Act to "pseudo-photographs"[40] and "tracings"[41] of photographs.

---

[35] See e.g. Charlotte Higgins and Vikram Dodd, 'Tate Modern Removes Naked Brooke Shields Picture after Police Visit', *The Guardian*, 30 September 2009, http://www.guardian.co.uk/artanddesign/2009/sep/30/brooke-shields-naked-tate-modern; Nigel Reynolds, 'Sir Elton John's Young Girl Art: No Charges', *The Telegraph*, 26 October 2007, http://www.telegraph.co.uk/news/uknews/1567383/Sir-Elton-Johns-young-girl-art-No-charges.html.
[36] Suzanne Ost, 'Children at Risk: Legal and Societal Perceptions of the Potential Threat That the Possession of Child Pornography Poses to Society', *Journal of Law and Society* 29, no. 3 (2002): 445; Gillespie, *Child Exploitation and Communication Technologies*, 38–39.
[37] Chapter 3, section 3(i).
[38] Akdeniz, *Internet Child Pornography and the Law*, 18.
[39] Section 160 of the Criminal Justice Act 1988.
[40] Section 84 of the Criminal Justice and Public Order Act 1994.
[41] Section 69 of the Criminal Justice and Immigration Act 2008.

These crimes have considerable advantages for prosecutors as compared with either communications offences or obscenity offences. In particular, they carry substantially greater maximum sentences, do away with the difficulties of obscenity varying according to the likely audience and the related public interest defence, and criminalise mere possession without the need to show transmission, publication or an intention to publish. Consequently, they now constitute the primary response of English law to CAI and the main source of rules administered by the IWF.

(b) Indecency

The offences created under the 1978 Act all require an indecent photograph or pseudo-photograph. What do we mean by "indecent" in this context? The legislation does not itself provide a definition. Instead, caselaw has established that indecency is a question of fact to be decided by the jury according to "recognised standards of propriety" and on an objective basis under which the motive of the person making the image (or the person viewing it) is irrelevant.[42]

The vague nature of this test presents difficulties. Jury verdicts can be unpredictable regarding images at the "lower end of the child pornography scale" such as simple nude images.[43] However, this jury unpredictability is forgivable when judgments of the Court of Appeal also differ on the question of whether non-sexual images of children involving no erotic posing may be classed as indecent.[44]

[42] *R. v. Graham-Kerr* [1988] 1 WLR 1098 citing *R. v. Stamford* [1972] 2 All ER 427. See also *R. v. Smethurst* [2002] 1 Cr App *R.* 6.
[43] Ost, *Child Pornography and Sexual Grooming*, 56–57.
[44] See in particular the apparent conflict between *R. v. Oliver* [2003] 1 Cr App R. 28 and *R. v. Carr* [2003] EWCA Crim 2416 discussed in Alisdair Gillespie, 'Child Pornography: Balancing Substantive and Evidential Law to Safeguard Children Effectively from Abuse', *International Journal of Evidence & Proof* 9, no. 1 (March 2005): 29–49; Ost, *Child Pornography and Sexual Grooming*, 58–59.

Consequently, as we have already seen in relation to the public interest defence in obscenity, there will be borderline cases where it will be difficult to judge whether a particular photograph might be deemed indecent. It is not surprising that the most controversial application of the Cleanfeed system to date – the blocking of the Wikipedia page on the album "Virgin Killers"[45] – involved such a photograph.[46] The result is to put ISPs in a difficult situation in relation to material hosted by them.

Ironically, the "objective" nature of the test for indecency will compound this difficulty in assessing borderline images. When examining the public interest we noted that the contextual nature of obscenity – depending as it does on the likely audience for material – complicates assessments of obscenity. The objective test for indecency, however, presents problems of its own. By preventing consideration of the circumstances surrounding an image, it can result in crude outcomes. In the Wikipedia case, for example, the IWF was compelled to ignore the fact that the image in question was first published on an album cover 32 years ago and had been made available worldwide without any attempt to prosecute.[47] Had these circumstances been taken into account they might well have resulted in a different decision being made.[48]

(c) Photographs, pseudo-photographs and tracings

The scope of the indecency offences is set out in section 7 of the Protection of Children Act 1978. This has been heavily amended over the years to widen the types of visual depictions criminalised, including several amendments aimed specifically at computer

[45] For background on the Wikipedia block see CJ Davies, 'The Hidden Censors of the Internet', *Wired*, 20 May 2009, http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet.aspx?page=all.

[46] Though note that the IWF and police remain of the opinion that the image was properly classified as 'potentially illegal'. See Internet Watch Foundation, 'Board Minutes 9 December 2008', 9 December 2008, http://www.iwf.org.uk/accountability/governance/board-minutes/2008-board-minutes/9-december-2008.

[47] Ibid.

[48] Gillespie makes a strong argument that the test for indecency should be reformed to take account of factors such as the intention of the photographer and the person possessing material: Gillespie, 'Child Pornography', 31–33.

images. As originally adopted, section 7(2) simply provided that: "[r]eferences to an indecent photograph include an indecent film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film". No special provision was made for electronically stored images. This section remained unchanged until 1994, when growing public concern about computerised child pornography prompted two significant changes in the Criminal Justice and Public Order Act 1994.

Computer images included

The first of these was to specify that references to a photograph include "data stored on a computer disc or by other electronic means which is capable of conversion into a photograph".[49] This put beyond doubt the application of the Act to computers and later to the internet.[50]

Pseudo-photographs

The second change was more fundamental and widened the scope of the 1978 Act significantly by extending it to "pseudo-photographs" also. This was prompted by police reports of encountering images which were not straightforward photographs but were manipulated or composites in some way – for example, where a child's head was superimposed onto the body of an adult. Such cases were not, according to CPS guidance, capable of being prosecuted under the 1978 Act as it stood.[51]

Although such images might not in themselves be directly abusive of a child, they nevertheless gave rise to a number of concerns – for example, that they might fuel the demand for other child pornography material, might be used to "groom" children for abuse, or might jeopardise prosecutions if technological advances meant that it became

[49] Section 7(4).
[50] The subsequent decision in *R. v. Fellows; R. v. Arnold* [1997] 2 All ER 548 relating to pre-1994 conduct eventually confirmed that images scanned to a hard drive were covered even under the prior definition.
[51] Akdeniz, *Internet Child Pornography and the Law*, 21.

difficult or impossible to distinguish realistic pseudo-photographs from genuine photographs.[52] Section 7 was amended to bring such images within its scope and now provides that 'pseudo-photograph' means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph". This amendment is, however, relatively limited in its scope in that it only applies where an item "appears to be a photograph" – requiring an element of realism which excludes cartoons or drawings.[53]

Tracings

For the sake of completeness, we should also mention the further expansion of section 7 by section 69 of the Criminal Justice and Immigration Act 2008 which criminalised any "tracing or other image" which is "derived from… a photograph or pseudo-photograph". This relatively new provision was described by the CPS as a response to a practice amongst some offenders of tracing images of children (whether by tracing paper or on computer) and subsequently destroying the original photograph, so that the resulting images would appear to be drawings falling outside the scope of the 1978 Act.[54]

(d) Possession

The possession offence in relation to photographs, pseudo-photographs and tracings is provided for in section 160 of the Criminal Justice Act 1988 which provides that "it is an offence for a person to have an indecent photograph or pseudo-photograph of a child in his possession".[55] This offence carries a maximum penalty of five years imprisonment.

---

[52] See e.g. Ibid., 20–24; Gillespie, *Child Exploitation and Communication Technologies*, 30–31.
[53] *R. v. Atkins; R. v. Goodland* [2000] 1 WLR 1427.
[54] Crown Prosecution Service, 'Indecent Photographs of Children: Legal Guidance'.
[55] Liability for possession of temporary and "deleted" files will depend on whether the accused was aware that these files could be retrieved: see *R. v. Atkins; R. v. Goodland* [2000] 1 WLR 1427 and *R. v. Warwick* [2006] EWCA Crim 560.

Defences to possession

Section 160(2) provides the following defences to a charge of possession:

> Where a person is charged with an offence under subsection (1) above, it shall be a defence for him to prove—
>
> (a) that he had a legitimate reason for having the photograph or pseudo-photograph in his possession; or
> (b) that he had not himself seen the photograph or pseudo-photograph and did not know, nor had any cause to suspect, it to be indecent; or
> (c) that the photograph or pseudo-photograph was sent to him without any prior request made by him or on his behalf and that he did not keep it for an unreasonable time.

The first of these defences is of particular relevance to ISPs, in that it will permit the temporary retention (but not copying) of indecent images for the purpose of criminal investigation.

(e) Making indecent photographs, etc. of children

One of the most serious offences is that of making an indecent image of a child, contrary to section 1(1)(a) of the Protection of Children Act 1978 which provides that it is an offence "to take, or permit to be taken or to make, any indecent photograph or pseudo-photograph of a child".[56] This offence carries a maximum penalty of ten years imprisonment and reflects a legislative judgment that the making of an image is substantially more culpable than mere possession of an image. However, this distinction is blurred in the online context where possession and making blend together.

Making, downloading and transient copies

As originally enacted, section 1(1)(a) covered the "taking" of photographs only. As part of the 1994 amendments the section was amended to include the "making" of such

[56] As amended by section 84(2)(a) of the Criminal Justice and Public Order Act 1994.

photographs also. This presents an important issue in relation to electronic images. Does a person "make" an image simply by downloading that image to their computer? This point arose in *R. v. Bowden*[57] where the Court of Appeal held that the act of downloading necessarily involved the "making" of a new image – the local copy – rejecting defence arguments that "making" should be understood to mean the creation of an entirely new image. Indeed, the making offence has been held to apply even to situations where a purely transient copy is made. In *R. v. Smith; R. v. Jayson*[58] the Court of Appeal found that deliberately calling up an image to the screen would suffice, stating that "the act of voluntarily downloading an indecent image from a web page on to a computer screen is an act of making a photograph or pseudo-photograph", on the basis that "[b]y downloading the image, the operator is creating or causing the image to exist on the computer screen".

This reasoning, logical as it is, presents two sets of problems. The first is that it makes the possession offence largely redundant in relation to computer images, as almost any act in relation to such images (even copying an image from a hard drive to a CD-ROM) will constitute making rather than mere possession – undermining the legislative intent that the two offences should be distinct. Indeed the courts have recognised this point in the context of sentencing, regarding downloading as being less serious than taking an original photograph and more akin to simple possession.[59]

Second, the expansive interpretation of the making offence meant that actions carried out by ISPs, the IWF and police in the context of investigating CAI offences were themselves crimes, as the statutory defences under the 1978 Act did not apply to the making offence. Consider, for example, the position of a police officer taking a forensic image of a suspect's hard drive or an IWF analyst viewing a web site on foot of a complaint from a member of the public.

[57] [2000] 1 QB 88.
[58] [2002] EWCA Crim 683.
[59] *R. v. Oliver* [2002] EWCA Crim 2766.

This inadvertent criminalisation was partly addressed by the fact that prosecutions under the 1978 Act required the consent of the DPP, which consent was unlikely to be given in cases where the making was by the IWF or took place in the context of a genuine investigation.[60] This was, however, still unsatisfactory – particularly from the perspective of ISPs. As Clayton put it: "ISPs, who may from time to time offend Government or police by their stance on unrelated matters such as data retention or competition issues might well take a less sanguine view".[61]

Public interest defence to a making charge

The legislative response came in the form of a new affirmative defence in section 46 of the Sexual Offences Act 2003 where making an image is necessary "for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings". The CPS and ACPO have provided guidance on this section in a Memorandum of Understanding setting out a number of factors to be taken in account when assessing this defence.[62] These include:

1. The way in which the indecent image was discovered or made;
2. The speed with which the image was reported, and to whom it was reported;
3. Whether the handling and storage of the image was appropriate and secure;
4. Whether any copying of the image was the minimum to achieve the objective and was appropriate; and
5. Whether, in all the circumstances, an individual acted reasonably.

[60] Peter Sommer, 'Evidence: A Case for the Defence', in *Policing Paedophiles on the Internet*, ed. Allyson MacVean and Peter Spindler (Bristol: New Police Bookshop, 2003), 101.
[61] Richard Clayton, 'Clause 53 of the Sexual Offences Bill: The Problem of "Making"' (FIPR, 23 March 2003), 3, http://www.cl.cam.ac.uk/~rnc1/SexualOffencesBill.pdf.
[62] Crown Prosecution Service and Association of Chief Police Officers, 'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003', 6 October 2004, http://www.iwf.org.uk/documents/20041015_mou_final_oct_2004.pdf.

That memorandum gives specific recognition to the role of the IWF and accepts that "reports made to the IWF in accordance with its procedures will be accepted as reports to a relevant authority" for the purposes of the defence.[63] This is, we will argue later, significant in helping to establish the status of the IWF as a body subject to public law.[64]

(f) Other offences

Three other offences created by the 1978 Act must also be mentioned.

Distribution

The first is that of distribution, and under section 1(1)(b) it is an offence for a person to "distribute or show such indecent photographs or pseudo-photographs". In *R. v. Fellows; R. v. Arnold*[65] it was accepted that this offence extended to the making available of images via the internet.

Possession with a view to distribution

The second offence is possession with a view to distribution, contrary to section 1(1)(c) which provides that it is an offence for a person to "have in his possession such indecent photographs or pseudo-photographs, with a view to their being distributed or shown by himself or others". Again in *R. v. Fellows; R. v. Arnold*[66] this offence was found to apply where images are held with a view to making them available online.

[63] Ibid., 6.
[64] See chapter 6.
[65] [1997] 2 All ER 548.
[66] [1997] 2 All ER 548.

Advertisements and newsgroup titles

The third offence is that of publishing an advertisement for indecent images, and section 1(1)(d) provides that it is an offence for a person to:

> publish or cause to be published any advertisement likely to be understood to be conveying that the advertiser distributes or shows such indecent photographs or pseudo-photographs, or intends to do so.

This offence has presented particular difficulties when applied to newsgroups. Consider, for example, the newsgroup "alt.binaries.pictures.child.erotica.female".[67] Clearly the postings within that newsgroup may themselves be illegal indecent images – but might the title of the newsgroup itself be an illegal advertisement "conveying that the advertiser distributes or shows such indecent photographs"?[68]

This issue came to the fore during 2001/2002 when the IWF sought to draw up a policy dealing with newsgroups which regularly contained illegal images. As part of this process, legal advice was given by the CPS and the IWF's own advisers that newsgroup names could themselves constitute illegal advertisements so that an ISP which knowingly carried such a group name could be committing an offence. Consequently, the IWF now prepares and updates a list of newsgroup names which it considers may be illegal advertisements and recommends to UK ISPs that those newsgroups should not be carried.[69]

This offence is particularly wide, and the CPS guidance on this point makes worrying reading for ISPs:

---

[67] This example is taken from Metropolitan Police, 'Pornographic Material on the Internet', August 1996, http://www.cyber-rights.org/documents/themet.htm.
[68] Peter Robbins and Roger Darlington, 'The Role of Industry and the Internet Watch Foundation', in *Policing Paedophiles on the Internet*, ed. Allyson MacVean and Peter Spindler (Bristol: New Police Bookshop, 2003), 85.
[69] Internet Watch Foundation, 'Newsgroups'.

> Internet newsgroup names constitute an advertisement and therefore Internet Service Providers (ISPs) risk prosecution for advertising news groups with names, which imply or declare that child pornography is likely to be found within...
>
> Publication can be "passive" and an ISP that facilitates the transmission of an indecent photograph of a child by storing it may be liable under section 3 PCA 1978 as the publisher of the material. A publisher of an advertisement may be guilty of aiding and abetting the offence or of incitement to commit criminal offences, or other offences depending on the circumstances of each case...[70]

Distribution, possession with a view to distribution and the publication of advertisements all carry a maximum penalty of ten years imprisonment.

(iv) Non photographic images of children

(a) Background

A controversial extension of the law took place through the Coroners and Justice Act 2009 which criminalised non-photographic pornographic images of children – bringing cartoons, drawings and entirely computer generated images within the scope of the law (though one might question whether purely virtual images should be termed CAI as they do not involve the actual abuse of a child). As we have previously seen, publication of such images may already have been an offence under the Obscene Publications Act 1959 but for the first time simple possession was also criminalised.

The rationale behind this extension was explained by the Ministry of Justice as follows:

> There were concerns that the images could be used as a "grooming" tool to prepare children for real abuse. In addition, it was recognised that modern computer software made it easy to create drawings and other fantasy style images of explicit child sexual abuse from photographic images. If the link to a real image that would not be covered by prior legislation could not be proved it could create a situation where an abuser could create a fantasy-style visual record of actual abuse. There was also a concern that the possession and circulation of these images could reinforce offenders' inappropriate feelings towards children.[71]

[70] Crown Prosecution Service, 'Indecent Photographs of Children: Legal Guidance'.
[71] Ministry of Justice, 'Circular 2010/06: Coroners and Justice Act 2009', 19 March 2010, 17, http://www.justice.gov.uk/publications/docs/circular-06-2010-coroners-justice-act-provisions.pdf.

Against this, however, the Act was criticised on the basis that non photographic images involve no direct harm to children and arguably therefore prohibiting simple possession is to involve the creation of a form of "thought crime".[72]

While the merits or otherwise of this extension are beyond the scope of this chapter the new offence presented an important issue for ISPs and the IWF – should it be included within the blocking remit? While there is a substantial international consensus in relation to actual indecent images of children, there is no such consensus in relation to simulated imagery. Many jurisdictions do not criminalise such imagery and the United States recognises a constitutional prohibition on criminalising images where there is no actual abuse of a child.[73] The result is that sexualised virtual images of children are very common online – much more so than actual images of abuse. Following the 2009 Act the IWF therefore decided against extending its blocking remit to such images for fear that the numbers involved would make the blocking system unworkable and also that such blocking might result in adverse publicity.[74] This is significant in demonstrating that the Cleanfeed system does not merely apply the law on "child pornography" in a passive manner – instead, the IWF as the gatekeeper to the system decides which "child pornography" offences should be taken into account.

(b) Elements of the offence

Section 62 of the Coroners and Justice Act 2009 creates the offence of being in possession of a "prohibited image" of a child, carrying a maximum sentence of three years imprisonment.

"Prohibited image" is defined as being an image which is:

---

[72] See generally Abhilash Nair, 'Real Porn and Pseudo Porn: The Regulatory Road', *International Review of Law, Computers & Technology* 24, no. 3 (2010): 223.
[73] See the discussion in Brian Simpson, 'Controlling Fantasy in Cyberspace: Cartoons, Imagination and Child Pornography', *Information & Communications Technology Law* 18, no. 3 (2009): 255.
[74] Internet Watch Foundation, 'Board Minutes 29 September 2009', *Internet Watch Foundation*, 29 September 2009, http://www.iwf.org.uk/corporate/page.215.617.htm.

1. Pornographic (that is, "of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal");
2. Grossly offensive, disgusting or otherwise of an obscene character; and
3. Focuses solely or principally on a child's genitals or anal region or portrays any of six specified sexual acts.

Section 64 sets out general defences in respect of this offence, which are the same as those for the possession of indecent images of children under section 160 of the Criminal Justice Act 1988. There is a defence where a person has "a legitimate reason for having the photograph or pseudo-photograph in his possession" which will apply to ISPs in the context of investigations carried out by them.

4. ISP exemptions from liability

From the above discussion it will be apparent that many ISP activities present a risk of criminal liability. These risks are compounded when dealing with vague concepts such as obscenity where an ISP may not be sure whether material hosted by it passes the boundaries of legality. This section will detail the extent to which those risks have been mitigated.

(i) 1996-2002: Threats of prosecution followed by de facto immunity

In August 1996 the Metropolitan Police wrote to UK ISPs asking ISPs to stop carrying certain newsgroups which they identified as containing illegal pornographic material.[75] This warning formed part of wider political pressure – led by the Minister for Science and Technology – aimed at prompting the industry to implement self-regulatory controls

[75] Akdeniz, *Internet Child Pornography and the Law*, 241–242.

over illegal material.[76] The clear message was that prosecutions would follow otherwise. As *The Observer* put it at the time:

> Scotland Yard has warned British service providers that unless they withdraw access to illegal material they will be prosecuted under the Protection of Children and Obscene Publications Acts. However, police sources said enforcement… would not begin until the industry had been given a chance to put its house in order.[77]

This pressure – and way in which the industry "put its house in order" by establishing the IWF – is discussed in more detail in Chapter 3.[78] For present purposes, however, we should note how the establishment of the IWF in 1996 operated to avert these threats of prosecution.[79] The IWF from the outset worked closely with the Home Office (represented on its steering group) and the Metropolitan Police (who provided training for its staff).[80] Consequently, membership of the IWF responded to official demands in a way which was understood to provide a *de facto* defence for ISPs – with the significant caveat that failure to follow IWF take down notices might result in prosecution on charges of knowingly permitting their services to be used for the distribution of illegal material.[81] In effect, membership of the IWF signified the goodwill and cooperation of an ISP and thereby provided a limited form of immunity.[82]

(ii) 2002 onwards: The effect of the E-Commerce Directive

The next significant development was the adoption of the Electronic Commerce (EC Directive) Regulations 2002[83] which implemented the hosting, caching and mere conduit

---

[76] DTI, 'DTI Press Release P/96/636', 14 August 1996, http://www.mit.edu/activities/safe/cases/demon/minister-statement.txt.
[77] David Connett and Jon Henley, 'These Men Are Not Paedophiles: They Are the Internet Abusers', *The Observer*, 25 August 1996.
[78] Chapter 3, section 3(i).
[79] Akdeniz, 'The Regulation of Pornography and Child Pornography on the Internet'.
[80] Chapter 3, sections 3(iii) and 3(iv).
[81] Akdeniz, 'The Regulation of Pornography and Child Pornography on the Internet'.
[82] Though the Home Office, police and CPS were keen to stress that no *formal* immunity or special protection was granted to ISPs – see KPMG Peat Marwick and Denton Hall, *Review of the Internet Watch Foundation* (London, February 1999), 22.
[83] SI 2002/2013.

immunities required by the Electronic Commerce Directive.[84] From 2002 onwards the *de facto* forbearance associated with the IWF system was, for the first time, accompanied by formal legislative protection for ISPs.[85] The most important aspects in the context of CAI are the hosting and mere conduit immunities, which will be considered in turn.

(a) Hosting immunity

The hosting immunity is established by regulation 19, which provides:

> Where an information society service is provided which consists of the storage of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage where –
>
> (a) the service provider –
>
> (i) does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would be apparent to the service provider that the activity or information was unlawful; or
>
> (ii) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information; and
>
> (b) the recipient of the service was not acting under the authority or the control of the service provider.

The hosting immunity creates an exemption from criminal liability provided that the ISP does not have actual knowledge of unlawful information and acts expeditiously to remove or disable access to such information on obtaining such knowledge. In practical terms, this largely mirrored the notice and takedown system which had already been established under the auspices of the IWF. This immunity has often been said to create perverse incentives for ISPs, by actively discouraging them from taking steps to police

[84] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
[85] On ISP liability generally see e.g. Broder Kleinschmidt, 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content', *International Journal of Law and Information Technology* 18, no. 4 (2010): 332.

content hosted with them for fear that by doing so they will acquire "knowledge or awareness" which might later be used to impose liability on them.[86] In this way, however, it dovetails neatly with the IWF's hotline system – as complaints about UK hosted material are largely diverted to the IWF, UK ISPs can avoid carrying out their own investigations which might put them on notice of illegality while any knowledge gained by the IWF cannot be attributed to the ISP.[87]

(b) Mere conduit

The mere conduit immunity is established by regulation 17:

> Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where the service provider –
>
> (a) did not initiate the transmission;
> (b) did not select the receiver of the transmission; and
> (c) did not select or modify the information contained in the transmission.

This secures the position of ISPs as a mere intermediary in respect of their role as access provider, and rules out any argument that by failing to prevent access they may be facilitating the commission of a crime. Unlike the hosting immunity, it is not based on knowledge or awareness, with the result that an ISP will benefit even if it is aware that (for example) a user is visiting a particular website which is known to host CAI.

The nature of this immunity presents an issue for ISPs who engage in blocking. As with the hosting immunity, an ISP which voluntarily takes steps to stop illegal content takes a risk. It may lose the mere conduit immunity if it is found to have voluntarily relinquished its otherwise passive role. This was an issue of concern for BT during the adoption of the Cleanfeed system. BT stated at the time its view that "in diverting traffic

[86] Tambini, Leonardi, and Marsden, *Codifying Cyberspace*, 124.
[87] The IWF's hotline function is considered in Chapter 3.

to a filter that may block access depending on the results of a URL match it does not 'select the recipient of the transmission' within the meaning of the E-Commerce Regulations" but also acknowledged that if it was wrong on this point it "potentially face[d] liability for all the traffic on its network (not just traffic that it blocked)" and would have to terminate the Cleanfeed system in the event of an adverse ruling.[88]

To date there has been no ruling from a UK court as to whether this type of filtering will result in loss of the mere conduit immunity and the question remains open. There is some tension on this point within the Directive itself. On the one hand recital 40 envisages voluntary blocking by service providers by providing that:

> [T]his Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; *such mechanisms could be developed on the basis of voluntary agreements between all parties concerned* and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; *the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology* within the limits laid down by Directives 95/46/EC and 97/66/EC [emphasis added].

This would suggest that the mere conduit immunity should be given a purposive meaning which would facilitate voluntary blocking. Against that, recital 42 states that the exemptions from liability apply only where the activity of the service provider is "a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored". The ECJ has confirmed that this qualifies all the immunities under the Directive, holding in *Google France v. LVM*:

> it follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'. Accordingly, in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine

[88] See Malcolm Hutty, 'Cleanfeed: The Facts', *LINX Public Affairs*, 10 September 2004, https://publicaffairs.linx.net/news/?p=154.

> whether the role played by that service provider is *neutral*, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores [emphasis added]. [89]

The later ECJ decision in *L'Oréal v. eBay* has elaborated on this concept of neutrality, holding that in the case of an online marketplace:

> Where… the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken *a neutral position between the customer-seller concerned and potential buyers* but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31 [emphasis added].[90]

Although both *Google France* and *L'Oréal* deal with the hosting immunity rather than the mere conduit immunity, the focus in each case on the "passive" and "neutral" position of the intermediary suggests that the blocking of particular sites would not fall within these criteria. This gains support from recital 43 which specifically addresses the mere conduit immunity and provides that:

> A service provider can benefit from the exemptions for "mere conduit" and for "caching" *when he is in no way involved with the information transmitted;* this requires among other things that *he does not modify the information that he transmits*; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission [emphasis added].

Recitals 42 and 43, taken together with the limited guidance from the ECJ, therefore suggest that blocking would constitute a modification of information transmitted so as to end the immunity. While there is almost no authority on the issue, this was the view taken by the Irish High Court in *EMI v. UPC*, which held that Deep Packet Inspection for the purpose of traffic prioritisation was acceptable but that going further to insert advertising or block content would cause an ISP to lose the immunity.[91]

[89] Joined cases C-236/08 to C-238/08, [2010] ECR I-2417, paras. 113-114.
[90] Case C-324/09, [2011] ECR I-6011, para. 116.
[91] [2010] IEHC 377, para.108.

This does not, of course, mean that an ISP would face liability for all content it transmitted. If the mere conduit immunity did not apply then liability would become an issue for national law which in many cases would provide an alternative defence.[92] It might also be argued that the loss of the immunity only applied to the particular data which was subject to non-passive or non-neutral treatment – leaving it intact in respect of other traffic which was handled in a neutral manner.[93] That said, the use of blocking creates a very real risk. It highlights the strength of the political pressure placed upon them that despite this risk ISPs have proceeded to implement the Cleanfeed system regardless.

(c) No general duty to monitor

Both the hosting and mere conduit defences must be read in conjunction with Article 15 of the E-Commerce Directive, which prevents Member States from imposing a general obligation on ISPs to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity. Following the decision of the ECJ in *Scarlet (Extended) v. SABAM*[94] it is clear that the courts in assessing a blocking obligation must consider whether it would require an ISP to "actively monitor all the data relating to each of its customers" in order to "prevent a future infringement"[95] – if so, it will be in breach of Article 15. In addition, that decision has made it clear that any blocking obligation must also take into account all fundamental rights involved – including the freedom of the ISP to conduct a business and the data protection and freedom of expression rights of users whose communications would be monitored and perhaps wrongfully blocked.[96]

[92] See e.g. *Bunt v. Tilley* [2006] EWHC 407 (QB).
[93] Kalle Hynönen, 'No More Mere Conduit? Abandoning Net Neutrality and Its Possible Consequences on Internet Service Providers' Content Liability', *Journal of World Intellectual Property* 16, no. 1–2 (2013): 81.
[94] Case C-70/10, [2011] ECR I-11959.
[95] Paras. 37-40.
[96] Paras. 45-53.

Scarlet involved a remarkably invasive order in the context of filesharing and it is possible that the ECJ in balancing fundamental rights might be more receptive to a narrowly tailored approach to blocking CAI. Nevertheless, on its face the decision will significantly limit the ability of Member States to impose mandatory blocking obligations. While systems which merely block particular URLs are likely to pass muster (on the basis that they do not require active monitoring of all users' communications and can be implemented in a relatively inexpensive fashion) any systems based on more detailed content matching and particularly deep packet inspection of the type involved in *Scarlet* would appear to be ruled out. This would in particular prevent Member States from imposing blocking systems based on the developing area of hash value matching.[97] It therefore creates an incentive for Member States to continue to rely on "voluntary" self-regulatory systems which would be beyond the scope of Article 15 and could go further in their monitoring.

5. Legal issues surrounding the implementation of filtering

There has been a great deal written on the general question as to whether states should require or encourage ISPs to block certain types of internet content and the regulatory and governance issues this may present.[98] There has been rather less, however, written on the legal implications of a filtering system introduced without legislative backup. The following section will consider these issues.

[97] As to which see McIntyre, 'Child Abuse Images and Cleanfeeds'.
[98] See e.g. Cormac Callanan et al., *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublin: Aconite Internet Solutions, 2009), http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf; Anne Cheung and Rolf H. Weber, 'Internet Governance and the Responsibility of Internet Service Providers', *Wisconsin International Law Journal* 26, no. 2 (2008); Lilian Edwards, 'The Fall and Rise of Intermediary Liability Online', in *Law and the Internet*, ed. Lilian Edwards and Charlotte Waelde, 3rd ed. (Oxford: Hart Publishing, 2009); Mann and Belzley, 'The Promise of Internet Intermediary Liability'; R. Polk Wagner, 'Filters and the First Amendment', *Minnesota Law Review* 83 (1999): 755.

(i) Loss of mere conduit status

The risk that ISPs may lose their mere conduit status has already been discussed. It is worth noting, however, that whether or not filtering of CAI will result in the loss of mere conduit status it has certainly helped to shift the overall debate towards the imposition of greater duties on ISPs including the imposition of blocking duties in other contexts. In the context of the Digital Economy bill, for example, the existence of the Cleanfeed system was decisive for many legislators as providing a proof of concept which could be applied to the blocking of alleged filesharing sites.[99]

(ii) Liability for wrongful blocking

Suppose that an IWF analyst mistypes a URL which is subsequently propagated to participating ISPs via the Child Abuse Image Content (CAIC) list. Suppose further that the site in question loses a substantial amount of traffic, suffers economic loss of some description, or finds that visitors are presented with a block page stating that the page is blocked on the basis that it "may contain indecent images of children". In those circumstances, what liability might either the IWF or the ISP face?

(a) Comparison with US immunities

In the United States, the ISP immunities introduced by section 230 of the Communications Decency Act were accompanied by a specific provision allowing "Good Samaritan" blocking of content which applied to "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable". Significantly, this provision did not merely provide that the

[99] See e.g. the comments of Lord Clement-Jones, quoted in 'Lib Dem Peer on Why Site Blocking Is Needed', *ZDNet.co.uk*, 4 March 2010, http://www.zdnet.co.uk/misc/print/0,1000000169,40070579-39001101c,00.htm.

section 230(1) immunity would not be lost in such circumstances, but went further to create an additional affirmative defence.

This has been the subject of a number of cases in the US, for the most part involving claims of wrongful inclusion in email spam filters.[100] While the precise scope of this defence remains uncharted, it seems likely that if it applied in the UK it would cover the activities of both the ISPs as "voluntarily taking action in good faith to restrict access" (under (c)(2)(A)) and the IWF "as making available... the technical means to restrict access" (under (c)(2)(B)).[101]

There is, however, no comparable provision in either the Electronic Commerce Directive or domestic UK law. While it would be possible for domestic law to introduce wider immunities, it has instead been restricted to a narrow and literal transposition of the Directive. Given that fact, what liability might either the IWF or an ISP face in cases of wrongful blocking? There is no specific authority on this point and the issue does not appear to have been considered in the literature.[102]

(b) Defamation

Given the absence of any contractual claim between the victim of wrongful blocking and either the IWF or the ISP, the strongest claim which might be made would appear to be in defamation. The basis of the claim would be that either the distribution of the CAIC list by the IWF, or the publication of a stop page by the ISP, constituted a defamatory statement about the victim – i.e. that they were responsible for making available

[100] See e.g. Jonathan I. Ezor, 'Busting Blocks: Revising 47 U.S.C. §230 To Address The Effective Lack Of Legal Recourse For Wrongful Inclusion In Spam Filters Under U.S. Law', *ExpressO*, 2010, http://works.bepress.com/jonathan_ezor/1.
[101] Eric Goldman, '47 USC 230(c)(2) and Immunity for Online Filtering', 2009, http://www.ericgoldman.org/Speeches/47usc230c2.pdf.
[102] Though see the comments in *Twentieth Century Fox v. British Telecommunications* [2011] EWHC 1981 (Ch) suggesting that liability for wrongful blocking would be difficult to establish. This is considered in more detail in chapter 7, section 2(v).

indecent images of children. Whether or not such a claim may be successful is difficult to assess in the abstract and much would turn on the specifics of the individual case.

Identification

It might be said, for example, that there is no defamation of an individual if the URL blocked does not permit identification – on the other hand, however, if tjmcintyre.com were to be blocked then identification would not be a problem as the contents of the site could readily be attributed to this author.

Nature of blocking

The manner in which the blocking was implemented would be of great importance. If an ISP were to return a fake "404 File Not Found" page then this, though deceptive, would not itself be defamatory. On the other hand, if an ISP were to block not just an individual URL but an entire domain (by using DNS filtering rather than URL filtering) then it is much more likely that there will be collateral blocking of innocent sites, so that the owners of those sites might be defamed even though one particular URL did host indecent images of children.

Use of block pages

The IWF is conscious of these risks, and has issued guidance[103] to members as to the use of block pages (also known as "stop pages" or "splash pages"):

> For transparency purposes, the IWF recommends a splash page (landing page) is displayed in response to a blocked internet request for a URL on the IWF URL list, however it is important that the content and application of such splash pages is accurate. Therefore, any such page which differs from the recommended text below and which makes any reference to the IWF or is considered by the IWF to imply an association with the IWF, such as by referring to a 'blocking

[103] Internet Watch Foundation, 'Internet Watch Foundation (IWF) Brand Guidelines', accessed 15 February 2011, http://www.iwf.org.uk/resources/brand-guidelines#IWFMemberCompanies:Splashpages.

> initiative' or a 'list of child sexual abuse websites/URLs', must be explicitly approved in advance and in writing by IWF…
>
> Any such splash page must never be displayed in response to an internet request for any specific URL which is not exactly replicated in the IWF's current list and must not be displayed for any blocked internet request at the domain level when that entire domain is not on the IWF's current list.

This final sentence in particular appears to be intended to avoid liability in possible situations where an ISP overblocks. For example: where the IWF lists a URL such as http://example.com/users/~johndoe/abuseimage.jpg in the CAIC, while an individual provider responds by using DNS blocking to prevent access to the entirety of example.com.[104]

In that guidance, the IWF also recommends the use of a particular form of wording on block pages, which again appears to be motivated in part by a desire to minimise the risk of liability in defamation:

> 403: Access Denied
>
> Access has been denied by your internet access provider because this page may contain indecent images of children as identified by the Internet Watch Foundation. If you think this page has been blocked in error please contact <your service provider>.

Despite the careful wording of this notice, however, it may well be that wrongful blocking will give rise to liability in defamation. There is therefore another perverse incentive for ISPs – the more open they are about their blocking practices (by using block pages) the more exposed to liability they may be.

[104] A similar situation recently took place in the US, where government seizure of a domain name resulted in 84,000 sites hosted on subdomains being wrongly accused of distributing child pornography. See 'U.S. Government Shuts Down 84,000 Websites, "By Mistake"', *Torrentfreak*, 16 February 2011, http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/.

(iii) Data protection

We have seen that defamation issues arise if a blocked URL can be associated with an individual. In much the same way data protection issues may arise to the extent that blocking systems involve the processing of information about individuals – both those responsible for particular URLs which are blocked and those who attempt to visit them. These issues are of particular importance insofar as the information may suggest that an individual has committed a criminal offence – something which might make the information sensitive personal data within the definition in sections 2(g) and (h) of the Data Protection Act 1998.

This point has recently been made by the European Data Protection Supervisor, Peter Hustinx, in the context of proposals for a child protection directive.[105] His opinion identifies several distinct issues which may arise:

> The EDPS has in previous opinions expressed his concerns regarding the monitoring of individuals by private sector actors (e.g. ISPs or copyright holders), in areas that are in principle under the competence of law enforcement authorities.
>
> The EDPS underlines that monitoring the network and blocking sites would constitute a purpose unrelated to the commercial purpose of ISPs: this would raise issues with regard to lawful processing and compatible use of personal data under Article 6.1.b and Article 7 of the Data Protection Directive.
>
> The EDPS questions the criteria for blocking and stresses that a code of conduct or voluntary guidelines would not bring enough legal certainty in this respect.
>
> The EDPS also underlines the risks linked with possible blacklisting of individuals and their possibilities of redress before an independent authority…
>
> This is particularly important considering the consequences of reporting: in addition to the information related to children, personal data of any individual connected in some way with the information circulating on the network could be at stake, including for instance information on a person suspected of misbehaviour, be it an internet user or a content provider, but also

[105] Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, [2010] OJ C 323/6. In relation to email filtering compare Article 29 Data Protection Working Party, 'Opinion 2/2006 on Privacy Issues Related to the Provision of Email Screening Services', 21 February 2006, 29, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_en.pdf.

information on a person reporting a suspicious content or the victim of the abuse. The rights of all these individuals should not be overlooked when developing reporting procedures: they should be taken into account in compliance with the existing data protection framework.

(a) Logging of information about visitors to URLs

These concerns have been shared by ISPs in the context of Cleanfeed. From the outset, BT was conscious of a risk of generating data suggesting that individuals are attempting to view illegal material and has therefore stated that it "does not log the IP addresses of users whose traffic is an attempt to reach a listed URL".[106] This has also presented an issue for ISPs in deploying block pages – there have been technical challenges in configuring systems to display block pages without thereby logging user details.[107]

On the other hand, there was one initiative in 2007 where two IWF members were permitted to use the CAIC list as an "intelligence tool" for the purpose of "monitoring of school networks to identify devices where an attempt was made to access a URL on a CAIC list". This was done in response to "pressure on IWF to allow the data to be used for the experiment". Significantly, however, the IWF board on learning of this took the view that "as the purpose of the project could lead to the identification of potential offenders, this was a matter outside [its] current remit". Consequently the IWF withdrew from the project, and "confirm[ed] with the two members that they may extend the use of the data for the duration of this project only".[108]

This incident and the concern of BT to avoid logging customer details reflect an interesting dynamic. It is clear that there is a desire on the part of some in policing to use systems such as Cleanfeed as an intelligence gathering tool and possibly even a tool to facilitate prosecutions.[109] This would be consistent with other UK police activity –

[106] Hutty, 'Cleanfeed: The Facts'.
[107] Andrew Cormack, Telephone interview, 30 July 2009.
[108] Internet Watch Foundation, 'Minutes of Board Meeting', 16 January 2007, http://www.iwf.org.uk/corporate/page.170.htm.
[109] Compare the desire of Irish police to view the browsing histories of those attempting to access blocked sites: Digital Rights Ireland, 'Garda Plans for Web Blocking Referred to Data Protection Commissioner',

notably Operation Pin from 2003 onwards which involved a website which served as a "honeytrap" for visitors seeking CAM.[110] However the IWF has largely curtailed this tendency, seeing it as being outside its remit. This supports the wider argument developed in chapters 4 and 5 that the structure of the IWF – as an industry funded, non-statutory and independent body – has helped to prevent function creep.

(b) Blacklisting URLs

The comments of the EDPS also suggest that there may also be a data protection issue associated with the blacklisting process. Consider, for example, the Finnish website lapsiporno.info. This site (which translates as childpornography.info) is well known as being owned by Matti Nikki, a civil liberties advocate who uses the site to criticise the Finnish police-led blocking system. His site is itself, however, blocked by that system, on the basis that he has published details of some sites on the blacklist in order to demonstrate that many sites have been blocked inaccurately.[111] In this situation a data protection issue arises. The site in question is known to be under the sole control of an individual so that a determination that the URL is to be blocked may be, in the words of the EDPS, a blacklisting of an individual without the "possibility of redress before an independent authority".

A comparison might be made with the area of credit cards. There is a legal basis[112] for English police to share details of convictions with credit card companies to enable them to cancel cards which are used for the purchase or sale of CAI.[113] In the case of the IWF, however, there is no comparable legislative basis. Consequently, if the view is taken that

---

Digital Rights Ireland, 29 March 2011, http://www.digitalrights.ie/2011/03/29/garda-plans-for-web-blocking-referred-to-data-protection-commissioner/.

[110] See the discussion in Richard Wortley and Stephen Smallbone, *Child Pornography on the Internet* (Washington, DC: US Department of Justice, 2006), 55, http://www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[111] See Dan Goodin, 'Finland Censors Anti-Censorship Site', *The Register*, 18 February 2008, http://www.theregister.co.uk/2008/02/18/finnish_policy_censor_activist/; Matti Nikki, 'Lapsiporno.info and Finnish Censorship', *Lapisporno.info*, 20 July 2009, http://lapsiporno.info/english-2008-02-15.html.

[112] Data Protection (Processing of Sensitive Personal Data) Order 2006, SI 2068/2006.

[113] Walden, *Computer Crimes and Digital Investigations*, 92.

the blacklisting of a URL involves the processing of sensitive personal data on an identifiable individual then it is likely that the lack of a legal basis contravenes the Data Protection Act 1998.

(iv) Net neutrality

To what extent might the emerging legal framework regarding network neutrality impact on the Cleanfeed system? There is no one definition of net neutrality, which is "a deceptively simple phrase hiding a multitude of meanings"[114] but we can broadly identify it as a principle limiting the extent to which ISPs are permitted to discriminate between traffic carried on their networks. From its inception, net neutrality has for the most part been narrowly framed as an issue of economics, innovation policy and consumer choice.[115] More recent work has challenged this and has sought to develop it to promote freedom of expression and privacy in communications.[116] For example, the 2011 net neutrality law adopted in the Netherlands reflects freedom of expression concerns by preventing blocking of sites except where required "to give effect to a legislative provision or court order"[117] or at the request of the user.[118] Despite these developments, however, the UK and European understandings of net neutrality remain cramped and are therefore unlikely to have any impact on the Cleanfeed system.

---

[114] Christopher Marsden, 'Network Neutrality: A Research Guide', in *Research Handbook on Governance of the Internet*, ed. Ian Brown (Cheltenham: Edward Elgar, 2013).
[115] Ibid.
[116] See e.g. Milton Mueller, 'Net Neutrality as Global Principle for Internet Governance' (Internet Governance Project, 5 November 2007), http://www.internetgovernance.org/wordpress/wp-content/uploads/NetNeutralityGlobalPrinciple.pdf; Christopher Marsden, *Net Neutrality: Towards a Co-Regulatory Solution* (London: Bloomsbury Academic, 2010), 18–19, 105–131; against this see Sluijs who argues that Article 10 ECHR may give ISPs more, rather than less, discretion in relation to the blocking of content: Jasper P. Sluijs, 'From Competition to Freedom of Expression: Introducing Article 10 ECHR in the European Network Neutrality Debate', *Human Rights Law Review* 12, no. 3 (2012): 509.
[117] Informal translation of Article 7.4a of the Telecommunications Act by civil rights group Bits of Freedom: Ot van Daalen, 'Translations of Key Dutch Internet Freedom Provisions', *Bits of Freedom*, 27 June 2011, https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/; see also Daphne van der Kroft, 'Net Neutrality in The Netherlands: State of Play', *Bits of Freedom*, 15 June 2011, https://www.bof.nl/2011/06/15/net-neutrality-in-the-netherlands-state-of-play/.
[118] See the summary in Wendy Zeldin, 'Global Legal Monitor: Netherlands: Amended Telecommunications Act Prescribes Net Neutrality, Stricter Cookie Provisions', *Library of Congress Global Legal Monitor*, 15 May 2012, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403143_text.

Our starting point is an absence, for the time being, of any general net neutrality obligations in either European or UK law.[119] Ofcom has taken a largely hands-off approach in this area and does not impose any direct controls on either the sites or services which ISPs may block. Its 2011 policy document on net neutrality restated its belief that market constraints on network operators have been effective at delivering consumer benefits so that there is no need to directly regulate traffic management. Ofcom has therefore rejected the notion of intervention to prevent blocking, relying instead on "the operation of market forces to address the issues of blocking and discrimination".[120]

Significantly, that policy document did not once mention either the ECHR or freedom of expression – its focus is entirely on the user as consumer, not the user as citizen, and it does not conceive of net neutrality or site blocking as having implications for fundamental rights. Instead Ofcom sees its role as being to promote effective competition between ISPs so that "sufficient information is available to enable consumers to make the right purchasing decisions; and consumers are able to act on this information by switching providers where appropriate".[121]

Ofcom therefore adopts a policy which focuses on transparency. It has two main elements. The first of these relates to the way in which services are marketed:

> [I]f ISPs offer a service to consumers which they describe as "internet access", we believe this creates an expectation that this service will be unrestricted, enabling the consumer to access any service lawfully available on the internet. As a result, if a service does not provide full access to the internet, we would not expect it to be marketed as internet access.[122]

[119] While Member States may take action to prevent discrimination against content they are not currently obliged to do so. See Christopher Marsden, 'Net Neutrality Law: Past Policy, Present Proposals, Future Regulation?' (presented at the United Nations Internet Governance Forum: Dynamic Coalition on Network Neutrality, Nusa Dua Bali, Indonesia, 2013), 4–5, http://papers.ssrn.com/abstract=2335359.
[120] Ofcom, 'Ofcom's Approach to Net Neutrality', 24 November 2011, 4, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf.
[121] Ibid.
[122] Ibid., 14–15.

Even this weak constraint does not, however, affect the actions of ISPs in implementing the Cleanfeed system. By referring to "any service lawfully available on the internet" it presupposes that ISPs may block access to "unlawful" services, but does not enter into any analysis as to how these might be determined or the safeguards which should apply. It therefore leaves open to ISPs the option of blocking access to any material they deem illegal.

The second way in which Ofcom has dealt with the issue of consumer information is in its support for a "Key Facts Indicator" system.[123] This has been developed since 2011 on a self-regulatory basis by UK ISPs who have agreed to use a standardised format to describe their traffic management policies.[124] A copy is reproduced on the following page:

[123] Ibid., 15–16.
[124] Broadband Stakeholder Group, 'Voluntary Industry Code of Practice on Traffic Management Transparency for Broadband Services', March 2011, http://www.broadbanduk.org/component/option,com_docman/task,doc_details/gid,1335/Itemid,63/.

TRAFFIC MANAGEMENT KEY FACTS INDICATOR*

Section 1: Traffic management in relation to your broadband product (not including during busy times and places to manage network congestion see Section 2)			
Name of broadband product			
Use and availability of services, content, application and protocols on this product			
Are any services, content, applications or protocols always blocked on this product?**			Y/N
If so what?	*List*		
Are any services, content, applications or protocols always prioritised?			Y/N
If so what?	*List*		
Are any managed services delivered on this product?			Y/N
If so what? What impact?	*This would highlight prioritisation of specific content or service and explanation on impact on any other traffic*		
Data caps and download limits			
What are the download/upload limits or data usage caps on this product?			Insert
Is traffic management used to manage compliance with data caps and download limits?			Y/N
Under what circumstances?			
Level of speed reduction?			
Duration of speed reduction?			
Is traffic management used in relation to heavy users?			Y/N
Under what circumstances?			
Level of speed reduction?			
Duration of speed reduction?			
Section 2: Traffic management to optimise network utilisation (what happens during busy times and places in addition to traffic management as described in section 1)			
Is traffic management used during peak hours?			Y/N
When are typical peak hours?	Weekdays:		Weekends:
What type of traffic is managed during these periods?***			
Traffic Type	*Blocked*	*Slowed down*	*Prioritised*
Peer to Peer (P2P)			
Newsgroups			
Browsing/email			
VOIP (Voice over IP)			
Gaming			
Audio streaming			
Video streaming			
Music downloads			
Video downloads			
Instant messaging			
Software updates			
Is traffic management used to manage congestion in particular locations?			Y/N
If so how?	The same practices are applied as during peak hours		

*This KFI gives an overview of typical traffic management practices undertaken on this product; it does not cover circumstances where exceptional external events may impact on network congestion levels.
**This excludes any service, content, application or protocol that an ISP is required to block by UK law and child abuse images as informed by the list provided by the Internet Watch Foundation.
***If no entry is shown against a particular traffic type, no traffic management is typically applied to it.

Figure 2 - Traffic management key facts indicator

Again, however, this will not restrict ISPs as it excludes from its scope: "any service, content, application or protocol that an ISP is required to block by UK law and child abuse images as informed by the list provided by the Internet Watch Foundation".[125] Consequently the Key Facts Indicator system does not provide any transparency on this point and does not even require ISPs to tell customers whether or not they filter connections against the IWF URL list.

In this, Ofcom reflects the dominant international approaches to net neutrality which tend to permit extra-judicial blocking. In the United States, for example, the Federal Communications Commission (FCC) Open Internet Order of 2010 expressly permits blocking of "unlawful content" and leaves it to the ISP to decide what is unlawful.[126] This approach is now being followed at European level also. On 11 September 2013 the Commission adopted a proposal[127] for a Regulation which would impose harmonised net neutrality obligations throughout Europe.[128] However, that proposal would still leave it open to ISPs to engage in "reasonable traffic management" which Recital 47 explains as the "prevention or impediment of serious crimes, including voluntary actions of providers to prevent access to and distribution of child pornography". Consequently, the proposal as it stands would not restrict ISP participation in Cleanfeed or similar systems.

[125] Ibid., 8.
[126] Federal Communications Commission, 'In the Matter of Preserving the Open Internet: Broadband Industry Practices', 21 December 2010, 60–61, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.
[127] Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final.
[128] See generally Marsden, 'Net Neutrality Law'.

6. European Union blocking measures

(i) Background

(a) Blocking permitted but not required

European attempts to stop online child pornography date to 1996 when the Commission adopted the *Communication on Illegal and Harmful Content on the Internet*[129] and the *Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services.*[130] These argued that the international nature of the internet would require a coordinated response from Member States but 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

[129] COM(96) 487 final.
[130] COM(96) 483 final.

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.[131] This indirectly facilitated some national blocking schemes – in the UK, for example, the IWF was able to piggyback on the hotline mechanism and funding to generate its URL list – but without directly promoting them.

These developments were paralleled in 2000 by the Electronic Commerce Directive which was drafted to leave filtering available as a policy option for Member States. This can be seen in particular in Article 12(3) which establishes the 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".

Similarly, the Authorisation Directive in 2002[132] also envisaged mandatory filtering obligations for ISPs. That directive established a light touch regime for the regulation of public communication networks and restricted the conditions which Member States

[131] Louise Cooke, 'Controlling the Net: European Approaches to Content and Access Regulation', *Journal of Information Science*, 33, no. 3 (2007): 360.
[132] Directive 2002/20/EC on the authorisation of electronic communications networks and services.

could impose on the operators of such networks – but explicitly permitted the imposition of "restrictions in relation to the transmission of illegal content" provided that those conditions were in accordance with the Electronic Commerce Directive.[133]

After the Electronic Commerce Directive and Authorisation Directive, therefore, the net effect of the European legal framework was that Member States could still legislate to require blocking while ISPs could choose to voluntarily block, subject only to the risk that by doing so they might lose the benefit of their mere conduit immunity.

(ii) Move towards blocking and requiring states to block

(a) Policy changes towards blocking; support of voluntary blocking schemes

The overall European position during this period left blocking as a policy option to Member States but did not promote it directly. 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.

The most significant was the publication in 2006 of the Final Evaluation of the 2003-2004 Safer Internet Programme. 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'.[134]

[133] See the Annex to the Directive, condition A9.
[134] COM(2006) 663 final.

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 total number of domains hosting child pornography increased from 1,894 in 2004 to 3,077 in 2006.[135] This growth fuelled demands for blocking and also, it has been argued, a moral panic which precluded any critical scrutiny of these demands.[136]

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 previously had been lacking. The Cleanfeed system also appeared to demonstrate 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 as 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, 2006 saw a significant turning point where the factors outlined above promoted the adoption of a new, pro-blocking approach. A number of initiatives soon followed. 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

[135] Internet Watch Foundation, '2006 Annual Report', 2007, 8, http://www.iwf.org.uk/documents/20070412_iwf_annual_report_2006_%28web%29.pdf.
[136] 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 (2006): 259.

2007 with the Commission document "Towards a general policy on the fight against cyber crime"[137] 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'.[138]

(b) Mandatory blocking proposed

Those initiatives were limited in that they sought to promote *voluntary* blocking schemes. The next initiative was much more ambitious, and sought to require *mandatory* blocking across the EU. This came in the form of a 2009 Commission proposal for a framework decision on combating the sexual abuse of children.[139] With the entry into force of the Lisbon Treaty this was replaced with a proposal for a directive[140] which would require the same result – significantly, however, that proposal and the directive ultimately adopted differed substantially from the proposal for a framework decision.

[137] COM(2007) 267 final.
[138] COM(2007) 267 final.
[139] COM(2009)135 final.
[140] COM(2010) 94 final.

(c) From legislative to self-regulatory blocking

Proposed framework decision

The Commission's 2009 proposal for a framework decision included a provision which would have required Member States to introduce mandatory 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 "the competent judicial or police authorities" was significant, reflecting a conclusion in the Commission's Impact Assessment that pure self-regulatory systems would not be "prescribed by law" as required by Article 10 ECHR. According to the Commission:

> [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... 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.[141]

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 strong resistance from some national governments who feared that it would require existing national systems to be placed on a legislative basis,

[141] Accompanying document to the Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, SEC(2009) 355, 30.

affecting industry-led schemes such as the IWF and probably also non-legislative police-led schemes.[142]

Proposed directive

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 government opposition by deleting any reference to police or judicial authorities. The amended provision (now Article 21) then read as follows:

> 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 blocking of access shall be 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, as far as possible, are informed of the possibility of challenging it.

The implications of this change were spelt out in a new recital 13 which made it clear that Member States would no longer have to adopt legislation but could 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". That change met with substantial criticism at the time, with civil liberties advocates asserting that the fundamental rights concerns expressed in the Impact Assessment had been sidestepped in order to ensure that existing national schemes could continue unchanged. It was also criticised by the European Data Protection Supervisor who took the view that "a code of conduct or voluntary guidelines would not bring enough legal certainty in this respect".[143]

---

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

[143] Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, [2010] OJ C 323/6.

Parliamentary pushback and compromise: Directive 2011/93/EU

Following a strong campaign by civil liberties advocates, the proposal for a directive was modified in Parliament to reject mandatory blocking, prioritise takedown of images at source and to require a legislative basis for national blocking systems. The eventual compromise text in December 2011 met the first two of these demands but left self-regulatory blocking essentially unaffected. As adopted the relevant provision is Article 25 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography which provides that:

> 1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.
>
> 2. Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.

Recital 47 makes clear that Article 25 is not intended to affect existing national systems by stating that the "measures undertaken by Member States… could be based on various types of public action, such as legislative, non-legislative, judicial or other". It goes on to say that the Directive "is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States". This is particularly important for the United Kingdom as it indicates that the safeguards in Article 25(2) have no application to "voluntary" action by ISPs even where this action is "supported" by Member States.

As a result the remaining language in recital 47 about ensuring "legal certainty", "predictability" and "end user rights" is hortatory only. If anything, the Directive incentivises national governments to promote self-regulatory systems instead of legislating as by doing so they can avoid the safeguards which the Directive would otherwise require. In a UK context therefore the requirements for proportionality,

transparency and judicial redress will not affect the Cleanfeed system except in the unlikely event that the government abandons its settled policy of self-regulation and moves to put blocking on a statutory basis.[144] This is an important outcome for the UK government as otherwise the requirement for judicial redress would at a minimum have required some form of legislation establishing independent judicial oversight of the IWF system. Instead, it is business as usual even after the Directive.

7. Conclusion

What conclusions can we draw from this survey of the law? It will be apparent from the review of the criminalisation of CAI that there were substantial risks for ISPs in relation to hosting until immunities were conferred upon them by the Electronic Commerce Directive. In light of such risks it is not surprising that there was enthusiastic take up amongst ISPs of the IWF notice and takedown system.

It is also apparent, however, that those risks were largely mitigated after 2002 – before the Cleanfeed system was established. Consequently, ISP adoption of that system cannot be said to have been motivated by a desire to minimise any risk of prosecution faced by them. If anything, the system has attracted more risk. This survey has revealed that UK law is – particularly when compared with US law – lacking in protections for ISPs who voluntarily block. By adopting the Cleanfeed system ISPs are potentially jeopardising their mere conduit status and exposing themselves to risks in defamation and data protection without the benefit of any statutory immunities. Their willingness to do so is, as will be further examined in Chapter 3, largely the result of political pressure.[145]

[144] Laidlaw argues that implementation of the Directive will require the UK government to reform the operation of the IWF. This is, however, based on a misreading of the Directive as requiring rather than permitting national blocking measures. The misreading stems from reliance on the initial text proposed by the Commission rather than the significantly changed final compromise text. See 'The Responsibilities of Free Speech Regulators', 24–25.
[145] Chapter 3, section 8.

It is important to note that not all illegal child pornography is treated equally by the IWF. We have seen that the IWF has declined to extend the CAIC URL list system to cover non-photographic images – despite the fact that such material is now equally prohibited by the law. In response to critics it is sometimes claimed that the IWF in carrying blocking is simply enforcing the law enacted by Parliament.[146] This chapter has illustrated that this claim is only partially true – the enforcement is selective and reflects a choice as to which material to block. This should not be taken as a criticism – if anything, it is an advantage of self-regulation that a body can choose to focus on the most serious harms and will be wary of blocking which may not enjoy full public support – but it does highlight that the IWF is carrying out an independent assessment of the types of images which are sufficiently serious to merit blocking, bearing its own reputation and effectiveness in mind. Claims that it is merely a neutral enforcer of the law are unsustainable.

[146] Davies, 'The Hidden Censors of the Internet'.

Chapter 3 – Development of Cleanfeed

1. Introduction

This chapter describes the development and operation of the Cleanfeed system. It begins by setting out the origins of the IWF and the development of its role from its establishment in 1996, including its first foray into wider censorship with the 2001/2002 newsgroup ban. It then focuses on the period from 2004 onwards when the IWF came to cooperate with BT, state bodies and subsequently other ISPs in the adoption of filtering systems – including filtering systems deployed in other jurisdictions. The chapter next turns to the way in which the UK government has sought to persuade (and threatened to compel) ISPs to deploy filtering systems from 2006 onwards, looking in particular at the 2009 episode in which draft legislation to compel the use of filtering systems was first leaked and then abandoned. This is followed by an examination of the controversy surrounding the blocking of pages on Wikipedia in December 2008. It explores in particular the reaction to the blocking, the appeal by Wikipedia, the procedures and limitations illustrated by that appeal, the internal decision making within the IWF that led to an ad-hoc decision to unblock, and the lessons learned from the incident.

2. Early years, early fears

(i) Computerised child pornography

Our starting point is 1994 when concern over computer content first came to the fore in the United Kingdom. In that year the House of Commons Home Affairs Committee identified[1] computer pornography as an area in need of control, leading to the adoption shortly afterwards of the Criminal Justice and Public Order Act 1994 which extended existing obscenity laws to include "pseudo photographs" (including computer generated

[1] House of Commons, Home Affairs Committee, *First Report on Computer Pornography*.

images) and "data stored on a computer disc or by other electronic means".[2] Despite the apparent breadth of that provision, however, the risks posed by networked technology were not then apparent to legislators, whose focus was on the risks of floppy discs and CD-ROMs.[3]

(ii) Availability online

While it is difficult to establish an exact date when internet content first appeared on the domestic regulatory radar, Akdeniz suggests that a turning point was reached in the summer of 1995 when a cover story ran in *Time* magazine entitled "On a screen near you: Cyberporn".[4] It was at around this time that the issue of internet pornography came to prominence in the UK media, with headlines such as "Not in front of the children"[5], "Caught in the sordid net of cybersex"[6] and the colourful "Flying Bimbo leads blitz on cyberporn".[7] The issue was also highlighted in July 1995 by "Operation Starburst"[8] which involved the arrest and prosecution of nine British men for possession and distribution of child pornography using the internet, as well as later that year by the action brought by German prosecutors against CompuServe in relation to the distribution of child pornography via newsgroups.[9] The result was to generate public concern as to the prevalence of illegal content online and the availability of pornographic content to children – a concern which Sutter has argued represented a largely unfounded moral panic.[10]

---

[2] See Yaman Akdeniz, *Sex on the Net: The Dilemma of Policing Cyberspace*, Behind the Headlines (London: South Street, 1999), 9.
[3] See Akdeniz, *Internet Child Pornography and the Law*, 17.
[4] Philip Elmer-Dewitt, 'On a Screen near You: Cyberporn', *Time*, 3 July 1995.
[5] Matthew May, 'Not in Front of the Children', *The Times*, 11 August 1995.
[6] Martin Hannan, 'Caught in the Sordid Net of Cybersex', *The Scotsman*, 27 July 1995.
[7] John Carlin, 'Flying Bimbo Leads Blitz on Cyberporn', *The Independent*, 3 December 1995.
[8] Owen Bowcott, 'Police Move on Internet Porn', *The Guardian*, 27 July 1995.
[9] Akdeniz, 'The Regulation of Pornography and Child Pornography on the Internet'.
[10] Gavin Sutter, '"Nothing New under the Sun": Old Fears and New Media', *International Journal of Law and Information Technology* 8, no. 3 (2000): 338.

Whether or not these fears were justified, late 1995 saw what appears to have been the first intervention by the executive and one which would set a pattern often repeated since. In December 1995 Science and Technology Minister Ian Taylor called on the internet industry (in the form of the then newly established Internet Service Providers' Association ("ISPA")) to block access to illegal content in newsgroups and develop a voluntary code of conduct, with the implicit threat of prosecution should they fail to do so.[11] This was followed shortly afterwards by a meeting hosted by the Home Office on 19 January 1996 to discuss "Regulation of Adult Material on the Internet" and attended by representatives of (*inter alia*) the Home Office, various police services, the Crown Prosecution Service, Customs and Excise, the Department of Trade and Industry, ICSTIS[12] and a wide selection of industry representatives from various ISPs and other interested parties such as Microsoft.[13] The letter sent to ISPs inviting them to attend is worth quoting at length, as it provides a clear summary of official thinking of the time:

> The Internet and similar computer networks are a new and rapidly growing medium for the exchange of information. The Government is committed to promoting their use and encouraging people to exploit the commercial and other opportunities which are offered by the latest information technology. However, there is considerable public concern about the availability of pornographic material on the Net. We are concerned about the protection of children and the control of unsuitable material, but also that the use of the Internet will be discouraged if it is tarnished with an undeserved reputation as a major purveyor of pornography.
>
> At present, apart from the general application of the criminal law, there is no control on the material available on the Net and indeed, given the nature of the system and its world-wide reach, any regulation of such material would pose considerable difficulty. Nonetheless, the Government considers that the risk of children being exposed to harmful material is sufficiently serious to justify careful consideration of the options.
>
> Our present position is that *we would want to encourage the industry to develop a system of self-regulation which might address these areas of concern, rather than considering statutory options* [emphasis added].[14]

That meeting was followed in January by the commencement of an inquiry by the House of Lords Select Committee on Science and Technology, the results of which were

[11] Greg Hadfield, 'Internet Firms Are Told to Switch off the Filth', *Daily Mail*, 30 December 1995.
[12] Independent Committee for the Supervision of Standards of Telephone Information Services.
[13] Clive Feather, 'Home Office Meeting of January 19th', *Clive Feather's Home Page*, accessed 14 January 2009, http://www.davros.org/homeoffice/.
[14] Ibid.

published in July 1996 as the report *Information Society: Agenda for Action in the United Kingdom.*[15] That report addressed issues of content regulation only to a relatively small extent – but where it did so, it echoed views expressed at the January Home Office meeting to the effect that what was required in respect of "undesirable content" was a system of light touch, flexible self-regulation, perhaps following the existing ICSTIS model in respect of telephone services, coupled with the promotion of parental filtering options.[16]

3. Establishing the IWF

(i) Creating a "self-regulatory" body

Events continued to move rapidly in 1996, most importantly in mid August when letters were sent to UK ISPs by the Metropolitan Police indicating that they believed that certain newsgroups contained illegal pornographic material and requesting ISPs to take action if satisfied about the nature and content of those newsgroups.[17] This was matched by a public statement by the Minister for Science and Technology who explicitly warned that prosecutions would follow unless ISPs prevented users from accessing pornography (particularly child pornography) via newsgroups[18] – saying "In the absence of self regulation, the police will inevitably move to act against service providers as well as the originators of illegal material".[19]

This gave rise to concern amongst UK ISPs as to possible criminal liability on their part and was the impetus for a meeting on 9 September 1996 when representatives from UK ISPs met with the Metropolitan Police and Home Office and which (facilitated by the

[15] House of Lords, Select Committee on Science and Technology, *Information Society: Agenda for Action in the United Kingdom* (London: HMSO, 1996).
[16] Ibid., chap. 5.
[17] Akdeniz, 'The Regulation of Pornography and Child Pornography on the Internet', sec. 5.2; Marjorie Heins, *Not in Front of the Children: 'Indecency', Censorship, and the Innocence of Youth*, 2nd ed. (Rutgers University Press, 2007), 213.
[18] Akdeniz, *Internet Child Pornography and the Law*, 241–242.
[19] DTI, 'DTI Press Release P/96/636'.

DTI) resulted in an agreement to establish a new self-regulatory body. That body – initially known as the Safety-Net Foundation, which soon became the IWF and is referred to as such here – was part of a package of measures agreed by the industry and contained in a document entitled *R3: Safety Net – Rating, Reporting, Responsibility for Child Pornography and Illegal Material on the Internet*.[20]

That document, approved by the ISPA, the London Internet Exchange ("LINX") and the IWF itself, envisaged that the regulation of content would be principles driven rather than rules driven and would be based on the following points:

> *The Internet is not a Legal Vacuum*
>
> In general, the law applies to activities on the Internet as it does to activity not on the Internet. If something is illegal 'off-line' it will also be illegal 'on-line', and *vice versa*…
>
> *Free Speech not Censorship*
>
> The issue addressed has nothing to do with censorship of legal material or free speech. The issue is how to deal with material or activity which society, through democratic process, has deemed to be unacceptable in law. The core issue is crime. Legal, but possibly offensive, material raises a quite separate issue. Here consumers should have the technological means to tailor the nature of their, or their family's, experience on the Internet according to their individual standards; thus supporting both individual responsibility and the Internet's traditions of diversity and free speech.
>
> *Responsibility*
>
> Service providers must take a responsible approach to the provision of services. They need to implement reasonable, practicable and proportionate measures to hinder the use of the Internet for illegal purposes, and to provide a response mechanism in cases where illegal material or activity is identified. Service providers should not be asked to take responsibility for enforcement of the law. End users should retain responsibility for the content they place on the Internet. The Police should retain responsibility for enforcement.
>
> *Self Protection*
>
> By taking appropriate measures, across the industry, service providers can offer protection to the end user and to themselves. All responsible service providers wish to hinder the availability of child pornography, and to see it removed from the Internet. This clearly protects the public. Establishing a common understanding of what steps constitute a reasonable, practicable and proportionate approach can also provide a defence for service providers against prosecution on charges of knowingly permitting services to be used for the distribution of illegal material.

[20] Internet Service Providers Association, LINX, and Safety-Net Foundation, 'R3 - Rating, Reporting, Responsibility for Child Pornography and Illegal Material on the Internet', 23 September 1996, http://www.mit.edu/activities/safe/labeling/r3.htm.

> *Establishment & Jurisdiction*
>
> The law that determines what material or activity is illegal is the law of the country in which the consumer is affected by it. These proposals relate to service providers offering access to the Internet in the UK. They are designed to avoid any extraterritorial effect. Service providers established in the UK will take the UK law as the relevant standard for their UK operation – whatever the source of the material...

The reference to self-protection is telling – the key motivation of the industry in signing up to this agreement was to provide a defence for service providers against what was seen as a realistic risk of prosecution on charges of knowingly permitting services to be used for the distribution of illegal material.[21] Adoption of this approach, carrying the implicit imprimatur of the Home Office and Metropolitan Police, effectively provided such a defence in a way which would not be matched by legislation for a further six years.[22]

(ii) Illegal v. offensive material

The *R3* agreement envisaged a two-fold role for the IWF – to establish a system for the reporting and takedown of illegal material on the internet, and to promote rating systems by which users could control the viewing of offensive material. This was an important distinction which reflected the underlying need for immunity from prosecution – despite the early focus of the Home Office on "adult", "harmful" and "unsuitable" material, the commitment made by the ISPs was primarily to the control of *illegal* material, particularly child pornography.

Other objectionable content was the subject of a more limited commitment – to assist consumers and especially parents with client-side filtering. This committed the IWF to assisting in the development of rating systems and recommended that ISPs "promote

[21] Clive Feather, 'Re: Cleanfeed and Wikipedia', 8 December 2008, http://markmail.org/message/jmmztsegqpcjykns.
[22] By the Electronic Commerce (EC Directive) Regulations 2002, SI 2013/2002. See generally Chapter 2, section 4.

PICS enabled software" for accessing the web, "[r]equire all their users to rate their own web pages" and "remove web pages hosted on their servers which are persistently and deliberately misrated".[23] This aspect of the IWF's remit met with significant opposition, particularly in March 1998 when it published a report calling for the development of a worldwide rating system to incorporate some element of "policing... to maintain the standards and credibility of the system".[24] As a result, while some UK ISPs – such as Demon Internet – did initially require users to rate their web pages, this was a short lived approach which was dropped in 1998 in the face of user opposition and recognition of its impracticability.[25]

With mandatory labelling gone, therefore, the control of legal but objectionable content shifted almost entirely to the user – although ISPs continued to promote filters to their users, they themselves played little role in policing content hosted by them which was merely "offensive". Similarly, while the IWF continued to work on the development of client side filtering, and was a founder member of the Internet Content Rating Association in 1999, it never itself took on the function of classifying or rating offensive material and instead left this entirely to third parties – and gradually moved away from issues of offensive content to concentrate solely on criminal content.[26]

---

[23] Internet Service Providers Association, LINX, and Safety-Net Foundation, 'R3 - Rating, Reporting, Responsibility for Child Pornography and Illegal Material on the Internet'.

[24] Internet Watch Foundation, 'Rating And Filtering Internet Content: A United Kingdom Perspective', *Internet Watch Foundation*, March 1998, http://web.archive.org/web/19990421120909/http://www.internetwatch.org.uk/rating/rating_r.html; Yaman Akdeniz, 'Cyber-Rights & Cyber-Liberties (UK) Report, Who Watches the Watchmen', *Cyber-Rights & Cyber-Liberties*, November 1997, http://web.archive.org/web/200012031831/http://www.leeds.ac.uk/law/pgs/yaman/watchmen.htm; Yaman Akdeniz, 'Cyber-Rights & Cyber-Liberties (UK) Report - Who Watches the Watchmen: Part II', *Cyber-Rights & Cyber-Liberties*, September 1998, http://www.cyber-rights.org/watchmen-ii.htm.

[25] Irene Graham, 'Will PICS Torch Free Speech on the Internet?', *Communications Law Bulletin* 17, no. 1 (1998): 11.

[26] At the time of writing, the IWF describes its remit as being 'To minimise the availability of potentially criminal internet content specifically: images of child sexual abuse hosted anywhere in the world; criminally obscene adult content hosted in the UK; non-photographic child sexual abuse images hosted in the UK': Internet Watch Foundation, 'Remit, Vision and Mission', *Internet Watch Foundation*, 2011, http://www.iwf.org.uk/about-iwf/remit-vision-and-mission.

Reflecting this and the aims of this research, the remainder of this chapter will focus on the developing role of the IWF in relation to *illegal* content only.

(iii) Procedures and functions

Under the *R3 Agreement* the primary role of the IWF was to act as a hotline for receiving and acting upon public complaints about illegal material online. Although the hotline model is now commonplace, at the time this was a pioneering approach based on the Dutch model which had been implemented in June 1996.[27] Under the initial agreement, the IWF would consider whether material (particularly child or adult pornography) was potentially illegal and if so it would:

- in respect of UK originated material, attempt to trace the source of material and to inform the author of the position under UK law, coupled with a request to remove the material; where co-operation is not forthcoming, request action from the relevant ISP and pass the details to the National Criminal Intelligence Service (NCIS); and confirm the action to the complainant.
- in respect of non-UK material, details would be passed to the foreign ISP, if it could be identified, and to NCIS, who would be able to liaise with the police force in the appropriate jurisdiction.[28]

As can be seen, this system originally envisaged that the IWF would first contact the source of potentially illegal material in order to request its removal, with escalation to the ISP and police as a fallback. This approach was, however, soon abandoned and instead IWF procedures were adapted to ensure that reports were made directly to ISPs and the police in all cases.[29] At this point, the relevant ISP would then be effectively obliged to take down the material in question, being no longer able to assert that they

[27] KPMG Peat Marwick and Denton Hall, *Review of the Internet Watch Foundation*, 21.
[28] Ibid., 21.
[29] Ibid., 23.

were unaware of the material and as such potentially facing liability (whether as a principal or accessory) for its possession or distribution. In making determinations of possible illegality, the IWF were guided by training and advice from the Metropolitan Police and also received informal feedback from the police on the action taken on foot of reports.[30]

The hotline was launched by the IWF in December 1996 and soon began to process public complaints – starting relatively slowly with 1,291 complaints in the first full year of operation but rapidly building up to 4,297 complaints in 1999 following the introduction of a web based reporting system.[31]

(iv) Governance and funding

Between 1996 and April 1997 the IWF was run on an interim basis by a steering group comprised of the IWF Chief Executive and members from the DTI, Home Office, ISPA and LINX.[32] Following an agreement with government and the industry representatives, governance was put on a more permanent basis with the creation of a two tier structure under which the IWF had both an Industry Board and a Policy Board.

The Industry Board represented the funders (from the internet industry), and had control of financial matters and the day to day operation of the IWF. Membership of that Board and voting rights were based on financial contributions. The Policy Board on the other hand was a weaker, primarily advisory body comprised of individuals representing various stakeholders and constituencies (such as children's groups, consumer interests, and other media regulators), who were appointed on the basis of personal invitation from

[30] Ibid., 46.
[31] Internet Watch Foundation, 'IWF Highlights', *Internet Watch Foundation*, 2011, http://www.iwf.org.uk/about-iwf/iwf-history/iwf-highlights.
[32] KPMG Peat Marwick and Denton Hall, *Review of the Internet Watch Foundation*, 57.

the Industry Board.[33] In 1999 these included representatives from the British Educational Communications Technology Agency (BECTa), NCH Action for Children, the Video Standards Council, the Independent Committee for the Supervision of Standards for Telephone Information Services (ICSTIS), the Independent Television Commission (ITC), the Department of Trade & Industry, the Home Office, the Commission for Racial Equality, the National Consumer Council and ChildNet International.[34]

Start-up funding was provided by Peter Dawe, founder of Pipex (the first commercial UK ISP), who established the IWF as a wholly owned subsidiary of the Dawe charitable trust and through that trust funded the setting up and initial running costs. Thereafter, running costs were provided by the industry members – by 1999 comprising LINX, Demon, UUNET, BT, ISPA UK, LineOne, Cable & Wireless and NTL Internet.[35]

4. DTI / Home Office Review

In March 1998 the Department of Trade and Industry (DTI) and the Home Office jointly announced that they intended to review the work of the IWF, with the objective being:

> to receive a detailed review of the IWF and its work, in order to ensure that forward planning is based on a sound understanding of the current situation and likely future evolution of the Internet and its use in the UK – together with the impact this will have on the occurrence of illegal or offensive material.[36]

The review was conducted by consultants KPMG and Denton Hall who published a report in 1999 which endorsed the core elements of the IWF self-regulation model but made a number of recommendations for change. In particular, the report considered whether the remit of the IWF should be widened. While rejecting arguments that the

[33] Roger Darlington, 'Chairing The Internet Watch Foundation', *Roger Darlington's Homepage*, accessed 21 July 2009, http://www.rogerdarlington.co.uk/iwf.html.
[34] KPMG Peat Marwick and Denton Hall, *Review of the Internet Watch Foundation*, 58–59.
[35] Ibid., 58.
[36] Ibid., 8.

IWF should extend its work into areas such as fraudulent advertising and copyright infringement, the review did conclude that it should widen its remit in respect of illegal racist material.[37] It also recommended that the IWF should take on a new function in relation to newsgroups, by playing a more proactive role in removing illegal material from Usenet and advising ISPs to voluntarily ban newsgroups which it had consistently identified as hosting illegal images.[38]

In addition, the report identified the industry-dominated structure of the IWF as a hindrance and recommended that the "public role" of the body should be reflected by a strengthened Policy Board which would have an independent chairman and a majority of members from other public bodies or charities and which would replace the Industry Board in managing the day to day activities of the IWF. The Industry Board would, in turn, be downgraded to an Industry Committee (later to become known as the Funding Council) which would represent industry interests and would report to ISPs to agree ongoing funding levels for the IWF's work.[39]

5. Changes at the IWF

(i) Relaunch

These recommendations were accepted by the IWF, which in January 2000 was relaunched with a new governance structure. This introduced a revised Board (with a new Independent Chair, Roger Darlington) including four industry and eight independent members, with a separate Funding Council comprising all the member companies (then nine).[40]

[37] Ibid., 5.
[38] Ibid., 53.
[39] Ibid., 6.
[40] Internet Watch Foundation, 'IWF Highlights'.

(ii) Extended remit

Following the review recommendation, the IWF also implemented a wider role in relation to potentially criminal racist material, following consultations with the Home Office, CRE, Metropolitan Police, National High Tech Crime Unit and the CPS. Under this, the state authorities agreed to provide the IWF with "a careful analysis of the relevant law, a study of the relevant off-line court cases, and a mechanism for consulting the prosecuting authorities" – in effect replicating and also somewhat expanding the existing relationship between the IWF and the Metropolitan Police in respect of child pornography and obscenity.[41] In turn, the IWF would then advise ISPs to remove racist material which it determined to be illegal.

(iii) Governance and funding

The IWF re-launch also led to a new understanding of its status, which according to Darlington was "acting in a quasi-regulatory role on matters of great public interest" so that it should commit itself to higher standards of governance and transparency.[42] This manifested itself first in 2000 in a commitment to publish board papers and minutes on the web site.[43] In April 2001 the IWF board also declared itself to be bound by the Human Rights Act 1998, stating that:

> The IWF accepts the principles of the European Convention on Human Rights and undertakes to be governed subject to the Human Rights Act on the basis that it should be treated as a public body.

The same board meeting also determined to adopt governance standards from the public sector, resolving that:

[41] Darlington, 'Chairing The Internet Watch Foundation'.
[42] Ibid.
[43] Internet Watch Foundation, '2000 Annual Report', 2001. Unfortunately, while board minutes continue to be published board papers are no longer available.

> The IWF accepts the Good Regulation Principles published by the Cabinet Office Regulatory Impact Unit, and undertakes that its policies and actions should be guided by those principles.[44]

On the funding front, there were also a number of developments at this time. In relation to government funding, the board adopted a policy that such funding was acceptable in principle but only in relation to specific projects or campaigns endorsed by the board – general government subscriptions would not be accepted.[45] Funding from Europe did not, however, meet the same degree of concern and from June 2000 extensive funding was received from the EU towards the hotline service under the Safer Internet Action Plan.[46]

(iv) Formalising of IWF role

The final significant development following the re-launch of the IWF was a formalising of its role and the provision of a statutory defence to the possible offence of making indecent photographs of children. As discussed in chapter 2 the IWF as initially established was vulnerable to such charges under the Protection of Children Act 1978, which did not provide a public interest defence in respect of the making offence. Following input from the IWF, section 46 of the Sexual Offences Act 2003 provided such a defence and its application to the IWF was confirmed by a 2004 Memorandum of Understanding between the CPS and ACPO which specifically permitted the making of reports to the IWF as a "relevant authority" for the purposes of that Act.[47]

At this point, therefore, the essential elements of the current structure were in place. While there have been changes since – notably in 2005 when it restructured in order to

[44] See Akdeniz, *Internet Child Pornography and the Law*, 264.
[45] Internet Watch Foundation, 'Board Minutes 25 April 2001', 25 April 2001.
[46] Internet Watch Foundation, 'Board Minutes 12 July 2000', 12 July 2000, http://web.archive.org/web/20020223200050/http://www.iwf.org.uk/about/board/board120700.htm.
[47] Crown Prosecution Service and Association of Chief Police Officers, 'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003', 6.

secure charitable status[48] and again in 2011 when incitement to racial hatred was removed from its remit[49] – in broad terms the IWF has maintained a similar form of governance, and in particular continues to be funded in part by industry and in part by the EU.

6. Newsgroups: from take-down of posts to banning groups

(i) Introduction

The early role of the IWF in respect of newsgroups was relatively limited. In particular, it did not go nearly as far as the Metropolitan Police had demanded in their letter of August 1996 when it had requested that 133 newsgroups should be banned outright. Instead, at the outset the IWF restricted itself to considering the legality of individual posts.[50]

This approach remained, however, the subject of considerable pressure from government and children's lobby groups and, as has already been seen, the DTI/Home Office Review called for a move towards the outright banning of newsgroups. This continued pressure led to difficulties for the IWF following its re-launch, causing a controversy which spread over two years, led to accusations of censorship, and in many ways presaged the later debates over the adoption of the Cleanfeed system.

(ii) Statistical reports to ISPs

In October 2000 the new Chair, following the DTI/Home Office Review recommendations, began a consultation process on newsgroup policy. Following a lengthy and extensive debate – including external consultation and consideration of the

[48] Registered charity number 1112398.
[49] This responsibility was transferred to an ACPO run service at www.report-it.org.uk. See Internet Watch Foundation, 'IWF Highlights'.
[50] Akdeniz, *Internet Child Pornography and the Law*, 256–257.

governance and Article 10 EHCR issues – the board adopted in July 2001 a compromise position which fell short of "banning" newsgroups, but recommended that ISPs should review their policies on which groups they carried, and established a system for providing ISPs with a monthly statistical report indicating how many illegal items were carried within each group. This board meeting also considered – but rejected – a proposal to harness consumer pressure by establishing a list of ISPs which blocked access to these groups (and thus implicitly challenging those which did not).[51]

(iii) Banning newsgroups

The compromise approach adopted in July 2001 was promptly rejected by children's charities and by the Home Office, which wrote to the IWF immediately thereafter calling for the IWF to adopt a list of newsgroups to be blocked and continued to apply intense pressure over the summer of 2001.[52] In the view of the Chair, this issue had the potential to threaten the basis of the IWF, so that there was a risk of a loss of government support and possible government intervention:

> Of course, the IWF is a self-regulatory model, which is independent of government. However, self-regulation can only work if we have the respect and support of government. My concern is that, if we do not take early steps to take on board the concerns of the children's groups and the public and to reflect the changing opinion among many ISPs themselves, we will lose the confidence of key stakeholders, most notably government itself. If that happens, at best we will become increasingly less relevant and proposals such as an Internet clearing house will pass us by and, at worse, government will be inclined to intervene in a manner which will negate the self-regulatory model and be very unwelcome to the ISP community.[53]

As a result of this pressure, board meetings in November 2001 and subsequently in 2002 and 2003 abandoned the approach adopted in July and instead endorsed policies which established a system for identifying groups which "regularly contained" child

[51] Internet Watch Foundation, 'Board Minutes 18 July 2001', 18 July 2001, http://web.archive.org/web/20040810233237/http://www.iwf.org.uk/about/policies/minutes_180701.html; Roger Darlington, 'IWF Newsgroup Policy', 18 July 2001, http://web.archive.org/web/20040308014713/http://www.iwf.org.uk/about/policies/ngpolrep.htm.
[52] Darlington, 'Chairing The Internet Watch Foundation'.
[53] Ibid.

pornography, or which had "names judged to support or condone paedophilic activity". "Regularly" was in turn defined to mean that on average at least one percent of images contained in that newsgroup were determined to be illegal.[54] In respect of these groups, the IWF would recommend that ISPs block them, and steps would be taken towards a Code of Practice which would require all member ISPs to follow these recommendations. Consequently, although that Code of Practice was not eventually adopted until January 2004[55], the new policies amounted in substance to a ban on certain newsgroups which member ISPs were obliged to implement if they wished to remain members.[56]

(iv) Controversy

> The original purpose [of the IWF] was to sift out kneejerk reactions that were going to be counterproductive... amid concerns that the police would go wading in there banning newsgroups... Now it's trying to set itself up as a regulator and claim that it has some kind of legal clout.
>
> – Malcolm Hutty, 2001[57]

This change in policy sparked strong criticism from civil liberties advocates. Although there had been fears in 1996 that the IWF might take on a wide role in controlling internet content, these fears had largely been mitigated as time went on to the point where one free speech activist could describe the IWF as "mostly harmless".[58] Now, however, those fears were resurrected and critics claimed that the IWF was caving in to government pressure, going beyond its original remit, and doing so in a way which lacked any legal basis. In February 2002 Malcolm Hutty (who represented civil liberties

---

[54] Akdeniz, *Internet Child Pornography and the Law*, 256–257.
[55] Internet Watch Foundation, 'Code of Practice for Full Members', January 2004.
[56] For the legal advice as to Article 10 ECHR and whether the banning of newsgroups could be made a condition of membership see Internet Watch Foundation, 'Board Minutes 22 July 2003', 22 July 2003, http://web.archive.org/web/20040810234039/http://www.iwf.org.uk/about/policies/minutes_220703.htm; Darlington, 'IWF Newsgroup Policy'.
[57] Wendy McAuliffe, 'IWF Lambasted for Plan to Ban Newsgroups', *ZDNet.co.uk*, 19 July 2001, http://news.zdnet.co.uk/emergingtech/0,1000000183,2091634,00.htm.
[58] Wendy Grossman, 'Watching the Internet Watchers', *The Inquirer*, 15 February 2002, http://www.theinquirer.net/inquirer/news/1017543/watching-the-internet-watchers.

interests) resigned from the IWF board in protest.[59] To understand these criticisms, we must first distinguish between those groups blocked on the basis of their *names* and those blocked on the basis of their *content*.

(a) Names

In respect of newsgroups with certain names (for example, alt.binaries.pictures.lolita) their prohibition may have been an inevitable outcome in any event, with or without the IWF.[60] As the IWF notes:

> IWF received legal advice from the Crown Prosecution Service and from our own independent Standing Counsel that, a newsgroup name could, in certain circumstances, be an illegal advertisement under the Protection of Children Act 1978 and an ISP which knowingly carries such a group name will be committing an offence. Following the July 2002 Board meeting and based upon the legal advice, a list of newsgroup names was compiled and the recommendations resulting from this policy resulted in IWF advising UK ISPs they should not carry specific newsgroups because their names are potentially illegal advertisements.[61]

For this reason, the banning of newsgroups based on names involved relatively little controversy.

(b) Content

It was a different story, however, in relation to newsgroups blocked on the basis of content. Here critics pointed out that the criterion for blocking – whether an average of at least one percent of images contained in that newsgroup were determined to be illegal – presupposed banning newsgroups in which the overwhelming majority of content was perfectly legal.[62] At the time Hutty cited alt.binaries.pictures.gillian-anderson, alt.binaries.pictures.teen-idols.princewilliam and alt.binaries.pictures.spice-girls as

---

[59] Internet Watch Foundation, 'Board Minutes 12 February 2002', 12 February 2002, http://web.archive.org/web/20020403125653/http://www.iwf.org.uk/about/bd12-02mins.htm.
[60] This was certainly the view of counsel. See Anthony Hudson, 'Advice in Relation to Usenet Newsgroup Names and Website Addresses', 16 July 2002.
[61] Internet Watch Foundation, 'Newsgroups'.
[62] Akdeniz, *Internet Child Pornography and the Law*, 256–257.

examples of groups which would be banned as a result.[63] In addition, the secrecy behind the list of blocked newsgroups (which would not be made public) further fuelled suspicion.[64]

(c) Wider implications

Moving away from the newsgroup ban itself, however, the episode also gave rise to concerns about the overall nature of the new, re-launched, IWF. There was an undoubted irony in the fact that a body set up in order to avoid banning newsgroups now found itself doing just that. Critics charged that the new board structure meant that the IWF had been removed from its ISP roots, so that it was being "built up into a child protection lobby", ignoring civil rights concerns.[65] The growing powers of the IWF, coupled with its willingness to give into Home Office pressure and its new racist material remit, suggested to some that it was becoming a *de facto* state body which evaded the usual constraints imposed by public law.[66]

Consequently, although the change in policy had important practical benefits (freeing up analysts to deal with web-based content, rather than fighting a resource intensive and ultimately futile battle in respect of newsgroups[67]) it nevertheless meant that the IWF brand name was significantly dented with a great deal of goodwill lost and stakeholders alienated.[68]

---

[63] Grossman, 'Watching the Internet Watchers'.
[64] Wendy Grossman, 'IWF: What Are You Looking At?', *The Independent*, 25 March 2002, http://www.independent.co.uk/news/business/analysis-and-features/iwf-what-are-you-looking-at-655425.html.
[65] Ibid.
[66] McAuliffe, 'IWF Lambasted for Plan to Ban Newsgroups'.
[67] Marsden, *Internet Co-Regulation*, 157.
[68] Internet Watch Foundation, 'Chief Executive's Report 14 May 2002', 14 May 2002, http://web.archive.org/web/20020820125010/http://www.iwf.org.uk/about/CEO05-02.htm.

7. Web blocking

Despite this extension of the IWF's remit, child protection advocates were still dissatisfied with the extent to which child pornography was available within the UK. They argued that although the use of Usenet had been disrupted, child pornography was beginning to move to websites which were hosted outside the UK and therefore beyond the reach of police or the IWF.[69] Consequently, there was some interest on their part in devising a way of blocking access to these sites for UK users.[70]

(i) BT takes the initiative

As we have already seen, 2001-2002 was a time of intense political pressure on the IWF. This was, however, merely one part of wider government pressure on the industry. The then Home Secretary, Jack Straw, began in March 2001 by establishing a taskforce on improving child protection on the internet, challenging ISPs to go beyond the existing work of the IWF.[71] The Home Office then followed this up in May 2001 with a proposal for a government funded "kitemark" scheme for ISPs, which would have provided a star rating for ISPs based on a child safety checklist – marking down and exerting consumer pressure on those ISPs which didn't take steps to prevent access to child pornography online. The political urgency was enhanced by the June 2001 general election, in which child protection was a significant Labour manifesto commitment.[72]

Nick Truman, then head of internet and customer security at BT, indicates that this initiative of Jack Straw prompted BT to begin work on developing a blocking system which would prevent users from accessing child pornography on the web (not merely

[69] John Carr, *Child Abuse, Child Pornography and the Internet* (London: NCH, 2004), 18–19, http://www.make-it-safe.net/esp/pdf/Child_pornography_internet_Carr2004.pdf.
[70] Martin Bright, 'BT Puts Block on Child Porn Sites', *The Observer*, 6 June 2004, http://www.guardian.co.uk/technology/2004/jun/06/childrensservices.childprotection.
[71] Home Office, 'Press Release: Improving Child Protection on the Internet - A Partnership for Action', 29 March 2001, http://www.cyber-rights.org/documents/safe_uk.htm; Nick Truman, Telephone interview, 8 February 2010.
[72] Ost, *Child Pornography and Sexual Grooming*, 17.

Usenet).[73] Blocking of child pornography websites had been tried elsewhere but had been hampered by technological limitations which caused massive over blocking – that is, collateral damage to innocent sites which were also blocked.[74] However, with the rollout of broadband enabling new approaches to be taken, BT felt that more targeted blocking was possible.

With high level support from within BT, substantial funding (ultimately totalling approximately one million pounds) was given to a project to devise a web blocking system.[75] Under the internal title "Cleanfeed" it put together a two stage filtering system intended to minimise both false positives and slowdown of connections by looking at the more granular level of individual URLs rather than domain names or IP addresses.[76]

(ii) Securing use of the IWF URL list

Having conceived this system, BT also needed to identify which URLs to block. The obvious (and indeed only) source was the IWF, which had generated a database of URLs hosting child pornography as a result of its hotline function. There was, however, initial reluctance on the part of the IWF which changed only when Peter Robbins took over as chief executive and was more supportive of the project.[77]

Legal advice was given in November 2002 indicating that the IWF could make this list of illegal URLs available to members for the purpose of blocking images to protect customers from inadvertent exposure, and it was decided at that point that the URL list

[73] Truman, Telephone interview.
[74] See the discussion in Zittrain, 'Internet Points of Control'.
[75] Hutty, 'Cleanfeed: The Facts'.
[76] Richard Clayton, 'Failures in a Hybrid Content Blocking System' (presented at the Workshop on Privacy Enhancing Technologies, Dubrovnik, 30 June 2005), http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.
[77] Truman, Telephone interview.

would be provided to member ISPs, subject to safeguards being put in place to control access to and dissemination of the list.[78]

There were, however, a number of obstacles to be overcome before the system could be deployed. According to Truman, BT was worried about the possible implications of blocking and therefore enlisted the Home Office in the development of the system for the purpose of "political cover". In particular, there was a concern that wrongful blocking might take place – exposing them to liability (either reputational or financial) if, for example, a Microsoft domain were put on the list.[79] For that reason, BT sought to build in a number of safeguards into the system. Following negotiations with the Home Office and the IWF, BT established the following principles which would govern its use of the URL list:

> BT does not log the IP addresses of users whose traffic is an attempt to reach a listed URL.
>
> BT has agreed with IWF and the Home Office that an independent academic audit shall be made of IWF's processes and procedures so as to ensure that it is capable of meeting the standards that it has set for itself.
>
> As this is an audit of procedures this shall not include examination of any individual decisions with regard to particular URLs.
>
> The audit report will be made to the Chair and Chief Executive of the IWF. The Home Office will receive a copy of the audit report. BT will not receive a copy.
>
> BT has agreed with the IWF and the Home Office that an independent appeals process shall be created for use by persons whose own sites appear on the IWF's database and who wish to challenge that designation.
>
> The adjudicator shall be appointed by POLIT, a unit within the National Crime Squad dedicated to online paedophilia.
>
> BT will not confirm whether a particular site is indeed listed (and, indeed, does not know). The "HTTP status code 404" response is specifically designed to hide from the user that access has been blocked.[80]

[78] Internet Watch Foundation, 'Child Sexual Abuse Content URL List', 10 April 2008, http://www.iwf.org.uk/corporate/page.49.233.htm.
[79] Truman, Telephone interview.
[80] Hutty, 'Cleanfeed: The Facts'.

The statement that BT would not log IP addresses was particularly significant, as there was some police interest at the time in using the system to identify users – this had been made impossible, however, by a deliberate design choice on the part of BT in order to maintain the system as a means of abuse management rather than an investigative or prosecution tool.[81]

(iii) Cleanfeed deployed

The BT system was trialled in 2004. Initially this was done quietly, reflecting a BT decision that Cleanfeed would not be used as a marketing tool.[82] This, however, soon changed when the children's charity with which BT was working on the system leaked its existence with the aim of generating political pressure on other ISPs to adopt similar systems.[83]

The result was intense media interest, not least as leaked figures claimed that the system was blocking "20,000 hits per day", something which the media took to mean that thousands of UK users were attempting to view child pornography.[84] Unfortunately the actual number could not be verified as the steps which BT had taken in designing the system (for example, not logging the IP addresses which attempted to reach a blocked site) ensured that no conclusive analysis of the figures could be carried out.[85] However, the headline figure was at the least very misleading as a substantial portion of this traffic appeared to be generated by spam, pop-ups, foreign users abusing UK proxies and other sources.[86]

---

[81] Truman, Telephone interview.
[82] Ibid.
[83] Hutty, 'Cleanfeed: The Facts'.
[84] Ibid.
[85] Truman, Telephone interview.
[86] Richardson, 'ISPA Seeks Analysis of BT's "Cleanfeed" Stats'; Tim Richardson, 'BT on Child Porn Stats', *The Register*, 22 July 2004, http://www.theregister.co.uk/2004/07/22/bt_ispa_cleanfeed/.

Following the leak, other ISPs were caught off-guard and were keen to play down the functionality of Cleanfeed as they came under pressure to deploy similar systems. ISPA in particular briefed the media as to the limitations of the system and the potential collateral damage which it might cause, and also questioned the reliability of the leaked statistics showing the claimed success of the BT system with a view to showing the continued effectiveness of the existing notice and take down system.[87] The reasons behind ISP unwillingness to follow suit were varied, but included a mix of concerns about cost (which would be particularly high on a per-subscriber basis for smaller ISPs), function creep, loss of mere conduit status and concerns about wider freedom of expression implications.[88]

8. Pressure to adopt blocking systems

(i) Partial industry rollout of "Cleanfeed" systems

Unsurprisingly, following the apparent success of this trial and the proof of concept it provided, there soon followed calls for other ISPs to follow BT's example and to filter against the IWF URL list. In this, children's charities were joined by the Home Office and by backbench MPs who kept the spotlight on ISPs. One prominent advocate was Margaret Moran MP who used the Ten Minute Rule to introduce a bill in October 2005 which would have compelled ISPs "to declare publicly whether or not they have taken, or are taking, appropriate technical steps to block access to web sites that contain child pornography" – framing the issue as one of corporate social responsibility and

[87] John Leyden, 'BT's Modest Plan to Clean up the Net', *The Register*, 7 June 2004, http://www.theregister.co.uk/2004/06/07/bt_cleanfeed_analysis/; Richardson, 'ISPA Seeks Analysis of BT's "Cleanfeed" Stats'; Richardson, 'BT on Child Porn Stats'.
[88] Mark Gracey, 'Censorship or Common Sense?' (presented at the Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities, Oxford Internet Institute, 8 September 2005), http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/mark_gracey.pdf.

accountability to the public, and seeking to muster consumer pressure against those ISPs who were said to be failing in their duty.[89]

Faced with extensive political pressure to block, for the most part ISPs agreed to do so. Where they did publicly express any reluctance it was generally to cite commercial and practical rather than principled concerns. Consequently, by early 2006 most of the major ISPs had adopted blocking systems, with approximately 80% of UK domestic users being covered.[90]

(ii) Legislation threatened

This, however, was still not acceptable to advocates of blocking. John Carr of children's charity NCH, who had been involved in the development of Cleanfeed, was the most visible proponent of extending the remit of filtering and claimed that the failure to achieve 100% coverage showed that internet self-regulation had reached "its outer limits", making legislation a necessity.[91] This call was soon taken up by the Home Office, which signalled in May 2006 an intention to introduce legislation unless 100% coverage was achieved "voluntarily" by the end of 2007.[92]

This pressure did encourage more ISPs to adopt filtering, and by early 2009 approximately 95% coverage had been achieved.[93] A number of smaller ISPs, however, remained outside the filtering system citing both cost and the ineffectiveness of the system against "paedophiles with minimal technical knowledge" using "simple technical

[89] Ingrid Marson, 'Child Porn: ISP Regulations Set for Commons Debate', *Silicon.com*, 26 July 2005, http://www.silicon.com/management/cio-insights/2005/07/26/child-porn-isp-regulations-set-for-commons-debate-39150769/.
[90] Sean Hargrave, 'Surfing with a Safety Net', *The Guardian*, 29 June 2006, http://www.guardian.co.uk/technology/2006/jun/29/guardianweeklytechnologysection.
[91] 'BT Sounds Child Web Porn Warning', *BBC News*, 7 February 2006, http://news.bbc.co.uk/1/hi/uk/4687904.stm.
[92] Hargrave, 'Surfing with a Safety Net'.
[93] 'Online Child Abuse Images Warning', *BBC News*, 23 February 2009, http://news.bbc.co.uk/1/hi/technology/7904607.stm.

counter-measures".[94] In response, the Home Office drew up plans to introduce legislation which would "compel domestic ISPs to implement the blocking of illegal images of child sexual abuse", to be flagged in the Queen's Speech in November 2009.[95]

(iii) Mandatory blocking abandoned

Perhaps surprisingly, however, those plans appeared to meet with little support elsewhere in the official community. Jim Gamble – chief executive of the specialist police Child Exploitation and Online Protection Centre (Ceop) – stated that the existing blacklist was a "fabulous success" but that it was essentially limited to inadvertent or novice access and ineffective against "hardcore predators". Instead, he claimed, the problem had largely moved on from websites and towards peer to peer networks, so that he was unconvinced of the need to legislate.[96]

Similarly, the All Party Parliamentary Communications Group (apComms) came out against mandatory blocking in their October 2009 report "Can we keep our hands off the net?" In that report they pointed out the limitations of the system – in particular, that it was primarily intended to protect against innocent exposure – and recommended against legislation on the basis that it would be counterproductive and would deter industry from taking part in future self-regulatory schemes.[97]

Not long afterwards the Home Office abandoned plans to legislate, on the basis that an Ofcom survey had revealed that 98.6% of connections were filtered, which they claimed demonstrated that voluntary compliance was substantially working. It did, however,

---

[94] Chris Williams, 'Small ISPs Reject Call to Filter out Child Abuse Sites', *The Register*, 25 February 2009, http://www.theregister.co.uk/2009/02/25/iwf_small_isps/.
[95] Jane Merrick, 'Internet Providers Face Child Porn Crackdown', *The Independent*, 6 September 2009, http://www.independent.co.uk/news/uk/crime/internet-providers-face-child-porn-crackdown-1782530.html.
[96] Chris Williams, 'New Web Filter Laws Questioned by Top Child Abuse Cop', *The Register*, 9 September 2009, http://www.theregister.co.uk/2009/09/09/ceop_iwf/.
[97] All Party Parliamentary Communications Group, *Can We Keep Our Hands off the Net? Report of an Inquiry by the All Party Parliamentary Communications Group*, 11.

secure a concession from the industry in return, in the form of a commitment that the IWF would publish a list of ISPs who were certified as having implemented the blacklist, to facilitate consumer pressure as a means of encouraging compliance amongst the remaining ISPs.[98]

The Government has also committed to using its own purchasing power to encourage take-up, and since March 2010 requires suppliers of internet services to deploy the IWF blacklist in respect of any services provided to departments, agencies or quangos.[99] Although this only requires suppliers to filter those services which are provided directly to public bodies, in practice it is likely to encourage filtering on other services also.

9. URL list scope

The URL list is limited to "child sexual abuse images", by which the IWF means those images prohibited by the Protection of Children Act 1978 as amended by the Sexual Offences Act 2003.[100] This does not include other material falling within the remit of the IWF such as criminally obscene adult content or "extreme pornography". Nor, significantly, does it include all forms of "child pornography" prohibited by UK law – non-photographic images of children ("virtual child pornography") have not been included by the IWF within the blocking system, due to concerns that inclusion of such images would significantly increase the reputational risks to the IWF and members and would make the blocking system unworkable.[101] This undermines the argument that the

[98] Chris Williams, 'Home Office Backs down on Net Censorship Laws', *The Register*, 16 October 2009, http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.
[99] See 'Procurement Policy Note – Blocking access to web pages depicting child sexual abuse. Action Note 05/10', discussed in Sean O'Neill, 'Government Ban on Internet Firms That Do Not Block Child Sex Sites', *The Times*, 10 March 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece.
[100] Internet Watch Foundation, 'FAQs Regarding the IWF's Facilitation of the Blocking Initiative'.
[101] Internet Watch Foundation, 'Board Minutes 29 September 2009', 29 September 2009.

IWF merely implements the law as it stands by highlighting a significant discretion on its part as to which parts of the law it will implement via blocking.[102]

10. Use of the URL list in other situations and jurisdictions

While we have so far described the use of the URL list in the context of UK consumer ISPs, it should be noted that it has been adopted far more widely. The IWF licence permits members to make use of the list for blocking outside the UK, and as a result there is a significant spill over effect to ISPs in many other countries (such as Ireland) where the IWF list is used in the absence of a local list.[103] In addition, the list is widely used in home, workplace and school filtering software and is also used by search engines (including both Google and Bing) on a worldwide basis to remove URLs from search results.[104] When considered in terms of numbers of users covered, therefore, the IWF list is likely to be the most widely used blocking list ever. English law is, in effect, being exported – in a way which may block content which might be legal in other jurisdictions.

11. The Wikipedia block and its aftermath

(i) Criticisms of the Cleanfeed system

Soon after BT's Cleanfeed trial was leaked it came in for criticism. The covert and extra-judicial nature of the system coupled with the potential for function creep triggered

[102] John Ozimek, 'IWF Takes "Pragmatic" Stance on Level One Images', *The Register*, 10 September 2009, http://www.theregister.co.uk/2009/09/10/iwf_policy_clarification/.
[103] See e.g. GSMA Mobile Alliance Against Child Sexual Abuse Content, 'Implementation of Filtering of Child Sexual Abuse Images in Operator Networks', November 2008, www.gsmworld.com/documents/GSMA_Child_Tech_Doc.pdf.
[104] Internet Watch Foundation, 'IWF URL List Recipients', *Internet Watch Foundation*, 2011, http://www.iwf.org.uk/services/blocking/iwf-list-recipients; Committee on Energy and Commerce, *Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites.* (Washington, DC: US Government Printing Office, 2006), http://ftp.resource.org/gpo.gov/hearings/109h/30530.txt.

concerns in a way which essentially reprised the newsgroups debate three years prior.[105] These criticisms were amplified over the following years – especially in 2006 and 2007 – after Home Office plans to achieve 100% coverage came to light.[106] Even quite moderate commentators were prompted to argue, in the words of Edwards, that "[i]f Cleanfeed-style technology is imposed on all UK ISPs – by law or voluntarily – it could be the most perfectly invisible censorship mechanism ever invented" – but, as Edwards also went on to note, these criticisms were limited to a relatively small technical and academic community and had achieved almost no public awareness.[107]

(ii) Blocking of Wikipedia

> Journey with us to a state where an unaccountable panel of censors vets 95 per cent of citizens' domestic internet connections. The content coming into each home is checked against a mysterious blacklist by a group overseen by nobody, which keeps secret the list of censored URLs not just from citizens, but from internet service providers themselves. And until recently, few in that country even knew the body existed. Are we in China? Iran? Saudi Arabia? No – the United Kingdom, in 2009. This month, we ask: Who watches the Internet Watch Foundation?
>
> – CJ Davies, 2009[108]

The situation changed significantly on Friday 5th December 2008, when parts of the encyclopaedia website Wikipedia effectively vanished from the United Kingdom internet.[109] On that day ISPs serving the overwhelming majority of UK internet users simultaneously blocked access to particular pages, bringing public attention to the filtering system in a dramatic fashion.[110]

---

[105] Hunter, 'BT's Bold Pioneering Child Porn Block Wins Plaudits amid Internet Censorship Concerns'; Bright, 'BT Puts Block on Child Porn Sites'.
[106] Hargrave, 'Surfing with a Safety Net'.
[107] Edwards, 'From Child Porn to China, in One Cleanfeed'.
[108] Davies, 'The Hidden Censors of the Internet'.
[109] Rupert Goodwins, 'UK ISPs Switch on Mass Wikipedia Censorship', *ZDNet.co.uk*, 6 December 2008, http://community.zdnet.co.uk/blog/0,1000000567,10009938o-2000331777b,00.htm.
[110] The ISPs in question included Virgin Media, Be Unlimited/O2/Telefonica, EasyNet/UK Online, PlusNet, Demon, and Opal, covering what was estimated at 95% of UK internet users. See 'Administrators' noticeboard/2008 IWF Action', *Wikipedia*, 2008, http://en.wikipedia.org/wiki/Wikipedia:Administrators%27_noticeboard/2008_IWF_action.

Following a complaint from a user to the hotline, the IWF had determined that a Wikipedia image of a 1976 album cover ("Virgin Killer" by German heavy-metal band The Scorpions) featuring a naked pre-pubescent girl was potentially illegal as an indecent image of a child under the age of 18. As a result, it added two URLs to the blacklist. (Though due to a technical mistake, neither URL blocked the image itself but rather webpages containing the image. The image itself remained available to UK users throughout.[111])

This, in and of itself, may not have been likely to cause a great controversy. The pages blocked – relating to an obscure German heavy metal album – were not of great inherent interest to the UK internet community. What was significant, however, was an unintended side effect of the blocking. By virtue of the technical approach most UK ISPs adopted, *all* traffic for any Wikipedia page or edit (not just for the two URLs) suddenly passed through a small number of ISP proxy servers. The result was to make it appear to Wikipedia that it was coming under attack from a narrow range of IP addresses. Wikipedia responded with automated counter-measures which prevented those IP addresses – and therefore almost all UK users – from editing pages or creating new accounts. As a result, Wikipedia users rapidly identified the existence of the block and were soon able to track down the URLs which had been blocked and to identify the "offending" image.[112]

(iii) IWF stands over the blacklisting

Soon after the blocking started, the IWF confirmed that it was responsible. It issued a statement indicating that it had received a complaint in respect of the pages. On viewing them, it had determined that the album cover was "a potentially illegal indecent image of a child under the age of 18" and as such it was added to the blacklist provided to ISPs

[111] Richard Clayton, 'Technical Aspects of the Censoring of Wikipedia', *Light Blue Touchpaper*, 11 December 2008, http://www.lightbluetouchpaper.org/2008/12/11/technical-aspects-of-the-censoring-of-wikipedia/.
[112] Ibid.

"to protect their customers from inadvertent exposure" to such images.[113] On being contacted by the Wikimedia Foundation (which runs Wikipedia) the IWF stood over the blocking, stating that it had carried out an appeals process which had confirmed the original decision.[114]

This did not dampen what had become an increasingly heated issue amongst UK internet users, many of whom had viewed the image and saw it as unobjectionable – and who pointed out that the album image remained unblocked on many other websites such as Amazon. Instead by confirming the existence of widespread filtering it heightened the controversy, causing many to ask how a private body with no legislative basis had become a *de facto* arbiter of legality for the UK internet. The result was a storm of publicity[115] in the mainstream media, much of which was critical of the IWF.[116]

(iv) IWF backs down

Ultimately, this controversy forced the IWF to back down and to withdraw the Wikipedia pages from its blacklist just four days later following an emergency board meeting.[117] Though it still asserted that the image in question was "potentially in breach of the Protection of Children Act 1978" and had been properly listed in the first place, nevertheless it varied policy so that the URLs would be removed from the list given the

[113] Cade Metz, 'Brit ISPs Censor Wikipedia over "Child Porn" Album Cover', *The Register*, 7 December 2008, http://www.theregister.co.uk/2008/12/07/brit_isps_censor_wikipedia/.
[114] Davies, 'The Hidden Censors of the Internet'.
[115] See e.g. Nicole Martin, 'Wikipedia Founder Considers Legal Action over Ban on "Pornographic" Album Cover', *The Telegraph*, 9 December 2008, http://www.telegraph.co.uk/technology/3689527/Wikipedia-founder-considers-legal-action-over-ban-on-pornographic-album-cover.html; 'Wikipedia Child Image Censored', *BBC News*, 8 December 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.
[116] See e.g. Bobbie Johnson, 'Wikipedia Falls Foul of British Censors over Alleged Child Pornography', *The Guardian*, 8 December 2008, http://www.guardian.co.uk/technology/2008/dec/08/wikipedia-censorship.
[117] Internet Watch Foundation, 'Board Minutes 9 December 2008'.

"contextual issues involved in this specific case" and "the length of time the image has existed and its wide availability".[118]

(v) Lessons from the Wikipedia block

What should we make of this incident? The short duration of the block, and the relatively insignificant nature of the content blocked, might make it seem rather minor. Significantly, however, it exposed to public scrutiny a hitherto low profile blocking system and highlighted a debate which had previously been the preserve of a small number of industry observers, child protection advocates, academics and journalists.[119] In doing so, it also raised fundamental questions about the nature of the system which had previously escaped detailed scrutiny. While it did not itself stop Home Office plans for mandatory blocking (which continued into 2009) it may have contributed to the lukewarm reception such plans received elsewhere in government.

(a) Legitimacy and procedural safeguards

Borderline images

At the very outset, by drawing attention to the borderline nature of images which would be adjudicated on (and the fact that the IWF acted on the basis of "potential illegality") the incident undermined the reputation which the IWF had built up as a reliable arbiter of legality. As Ozimek notes:

> [T]he scene was set for the IWF to take a fall. Gone is its record for 100 per cent undisputed blocking. Gone, too, is its reputation for being the undisputed good guy. Many people have looked at the image in question and have taken the view that it is not porn, or indecent, or abuse.

[118] Cade Metz, 'IWF Pulls Wikipedia from Child Porn Blacklist', *The Register*, 10 December 2008, http://www.theregister.co.uk/2008/12/10/iwf_reverses_wikiban/.

[119] Early participants in this debate included Edwards, Hargrave and Grossman. See e.g. Edwards, 'From Child Porn to China, in One Cleanfeed'; Hargrave, 'Surfing with a Safety Net'; Wendy Grossman, 'The Great Firewall of Britain', *Net.wars*, 24 November 2006, http://www.pelicancrossing.net/netwars/2006/11/the_great_firewall_of_britain.html.

> Having made that judgement, they have started to ask questions about other imagery that the IWF has sought to block.[120]

It should be said, in fairness to the IWF, the fault here is primarily with the law itself. As we have already seen, there have long been complaints that the law is vague and overbroad in its terms and indeed has led to raids on art galleries.[121] Nonetheless, when the public took the view that the blocking was unjustified then the IWF became the obvious target for criticism.[122]

Fair procedures

Also jeopardised was the integrity of the process operated by the IWF.[123] At the outset, BT had insisted on an appeals process being established by the IWF as a safeguard. Until the Wikipedia case that mechanism had never been tested.[124] On being tested, however, it proved unsatisfactory.

First, it provided a right of complaint only to those "responsible for the hosting or content" of the URL in question, with no remedy for the user who was wrongly denied access. This privileged the rights of the speaker over those of the recipient of speech and, in practical terms, made it substantially more likely that wrongful blocking will continue. A site owner, particularly if based outside the UK, may be entirely unaware of the blocking, much less the involvement of the IWF, and may have little interest in engaging with the intricacies of UK law to overturn the block.

---

[120] John Ozimek, 'Scorpions Tale Leaves IWF Exposed', *The Register*, 9 December 2008, http://www.theregister.co.uk/2008/12/09/iwf/.
[121] See chapter 2, sections 3(ii)(e) and 3(iii)(b).
[122] By comparison the 'worst of' list distributed by INTERPOL avoids many of these problems by restricting itself to 'severe' abuses and to children younger than 13 years: Interpol, 'Criteria for Inclusion in the List', accessed 25 February 2011, http://www.interpol.int/Public/THBInternetAccessBlocking/Criteria.asp.
[123] Outlined here as it stood in 2008: Internet Watch Foundation, 'Child Sexual Abuse Content URL Service: Complaints, Appeals and Correction Procedures', 7 December 2008, http://www.iwf.org.uk/public/page.148.341.htm.
[124] Charles Arthur, 'Internet Watch Foundation Reconsiders Wikipedia Censorship', *The Guardian*, 9 December 2008, http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-censorship-iwf-reconsiders.

Second, it did not provide for any appeal to a court or other independent tribunal – the assessment by police was not an adequate substitute. Police judgement in relation to the possible illegality of images of children has been criticised in a number of high profile cases involving material by prominent artists, highlighting the need for an independent and preferably judicial review.[125]

Third, the complaint mechanism did not provide for any right to make representations or to reply to any police input. In this case, therefore, it transpired that the "appeal" was carried out without the involvement of the "appellant". In the words of Mike Godwin, general counsel for the Wikimedia Foundation:

> When we first protested the block, their response was, 'We've now conducted an appeals process on your behalf and you've lost the appeal.' When I asked who exactly represented the Wikimedia Foundation's side in that appeals process, they were silent.[126]

Lastly, the Wikipedia block also highlighted that the appeals process is not in fact final but can be overruled by a decision of the Board in individual cases, creating a risk that the system will favour those with the deepest pockets or most vocal supporters.

To a large extent, the IWF claim to legitimacy was and is a procedural one, relying on the fact that it operates a formal mechanism for identifying material to be blocked, along with an appeals procedure. In this case, however, the apparently *ad hoc* nature of the decision-making – where the "appeal" was determined without any opportunity for Wikipedia to be heard and where the IWF Board eventually set aside the outcome of their own appeal mechanism – suggested that there were different rules in place for high profile sites.[127]

---

[125] For two examples see Higgins and Dodd, 'Tate Modern Removes Naked Brooke Shields Picture after Police Visit'; Reynolds, 'Sir Elton John's Young Girl Art'.
[126] Davies, 'The Hidden Censors of the Internet'.
[127] Lilian Edwards, 'IWF v. Wikipedia and the Rest of the World (except OUT-LAW)', *panGloss*, 15 December 2008, http://blogscript.blogspot.com/2008/12/iwf-v-wikipedia-and-rest-of-world.html.

(b) Parity of treatment for online/offline content

The Virgin Killer album had been available for purchase in the High Street for over 30 years. There had never been a prosecution relating to it.[128] Had such a prosecution been brought it would have been public and the subject of intense media coverage. A single complaint to the IWF, however, was enough to result in an immediate and secret nationwide block, with no notice to Wikipedia, which might well have gone unnoticed but for the technical side effects. This difference in treatment was, of itself, disturbing to those who believed in the principle that, as far as possible, there should be parity of treatment between the offline and online worlds.[129]

(c) Transparency

What did users see when they attempted to visit the blocked pages? The overwhelming majority of ISPs displayed deceptive error messages – usually a "404: File Not Found" error which falsely claimed that there was a technical problem at Wikipedia's end and intentionally obscured the involvement of the ISP.[130] In this regard, the episode reinforced earlier complaints about the secret nature of the system – particularly as blocking systems in Europe had, in the meantime, moved toward using block pages which notified users of the fact that a page had been blocked and the reason why.[131]

(d) Collateral damage

The claim that hybrid blocking systems (as implemented by BT) could block specific URLs with no collateral damage to innocent content was also shown to be overstated.[132]

---

[128] Internet Watch Foundation, 'Board Minutes 9 December 2008'.
[129] On online/offline equivalence see generally Maurice Schellekens, 'What Holds off-Line, Also Holds on-Line?', in *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, ed. Bert-Jaap Koops et al. (The Hague: TMC Asser, 2006).
[130] 'Administrators' noticeboard/2008 IWF Action'.
[131] See e.g. McIntyre, 'Blocking Child Pornography on the Internet'.
[132] Clayton, 'Technical Aspects of the Censoring of Wikipedia'.

This point was reemphasised just one month later – in January 2009 – when numerous UK users found themselves unable to access the Internet Archive's Wayback machine (an 85 billion page archive of internet history) as a result of one page on that site being put on the IWF blacklist.

As with the Wikipedia block, the blame was not to be laid directly at the door of the IWF – in this case, the overblocking resulted from one ISP's proxy server system and the way in which it interacted with the Internet Archive's caching system.[133] Nevertheless, this episode reinforced the point that blocking systems in general were prone to causing unpredictable collateral damage.

12. After Wikipedia: IWF changes in response

As with the newsgroups ban several years before, the IWF recognised that the Wikipedia had done substantial damage to its reputation. In response, under its new chair Eve Salomon[134] it took a number of steps to change the way in which URLs are blacklisted and the use of the list by ISPs, as well as to better communicate its aims and operation.

(i) Contextual assessment and blocking of images

One of the first changes was in relation to images such as the Virgin Killer album cover which were either of a borderline nature or presented some other risk (such as reputational or technical harm) if blocked. The IWF follows police practice by training analysts with reference to the Sentencing Guidelines Council classification[135] of

[133] Cade Metz, 'Brit Porn Filter Censors 13 Years of Net History', *The Register*, 14 January 2009, http://www.theregister.co.uk/2009/01/14/demon_muzzles_wayback_machine/; Cade Metz, 'IWF Confirms Wayback Machine Porn Blacklisting', *The Register*, 14 January 2009, http://www.theregister.co.uk/2009/01/14/iwf_details_archive_blacklisting/; Cade Metz, 'Demon Ends Porn-Less Internet Archive Block', *The Register*, 16 January 2009, http://www.theregister.co.uk/2009/01/16/demon_resolves_wayback_issue/.
[134] Appointed in April 2009.
[135] Sentencing Guidelines Council, 'Sexual Offences Act 2003: Definitive Guidance', April 2007, 109.

indecent photographs of children, under which such images fall under a five part scheme:

> Level 1 Images depicting erotic posing with no sexual activity
> Level 2 Non-penetrative sexual activity between children, or solo masturbation by a child
> Level 3 Non-penetrative sexual activity between adults and children
> Level 4 Penetrative sexual activity involving a child or children, or both children and adults
> Level 5 Sadism or penetration of, or by, an animal

Level 1 images – such as the image at the centre of the Wikipedia incident – clearly presented the greatest reputational risk to the IWF and consequently in January 2009 the board endorsed an emergency interim decision to stop automatically putting such images onto the URL list (except in cases where they were being sold commercially).[136] This subsequently hardened into a decision to apply a contextual assessment to images generally, which would address situations such as the Wikipedia case, so that decisions to block would be made on a case by case basis where there was a risk that blocking might trigger an undesirable outcome.[137] Under the new policy, therefore, decisions as to whether images were potentially illegal would take into account the context of the image (something which had been absent in the Wikipedia case) while decisions to block would also take into account the following criteria:

> Consideration will also be given to the following risks potentially associated with adding a URL to the IWF URL List i.e.
> a. Creation of significant problems for internet users.
> b. Creation of significant problems for list licensees.
> c. Likelihood of listing leading to increased availability of the image.
> d. Impact on the reputation of website owner and consequential impact on the IWF and its Members.

Where such risks are present, the matter will be referred to a committee of the board for its decision.

---

[136] Internet Watch Foundation, 'Board Minutes 27 January 2009', 27 January 2009, http://www.iwf.org.uk/accountability/governance/board-minutes/2009-board-minutes/27-january-2009.
[137] Internet Watch Foundation, 'IWF URL List Policy and Procedures', accessed 15 February 2011, http://www.iwf.org.uk/services/blocking/iwf-url-list-policy-and-procedures.

(ii) Prioritising takedown

A second strand of the response was to give greater prominence to the removal of images at source where possible. A longstanding criticism of Cleanfeed and other blocking systems has been that they create a tendency to use a relatively easy tactic – blocking – rather than the more difficult but much more desirable approach of developing international cooperation and takedown of images at source.[138] The IWF had already taken some steps towards greater international cooperation[139] but following the Wikipedia blocking these intensified, with greater focus being placed on developing relationship with hosting companies abroad and in the US in particular.[140] Significantly, this new approach includes a commitment to seek to takedown images where possible.[141]

(iii) Transparency

One of the ways in which the Wikipedia block most harmed the reputation of the IWF stemmed from the lack of transparency associated with the blocking system. In addition to governance concerns, the opaque nature of the system fuelled confusion as to its role and led to it being blamed in the public mind for many other forms of blocking – even where those were nothing to do with it.[142]

To some extent this stemmed from the fact that the IWF had poorly communicated its role to the public. More specifically, however, it resulted from the obscure way in which the IWF URL list and individual ISP blocking systems interacted. While this lack of

[138] See e.g. Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010), chap. 9; Joe McNamee, *The Slide from 'Self-Regulation' to Corporate Censorship* (European Digital Rights, 2011), http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf.
[139] Internet Watch Foundation, 'Board Minutes 25 November 2008', 25 November 2008, http://www.iwf.org.uk/accountability/governance/board-minutes/2008-board-minutes/25-november-2008.
[140] Internet Watch Foundation, 'Board Minutes 29 September 2009', 29 September 2009, http://www.iwf.org.uk/accountability/governance/board-minutes/2009-board-minutes/29-september-2009.
[141] Internet Watch Foundation, 'IWF URL List Policy and Procedures'.
[142] Chris Williams, 'IWF Denies Wielding Pirate Bay Banhammer', *The Register*, 21 April 2009, http://www.theregister.co.uk/2009/04/21/iwf_pirate_bay/.

transparency had been flagged from an early stage, little had been done about it.[143] In particular, at the time of the Wikipedia block it was often unclear as to what ISPs were blocking against the URL list and how they were doing so. Consequently, as part of the response to the Wikipedia incident the board set out to improve transparency, despite the fact that this had previously been resisted by industry. Perhaps ironically, in so doing it also catered to both pro- and anti- blocking lobbies – the pro-blocking constituency (children's charities) having consistently called for greater publicity in order to exert consumer pressure on those ISPs which did not block.

(a) Promoting stop pages

The first way in which this was done was through promoting the use of what the IWF termed "splash pages" and are generally known elsewhere as stop pages – that is, pages which notify the user that their attempt to visit a particular page has been blocked and which explain why. From 2010 onwards the IWF has recommended (but does not require) that such pages be used – but only where an ISP is blocking at the level of full URLs, not at domain level.[144] The recommended text is as follows:

> 403: Access Denied
>
> Access has been denied by your internet access provider because this page may contain indecent images of children as identified by the Internet Watch Foundation. If you think this page has been blocked in error please contact <your service provider>.

While this may improve transparency, it nevertheless leaves open the issue that ISPs are not required to use such pages – and indeed, under the IWF rules, may not do so when blocking at domain level. Consequently, there remains a real risk that users may find themselves blocked without knowing why.

[143] Internet Watch Foundation, 'Board Minutes 11 July 2006', 11 July 2006, http://web.archive.org/web/20061111152429/http://www.iwf.org.uk/corporate/page.163.htm.
[144] Internet Watch Foundation, 'Internet Watch Foundation (IWF) Brand Guidelines'.

(b) Recipients of the URL list and self-certification

As already discussed, a long-standing concern of children's groups has been to identify those ISPs who are using (or not using) the IWF list for blocking purposes. Following the Wikipedia incident, this became all the more urgent as the IWF sought greater transparency to repair its reputation – and, as we have seen, identifying blocking ISPs also formed part of the *quid pro quo* by which mandatory blocking was averted. For that reason, in 2010 the IWF moved towards a two stage system of disclosure regarding use of the list – where members licensed to use the list would be listed on the website and in addition would be required to take part in a self-certification procedure which tested whether it was being deployed correctly.[145]

This again, however, contributes to transparency only in a very limited way. It primarily addresses the interests of children's groups and the Home Office by creating a mechanism which will test (via dummy URLs) whether the ISPs are living up to their commitment by blocking material on the URL list. It does not, however, test in any other way how the blocking systems operate – and in particular it does not identify any over-blocking or collateral damage which might be caused. It would do nothing, therefore, to guard against another Wikipedia incident.

(iv) Revised appeals process

A further IWF response to the Wikipedia episode was to introduce a revised appeals process[146] which widened the categories of person entitled to appeal so that:

[145] Internet Watch Foundation, '2010 Annual Report', 2011, 4, http://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf.
[146] Internet Watch Foundation, 'Content Assessment Appeal Process', 2010, http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process.

> Any party with a legitimate association with the content or a potential victim or the victim's representative, hosting company, publisher or internet consumer who believes they are being prevented from accessing legal content may appeal against the accuracy of an assessment.

As before, however, the ultimate appeal is to an outside police agency whose decision is final. A truly independent appeal is still lacking.

(v) Independent review of blacklist

One of the immediate responses of the IWF after the Wikipedia block was to explore the possibility of a regular review of the content of the blacklist itself, to be carried out by a senior independent figure such as a judge.[147] While this was accepted in principle by the board[148] it was not ultimately implemented – apparently due to difficulties agreeing with the CPS a procedure by which this could be done.[149] Consequently the only outside review of the blacklist appears to be a sampling process of current and historic screen captures which is carried out as part of the periodic audit process.[150]

13. Current developments: towards stop pages and proactive searches

In 2013 the Prime Minister, David Cameron, launched a broad initiative on internet safety and children[151] followed by a "cyber-summit" with the internet industry in

[147] Internet Watch Foundation, 'Board Minutes 27 January 2009'.
[148] Internet Watch Foundation, 'Board Minutes 1 December 2009', 1 December 2009, http://www.iwf.org.uk/accountability/governance/board-minutes/2009-board-minutes/1-december-2009.
[149] Internet Watch Foundation, 'Board Minutes 30 March 2010', 30 March 2010, http://www.iwf.org.uk/accountability/governance/board-minutes/2010-board-minutes/board-30-march-2010.
[150] The only audit report which is publicly available is Allan Gibson et al., 'Inspection of the Internet Watch Foundation', 30 March 2011, http://www.iwf.org.uk/assets/media/news/Inspection%20of%20the%20IWF%202011.pdf. Two prior audits have been carried out. The first by Police Commander David Armond (Metropolitan Police) and Professor David Wall in 2004 and the second by Assistant Chief Constable Stuart Hyde (West Midlands Police), Professor Peter Sommer (LSE), Professor June Thorburn (UEA) and Jim Warnock (CEOP) in 2008. These have not been made public by the IWF and the Home Office has, in response to FOI requests, denied holding copies.
[151] David Cameron, 'The Internet and Pornography' (presented at the NSPCC, London, 22 July 2013), https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action.

Downing Street in November 2013 focusing specifically on CAI.[152] While the wider initiative deals with a variety of issues tangential to this thesis – such as the use of opt-in or opt-out parental control filters by UK ISPs[153] and blocking of certain search terms by ISPs[154] – it also proposes two changes to the Cleanfeed system which should be mentioned.

The first of these aims at the greater use of warnings for those seeking to view CAI. In response to pressure from the Prime Minister Google and Microsoft have already rolled out warnings in relation to certain search terms, and an example can be seen below.[155]

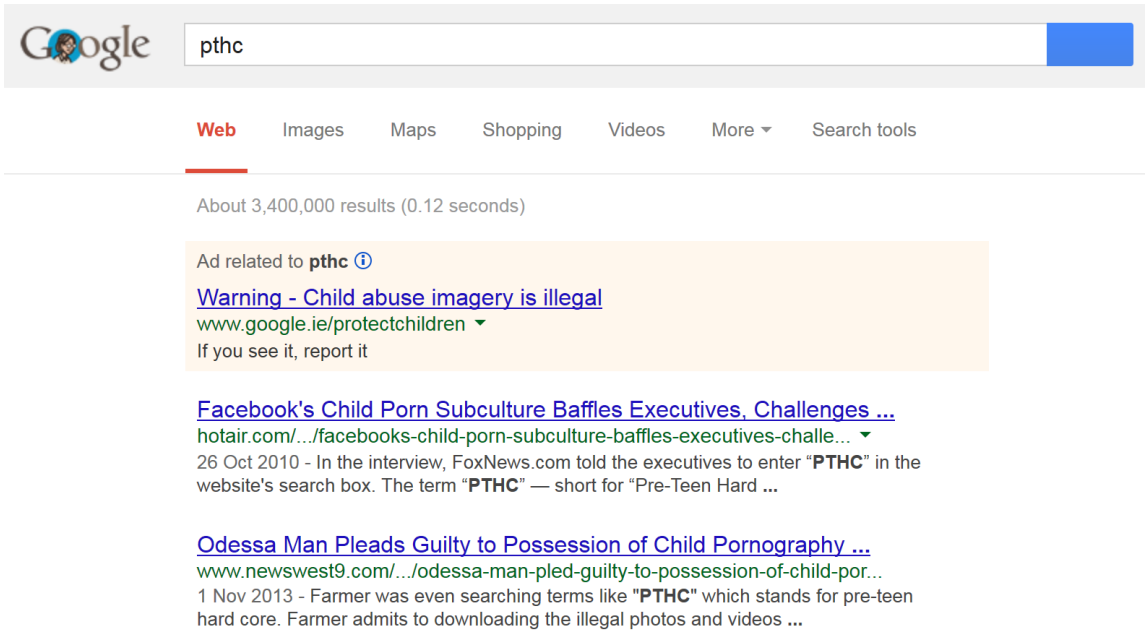

Figure 3 - Google search warning[156]

[152] Samuel Gibbs, 'UK's Top Tech Executives Meet for Summit against Online Child Abuse', *The Guardian*, 18 November 2013, http://www.theguardian.com/technology/2013/nov/18/uk-top-tech-executives-online-child-abuse.
[153] Georgia Graham, 'Embarrassed Husbands Will Have to Discuss Plans to Watch Online Porn with Their Wives, Says David Cameron', *The Telegraph*, 18 November 2013, http://www.telegraph.co.uk/technology/google/10457726/Embarrassed-husbands-will-have-to-discuss-plans-to-watch-online-porn-with-their-wives-says-David-Cameron.html.
[154] Nicholas Watt and Juliette Garside, 'Google to Tackle Images of Child Sexual Abuse with Search and Youtube Changes', *The Guardian*, 18 November 2013, http://www.theguardian.com/technology/2013/nov/18/uk-us-dark-web-online-child-abuse-internet.
[155] Ibid.

The Prime Minister has sought to match this under the Cleanfeed system by promoting the use of stop pages by ISPs, stating that:

> What we've already done is insist that clear, simple warning pages are designed and placed wherever child abuse sites have been identified and taken down so that if someone arrives at one of these sites they are clearly warned that the page contained illegal images… These warning pages should also tell people who've landed on these sites that they face consequences like losing their job, losing their family or even access to their children if they continue. And vitally they should direct them to the charity Stop it Now! which can help people change their behaviour anonymously and in complete confidence.[157]

In response, some ISPs which previously did not use stop pages (such as BT) have now introduced them.[158] However many continue to be reluctant to do so[159] and it remains to be seen whether their use will become universal and whether ISPs will start using the types of warning sought by the Prime Minister.

A second, potentially much more significant, aspect of this initiative is that the government has asked the IWF to begin proactively searching for illegal content to block.[160] According to the Culture Secretary, Maria Miller "Until now, action has only been taken by the IWF when a child sexual abuse image is reported. Now, for the first time, the IWF has been asked to work alongside Ceop to search for illegal and abusive images and block them".[161]

---

[156] Accessed 9 December 2013.
[157] Cameron, 'The Internet and Pornography'.
[158] Nicole Kobie, 'BT to Warn Users Attempting to View Child Abuse Images', *PC Pro*, 14 June 2013, http://www.pcpro.co.uk/news/security/382459/bt-to-warn-users-attempting-to-view-child-abuse-images.
[159] Internet Watch Foundation, 'Board Minutes 28 May 2013', 28 May 2013, https://www.iwf.org.uk/assets/media/accountability/board/Final%20IWF%20Board%20Meeting%20approved%20amended%20Minutes%2028May2013%20web%20version.pdf.
[160] Internet Watch Foundation, 'IWF Ready to Step up the Fight against Online Child Sexual Abuse Content', 18 June 2013, http://www.iwf.org.uk/about-iwf/news/post/360-iwf-ready-to-step-up-the-fight-against-online-child-sexual-abuse-content; LINX, 'IWF to "proactively" Search for Illegal Content', *LINX Public Affairs*, 20 June 2013, https://publicaffairs.linx.net/news/?p=9861.
[161] Nicholas Watt, Josh Halliday, and Juliette Garside, 'Web Firms Pledge £1m to Help Block Child Abuse Images', *The Guardian*, 18 June 2013, http://www.theguardian.com/technology/2013/jun/18/internet-service-providers-child-abuse-images.

This addresses an important criticism of the Cleanfeed system as it stands – that by relying on *ad hoc* reports from the public the URL list can only block access in a haphazard way. When implemented, therefore, this has the potential to significantly increase the effectiveness of the system in preventing inadvertent or casual access. There must be a question mark, however, as to the possible effect of an expanded URL List. The Wikipedia incident highlighted the collateral damage that can be caused by even advanced blocking systems. Since then there have been a number of comparable examples[162] – but overall these appear to be relatively few. It is likely that this is due in part to the fact that the URL list contains a relatively small number of URLs at any one time. Should the size of the list increase significantly then the risk of collateral damage will also increase.[163] More fundamentally, this change also marks a significant move on the part of the IWF away from simply operating an industry hotline and towards an active policing role which is likely to be more controversial. The reference to working "alongside Ceop" is significant and reflects the fact that, as in other situations, the IWF will be engaged in intelligence sharing on foot of its activities.[164]

14. Conclusion

> The Internet Watch Foundation (IWF) is a prime example of how self-regulation can produce excellent results – even in such a sensitive area as combating child sexual abuse images on the internet. By successfully cooperating with a wide range of internet players, the IWF has made a breakthrough in the United Kingdom. It simply cannot be tolerated that internet users would accidentally be exposed to such horrific images.
>
> – Neelie Kroes, 2011[165]

> IWF falls into a category of 'least worst' rather than 'perfect'.
>
> – Peter Sommer, 2008[166]

[162] See e.g. this 2011 incident with Fileserve.com: 'UK ISP Block of Fileserve Site Blamed on Internet Watch Foundation Filter', *ISP Review*, 19 November 2011, http://www.ispreview.co.uk/story/2011/11/19/uk-isp-block-of-fileserve-website-blamed-on-internet-watch-foundation-filter.html.
[163] See also the discussion in chapter 8, section 3.
[164] Internet Watch Foundation, 'Police', accessed 10 December 2013, https://www.iwf.org.uk/partnerships/police.
[165] Internet Watch Foundation, '2010 Annual Report', 2.

Notwithstanding its relatively short history, informed observers differ significantly as to the merits of the IWF and in particular the blocking systems which it facilitates. What is striking, however, is a remarkable level of consensus even amongst its critics that the IWF has served a desirable function in helping to restrain more intrusive government regulation of the internet in the UK.

There is a widely held view – even amongst those who describe themselves as suspicious of the IWF – that it provides a "pragmatic solution to reconciling two principles: as much Internet freedom as possible and preventing the distribution of material which the UK Parliament, as long ago as 1978, decided was illegal".[167] This view is echoed by many who would prefer not to see the system put on a legislative basis.[168] The majority of those interviewed for this research have said that fears of wider censorship are mitigated rather than exacerbated by the current structure of the IWF, which has been described as "the saviour of the UK internet from further regulation".[169] Industry sources have argued that governmental schemes by comparison are "massively less transparent".[170]

These comments about the IWF should not necessarily be taken as approval of the Cleanfeed system, where views have been much more mixed, and it is notable that the IWF itself has begun to de-emphasise the role of blocking in the wake of the Wikipedia incident. It is important, therefore, to separate out the two for the purposes of analysis – not least as the manner in which individual ISPs block differ significantly (whether stop pages are used, for example). When we do so, the role of filtering becomes significantly more problematic and the following two chapters will consider the operation of the

---

[166] Peter Sommer, 'Re: Cleanfeed and Wikipedia', 9 December 2008, http://markmail.org/message/pd5vhqrofd7brqxm.
[167] Peter Sommer, 'Re: Cleanfeed and Wikipedia', 8 December 2008, http://markmail.org/message/kobuqgxlorakesnx; Sommer, 'Re: Cleanfeed and Wikipedia', 9 December 2008.
[168] E.g. Cormack, Telephone interview.
[169] Truman, Telephone interview.
[170] Roland Perry, Telephone Interview, 1 March 2009.

Cleanfeed system in more detail, using a three part analytical framework (code as law, gatekeeper regulation and self-regulation) drawn from the cyber-libertarian and cyber-paternalist literature.

Chapter 4 – Cyber-libertarianism, Cyber-paternalism and Cleanfeed: Code as Law and Gatekeeper Regulation

1. Introduction

Technological changes are often disruptive of social and legal structures.[1] In the case of the internet this disruption has challenged the power of the state to enforce national laws against online content.[2] In response, states have adopted new regulatory strategies which appear to meet that challenge, but which have in turn been criticised as undermining constitutional values, in particular the protections associated with freedom of expression in other (offline) contexts.[3]

An extensive literature has developed within the field of regulatory governance which examines this interplay between technological change and state response, considering the role of technology both as a subject of regulation and as a regulatory tool in its own right.[4] The literature makes a number of predictions about the impact of technology, the types of regulatory strategies which may be adopted, their effectiveness and their impact on constitutional values. This chapter examines the operation of the Cleanfeed system in light of this literature, with a view to testing and refining these predictions. In particular, it:

- Outlines the cyber-libertarian/cyber-paternalist debate as to the extent to which the internet is resistant to control by states;

[1] See generally Mathias Klang, *Disruptive Technology: Effects of Technology Regulation on Democracy* (Göteborg University, 2006), http://www.digital-rights.net/wp-content/uploads/2007/12/klang_thesis2.pdf.
[2] Taylor and Quayle, *Child Pornography: An Internet Crime*.
[3] See e.g. Yaman Akdeniz, 'Who Watches the Watchmen? The Role of Filtering Software in Internet Content Regulation', in *The Media Freedom Internet Cookbook* (Vienna: Organisation for Security and Cooperation in Europe, 2004), http://www.osce.org/publications/rfm/2004/12/12239_89_en.pdf.
[4] See in particular Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008).

- Introduces the practical difficulties (such as anonymity/pseudonymity, jurisdictional arbitrage and technological challenges) associated with tackling child pornography and other forms of content online;
- Describes the regulatory strategies suggested by cyber-paternalists (in particular intermediary or gatekeeper regulation, and regulation by code or architecture) and assesses how these have been used in Cleanfeed;
- Describes the concerns expressed about such strategies (such as fears of overblocking) and considers to what extent those concerns have been borne out in the UK context; and
- Examines claims that effective regulation of the internet requires that these regulatory strategies be used, by considering the extent to which these strategies (as embodied in Cleanfeed) have proved effective at tackling the distribution of child pornography online.

2. The cyber-libertarian vision

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather…
>
> I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear...
>
> – John Perry Barlow, 1996 [5]

An early view of the internet was that it was a place beyond the control of states. As Barlow's famous Declaration of Independence of Cyberspace shows, this view combined both normative and descriptive elements. The normative claim was founded on the argument that state regulation was illegitimate – that the internet created a new "cyberspace" which was not the property of any one jurisdiction and was instead a realm of the mind. The descriptive aspect, on the other hand, was based on the belief that

[5] John Perry Barlow, 'A Declaration of the Independence of Cyberspace', 8 February 1996, http://homes.eff.org/~barlow/Declaration-Final.html.

technological features of the internet meant that governments had no "methods of enforcement" that users had "reason to fear". Instead, so the vision went, new structures of governance would emerge from the internet itself, as online communities would develop their own systems of self-regulation.[6] This view came to be dubbed "cyber-libertarianism", reflecting its obvious appeal for an internet community which was seen as libertarian in its views generally.[7]

Events since then have to a large extent undermined that early vision, and even "virtual selves" have proved to be subject to the control of the state – not always, admittedly, but sufficiently often that the Declaration of Independence of Cyberspace is now commonly the subject of mockery.[8] To understand why, however, we must first understand the claims which the cyber-libertarians made in order to see how their points – so convincing to many at the time – were later circumvented.

(i) Legitimacy of regulation

At the core of the cyber-libertarian argument was the bold claim that state regulation of the internet was *illegitimate* – not merely impractical, undesirable or unwise. This was an audacious proposition even at the height of cyber-utopianism, challenging as it did the powers of democratically elected governments. When examined more closely, it can be seen to have three components: one which focuses on issues of jurisdiction and applicable law, one which privileges self-governance by "netizens"[9] over state action, and one which deems cyberspace to be a place of thought and speech rather than action. Each will be considered in turn.

---

[6] See in particular Johnson and Post, 'Law and Borders - The Rise of Law in Cyberspace'.
[7] Boyle, for example, spoke of the 'libertarian culture that dominates the Net at present' - Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors'.
[8] See e.g. Aimée Hope Morrison, 'An Impossible Future: John Perry Barlow's "Declaration of the Independence of Cyberspace"', *New Media & Society* 11, no. 1–2 (2009): 53.
[9] A term which itself challenged the traditional notion of citizen.

(a) Jurisdiction and applicable law

One of Barlow's claims was that cyberspace "is a world that is both everywhere and nowhere, but it is not where bodies live".[10] In this, he echoed the views of lawyers who concluded that the cross-border nature of internet activities meant that no one sovereign could have any claim to legitimately regulate the online world, and that even "local" regulation would have an improper spillover effect into other jurisdictions – for example, by requiring US firms to censor material from their US users on the basis that it might be illegal in some other jurisdiction such as Germany.

The most famous exemplars of this view were Johnson and Post who in their seminal 1996 article "Law and Borders – the Rise of Law in Cyberspace" argued that territorial claims to jurisdiction were self-defeating. Dealing with the argument that states may properly regulate online activity which has effects within their borders, Johnson and Post argued that this claim, brought to its logical conclusion, would mean that online activities would simultaneously be subject to the laws of all states. Instead, therefore, Johnson and Post argued for a vision of cyberspace as a new and distinct place, sitting outside national boundaries, to which new and distinct rules should apply. Any other solution would invariably result in improper spillover effects, in which the law of one state would affect those located elsewhere.[11]

(b) Self-governance as a substitute for state control

Even if we accept the premise of cyberspace as a new and distinct place it still raises a further question – who should make its new and distinct rules? If no one state can assert a right to legislate for the internet then why isn't the appropriate response for states to work together to make new law at a multi-lateral level? The response of the cyber-libertarians was to argue that self-regulatory structures would grow up within

[10] Barlow, 'A Declaration of the Independence of Cyberspace'.
[11] Johnson and Post, 'Law and Borders - The Rise of Law in Cyberspace', 1374.

cyberspace, formulated by the "people who cared most about and best understood their new creation" with the implication that such structures would enjoy greater legitimacy amongst internet users.[12] Johnson and Post set out their fundamental principle as being that:

> If the sysops and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government.[13]

This view relied on the argument that the internet permitted individuals to choose freely between different sets of rules within cyberspace, and portrayed this active consent of the netizen to online structures as preferable to the "fictional" consent of the citizen to the power of the state.[14]

(c) "Cyberspace, the new home of mind"

The third strand of the cyber-libertarian challenge to legitimacy of state regulation was to portray the internet as a realm of thought and speech alone and thus presumptively beyond the realm of state control. As Boyle commented:

> The libertarian culture that dominates the Net at present posits that state intervention into private action is only necessary to prevent "harms." Seeing the Net as a "speech-dominated" realm of human activity in which harm would be comparatively hard to inflict, libertarians have been even more resistant to state regulation of the digital environment than of, the disdainfully named, "meatspace." "Sticks and stones can break my bones but bytes can never hurt me," or so goes their assumption.[15]

This argument drew heavily on US law – by classifying internet use as "speech" rather than "action" the cyber-libertarians sought to bring it within the strong protections of the

[12] Ibid., 1390.
[13] Ibid., 1398–9.
[14] Ibid., 1398.
[15] Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors', 179–180.

First Amendment. Ironically, therefore, the idea of a distinct online realm relied in large part on one national legal doctrine.[16]

(ii) Practicability of regulation

Quite distinct from these claims about the legitimacy of regulation were claims about the practicability of regulation. Here, the cyber-libertarians argued that the nature of the internet would preclude government control – short of the draconian step of disconnecting a state from the internet entirely. This represented a variety of strong technological determinism[17] in its belief that technology would irresistibly shape social practices, and the following passage from Johnson and Post was typical of this view:

> [E]fforts to control the flow of electronic information across physical borders – to map local regulation and physical boundaries onto Cyberspace – are likely to prove futile, at least in countries that hope to participate in global commerce. Individual electrons can easily, and without any realistic prospect of detection, "enter" any sovereign's territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities.[18]

When examined closely, this claim can be seen to have a number of different components, which will be examined separately.

(a) Jurisdictional arbitrage

A central part of the cyber-libertarian case was that states could not, in the words of Johnson and Post, "map local regulation and physical boundaries onto Cyberspace". This seamless nature of the internet appeared to open the door to jurisdictional arbitrage,

---

[16] Jack L Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006), 19.
[17] For criticism of strong technological determinism in the context of the internet see e.g. Ralf Bendrath and Milton Mueller, 'The End of the Net as We Know It? Deep Packet Inspection and Internet Governance', *New Media & Society* 13 (27 April 2011).
[18] Johnson and Post, 'Law and Borders - The Rise of Law in Cyberspace', 1372.

so that users could, in effect, choose which law applied to their internet use.[19] Local laws against pornography, for example, would be ineffective if users could access sites based in jurisdictions such as the United States where the law was more permissive. According to cyber-libertarians, therefore, governments would be faced with a dilemma – either cut off access to the internet entirely (with resulting economic harm) or face the impossible task of applying local laws to the worldwide internet.

(b) Disintermediation

Unlike traditional newspapers, radio or television, the internet did not require communications to be filtered via an editor, allowing for a wider range of views to be aired and limiting the traditional points at which states could exercise formal or informal control.[20] Unlike the broadcast spectrum, bandwidth was not lacking, undermining traditional rationales for the regulation of broadcasting. It became viable to deliver content worldwide for even the most niche interest – it was no longer necessary to aggregate a critical mass of readers or viewers to make distribution economically feasible. Suddenly the tools of broadcasting and mass publication became available to almost anyone, and as a result Barlow and others saw the internet as creating "a new social space, global and anti-sovereign, within which anybody, anywhere can express to the rest of humanity whatever he or she believes without fear".[21]

(c) Anonymity, privacy and the crypto-anarchist vision

The cyber-libertarian argument also relied on the existence of a network structure which was perceived to promote anonymity – or at least pseudonymity.[22] As a result, so the

[19] John Perry Barlow, 'Thinking Locally, Acting Globally', *Time*, 15 January 1996, http://www.time.com/time/magazine/article/0,9171,983964,00.html.
[20] Robert Gellman, 'Disintermediation and the Internet', *Government Information Quarterly* 13, no. 1 (1996): 1.
[21] Barlow, 'Thinking Locally, Acting Globally'.
[22] Gia Lee, 'Addressing Anonymous Messages in Cyberspace', *Journal of Computer-Mediated Communication* 2, no. 1 (1996), http://www.ascusc.org/jcmc/vol2/issue1/anon.html.

argument went, governments would find it difficult or impossible to trace the users behind any given communication, putting them effectively beyond control. In Lessig's words: "[t]he invisible man doesn't fear the state... If you can't know who someone is, or where he is, or what he's doing, you can't regulate him".[23]

When coupled with the widespread availability of strong encryption, this appeared to some to create the conditions for "crypto-anarchy" – an online world in which public key cryptography enabled communications which could not be monitored by states, along with digital cash which would be anonymous and untraceable. According to its advocates, therefore:

> The combination of strong, unbreakable public key encryption and virtual network communities in cyberspace will produce interesting and profound changes in the nature of economic and social systems. Crypto anarchy is the cyberspatial realisation of anarcho capitalism, transcending national boundaries and freeing individuals to make the economic arrangements they wish to make consensually.[24]

(d) Volume of communications and rate of change

> The complexity of Third Wave society is too great for any centrally planned bureaucracy to manage. Demassification, customization, individuality, freedom – these are the keys to success for Third Wave civilization.
>
> – Esther Dyson, George Gilder, George Keyworth and Alvin Toffler, 1994[25]

In addition to other restraints on states, Johnson and Post argued that monitoring of communications was impractical where "[t]he volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities".[26] A similar point was often made (and continues to be made in respect of filesharing) in respect of controls aimed at individual users and websites, where it was argued that the numbers involved would undermine traditional legal

[23] Lawrence Lessig, *Code: Version 2.0*, 2nd ed (New York: BasicBooks, 2006), 38.
[24] Timothy C. May, 'Crypto Anarchy and Virtual Communities', *Internet Security*, April 1995, 4–12.
[25] Esther Dyson et al., 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2)', *Future Insight*, August 1994, http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html.
[26] Johnson and Post, 'Law and Borders - The Rise of Law in Cyberspace', 1372.

controls which were resource intensive and depended on targeting a relatively small number of actors.[27] On a related point, it was also sometimes argued that the speed of technological change would also present problems for states – so that legislation could not keep pace with developments on the internet, stymieing attempts to pursue online activity through traditional legal tactics.[28]

Events in the UK have, to a large extent, proved the truth of these points. Where perpetrators can be identified, in some cases their numbers have challenged police resources. In the 2002 case of Operation Ore, for example, Jewkes and Andrews note that 7,200 UK users were suspected of buying child pornography, of whom only 1,200 were arrested. Even this selective response however was described by police as "crippling" their capabilities, taking up all available resources in a way which jeopardised their ability to respond to other forms of cybercrime.[29]

3. The cyber-paternalist response

From approximately 1996 onwards the cyber-libertarian vision was met with a number of objections by a group of theorists dubbed cyber-paternalists, who challenged the normative and descriptive claims on which it was based, arguing that the internet both *could* and *should* be regulated.[30]

[27] Swire, 'Of Elephants, Mice, and Privacy'.
[28] See e.g. Bert-Jaap Koops et al., 'Should Self-Regulation Be the Starting Point?', in *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, ed. Bert-Jaap Koops et al. (The Hague: T.M.C. Asser Press, 2006).
[29] Yvonne Jewkes and Carol Andrews, 'Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales', *Policing & Society* 15, no. 1 (March 2005): 48–49.
[30] Andrew Murray, 'The Regulatory Edge of the Internet', *International Journal of Information Technology* 11, no. 1 (2003): 87.

(i) Legitimacy

(a) Jurisdiction and applicable law

On the normative side, the cyber-paternalist view began by rejecting as overblown claims that the internet should be treated as a new world for the purposes of private international law, describing it instead as being "functionally identical to transnational activity mediated by other means, such as mail or telephone or smoke signal".[31] Critics such as Goldsmith noted that spillover effects and multiple concurrent jurisdictions were nothing new in private international law, and suggested that existing choice of law rules were capable of resolving the majority of conflicts which would arise.[32]

(b) Against self-governance

The cyber-paternalist response also attacked the core of the cyber-libertarian argument that self-regulation was inherently more desirable in an online environment than rules imposed by states. This attack took various forms, but one of the most important was the claim that the "bottom up" governance involved in self-regulation would result in the systematic erosion of important public and democratic values. Lessig identified this as "policy-making by the invisible hand" and argued that profit motives and other factors would ensure that "the invisible hand, through commerce [constructs] an architecture that perfects control" and thereby restricts liberty.[33] In a striking analogy, he compared the internet with post-Communist Russia and argued that in each case the decline of the state did not automatically result in freedom, but instead laid the foundations for a

[31] Jack Goldsmith, 'Against Cyberanarchy', in *Who Rules the Net*, ed. Adam D. Thierer and Clyde Wayne Crews (Washington, D.C.: Cato Institute, 2003), 62.
[32] Goldsmith, 'Against Cyberanarchy'.
[33] Lawrence Lessig, 'The Spam Wars', *The Industry Standard*, 31 December 1998, http://www.lessig.org/content/standard/0,1902,3006,00.html; Lessig, *Code*, 5–6.

transfer to the private sector which resulted in merely replacing one system of power and corruption with another.[34]

In a similar vein, Reidenberg expressed concern that the cyber-libertarian vision was fundamentally anti-democratic. Rather than promoting democracy, he argued, the effect of embedding policy rules in the technical infrastructure of the internet was to give a small technocratic elite the power to set at naught the legitimate decisions of democratic governments. In his view, therefore, there was a democratic imperative to ensure that states could exert effective control over information available in their territories, and he rejected attempts by US firms to export First Amendment values as showing little respect for the balances which other democracies set in relation to fundamental rights and hate speech.[35]

(c) Limits of the "Realm of Mind"

The cyber-libertarian viewpoint was also dismissed by many who did not share their starting point of cyberspace as a "realm of the mind" which should presumptively be beyond state regulation. Two distinct aspects to this response can be identified. The first is exemplified by Reidenberg who pointed out that this view itself privileged one jurisdiction – that the "American belief in information freedom" did not "reflect more subtle policies of information freedoms found in other democracies and in international human rights law".[36]

Perhaps more importantly, however, the idea of cyberspace as a separate realm of speech and thought was questioned – even by those otherwise sympathetic to the cyber-libertarian cause – as neglecting the real world effects which communications have on third parties. For example, Hardy, though supporting decentralisation and self-regulation

[34] Lessig, *Code: Version 2.0*, 1–3.
[35] Joel R. Reidenberg, 'Yahoo and Democracy on the Internet', *Jurimetrics* 42 (2002): 261.
[36] Ibid., 273.

online where possible, argued that contractual governance in cyberspace was inapt where the primary effect of a wrong such as libel was harm to a third party.[37]

This point becomes even stronger in the context of child pornography, where recent work has developed the argument that the distribution of images of abuse online constitutes a form of re-victimisation, particularly where the victim of abuse has to live with the knowledge that their image is perpetually available and may even be seen by someone they know.[38] In this context, the early idea that cyberspace is merely a "realm of the mind" becomes much more difficult to sustain.

(ii) Practicability of regulation

Turning away from the cyber-paternalist claims about the *legitimacy* of state regulation of the internet we come to the *practicability* of regulation. Here, the cyber-paternalists warned against a naive faith in the ability of technology to undermine government power, arguing instead that the growth of the internet created an opportunity for governments to consolidate and perfect their power in a way which went beyond anything possible offline and which might systematically undermine existing civil liberties. If these tendencies were to be checked, they argued, the cyber-libertarians would have to descend from their "realm of the mind" and fight battles in the traditional political world.

(a) Online activities escaping the reach of offline laws

> For five hundred years a struggle was fought, and in a few countries won, for the right of people to speak and print freely, unlicensed, uncensored, and uncontrolled. But new technologies of electronic communication may now relegate old and freed media such as pamphlets, platforms and periodicals to a corner of the public forum. Electronic modes of communication that enjoy lesser rights are moving to center stage. The new communications technologies have not

[37] I. Trotter Hardy, 'The Proper Legal Regime for Cyberspace', *University of Pittsburgh Law Review* 55 (1993): 993.
[38] Taylor and Quayle, *Child Pornography: An Internet Crime*, 31; O'Donnell and Milner, *Child Pornography: Crime, Computers and Society*, 70–71.

> inherited all the legal immunities that were won for the old... And so, as speech increasingly flows over those electronic media, the five-century growth of an unabridged right of citizens to speak without controls may be endangered.
>
> – Ithiel de Sola Pool, 1983[39]

One of the cyber-libertarian claims was that existing (offline) legislation would soon find itself outdated, as government could not move fast enough to legislate for new (online) situations. While there was undoubtedly some truth in this point, the result was not necessarily to their advantage. As de Sola Pool had presciently observed a decade earlier, new communications technologies were frequently more rather than less vulnerable to state control. In particular, many legislative protections for freedom of expression and privacy had been established with traditional means of communication in mind and did not necessarily carry over to the online world.

As a result, the cyber-libertarian vision neglected the fact that technological change could permit governments to take measures online which would be denied to them in the offline world. Without legislative updates, postal packets might enjoy greater legal protection than IP packets.

To some this might have seemed a minor objection. After all, the cyber-libertarian position (at least in its strongest form) was based on a belief that governments *could not* control the online world, irrespective of the legal powers they enjoyed. It did, however, mean that the cyber-libertarian position was extremely brittle – once a government acquired a particular technical capability, failure to update legislation meant that there might not be a fallback position in the form of a legal control on the use of that capability.

[39] *Technologies of Freedom* (Cambridge, Mass: Belknap Press of Harvard University Press, 1983), 1.

(b) Techno-utopianism as a distraction from political action

This brittleness was compounded by a refusal on the part of some cyber-libertarians to engage with the political process. For many critics cyber-libertarianism was positively harmful to the extent that it encouraged technologists to passively rely on their belief in technological determinism instead of actively lobbying for the protections they sought. Morrison eloquently expresses this view when she argues that:

> Barlow's piece and others like it promoted self-congratulatory and heroic poses that allowed the adherents of the *Wired* philosophy to see themselves as intrinsic revolutionaries. It is easy enough to see the appeal of such a position; it is far less taxing to don a pair of cyberpunk sunglasses and gesticulate insultingly to The Powers That Be than it is to put on a suit, prepare to compromise and lobby for a position at the legislative table… [I]t distracted passionate, fundamentally decent people from taking meaningful and substantive action by proposing lifestyle libertarianism as a viable political strategy.[40]

Lessig has expanded on this point further, arguing that a reliance on "technological short-cuts" is undesirable as undermining democratic participation:

> Of course, my view is that citizens of any democracy should have the freedom to choose what speech they consume. But I would prefer they earn that freedom by demanding it through democratic means than that a technological trick give it to them for free.[41]

One does not have to agree with his apparent feeling that a freedom which is *earned* is more virtuous than one which is *given* to see the strength of the underlying point that the cyber-libertarian view, taken to its logical conclusion, may lead to an unhealthy detachment from (or even disdain for) the democratic process.

(c) Remaking the architecture of the internet

Probably the single most important contribution of the cyber-paternalists was their recognition that the technology which made the internet resistant to state control was

[40] Morrison, 'An Impossible Future', 67.
[41] Lessig, *Code: Version 2.0*, 309.

malleable – that the architecture of the internet could be remade in a way which would facilitate censorship and surveillance.[42]

When examined closely, the cyber-libertarian argument relied on a form of strong technological determinism and implicitly assumed that technology would inevitably remake society via a one way causal chain. In that assumption, however, it overlooked the point that the causal relationship is not solely one way – that society could also shape technology. In particular, it neglected a well established body of scholarship which emphasised technology as a social product, which is itself the result of specific political and ideological forces.[43]

Seen against this background, claims based on a particular technical architecture of the internet became much more problematic. While the cyber-libertarian school accepted that the internet was not static, they did hold the belief that the general trends embedded in it were inevitable and irreversible. As Dyson *et al.* put it in their grandly titled "Magna Carta for the Internet Age":

> Living on the edge of the Third Wave, we are witnessing a battle not so much over the nature of the future – for the Third Wave will arrive – but over the nature of the transition.[44]

Against this, however, theorists such as Lessig pointed out that the aspects of the internet which resisted state control were not set in stone –they were the result of choices as to the design of the underlying technology and those choices could be reversed and the design changed. For example, governments could mandate the introduction of data retention rules, requiring ISPs to track user behaviour – or could require user authentication to be built into online transactions. Once this was understood, the cyber-libertarian claims took on a much more contingent nature.[45]

---

[42] See in particular Lessig, *Code*.
[43] Langdon Winner, 'Cyberlibertarian Myths and the Prospects for Community', *ACM SIGCAS Computers and Society* 27, no. 3 (1997): 14–19.
[44] Dyson et al., 'Cyberspace and the American Dream'.
[45] Lessig, *Code: Version 2.0*, chap. 5.

(d) Three strategies: Code as law, gatekeeper regulation and self -regulation

Building on this insight, the cyber-paternalists argued that a number of regulatory strategies could be adopted which would permit states to reassert their authority over the internet. In particular, they identified three strategies which intersect in the Cleanfeed system. The first of these – the use of code as law – promised more efficient and automated enforcement of legal rules.[46] The second – gatekeeper regulation – appeared to provide a reduced workload for governments by enabling them to target a relatively small number of actors.[47] Finally the third – promoting self-regulation – seemed to permit regulation which was more responsive and could avoid legal constraints which would otherwise apply to direct state action.[48]

The first two strategies will be considered in the following sections which discuss the use of code as law and gatekeeper regulation, outline the criticisms of each, and assess to what extent those criticisms have been borne out in the context of Cleanfeed, while the issues associated with self-regulation will be dealt with in chapters 5 and 6.

4. Code as law

(i) Introduction and advantages

> The issue here is how the architecture of the Net—or its "code"—itself becomes a regulator. In this context, the rule applied to an individual does not find its force from the threat of consequences enforced by the law... Instead, the rule is applied to an individual through a kind of physics. A locked door is not a command "do not enter" backed up with the threat of punishment by the state. A locked door is a physical constraint on the liberty of someone to enter some space.
>
> – Lawrence Lessig, 2006[49]

[46] Lessig, *Code*.
[47] Zittrain, 'Internet Points of Control'.
[48] Rik Lambers, 'Code and Speech: Speech Control Through Network Architecture', in *Coding Regulation: Essays on the Normative Role of Information Technology*, ed. Egbert Dommering and Lodewijk Asscher, Information Technology & Law 12 (The Hague: T.M.C. Asser Press, 2006).
[49] Lessig, *Code: Version 2.0*, 82.

Following on from the insight that network architecture could be remade, a number of theorists (led in particular by Lessig[50], Boyle[51] and Reidenberg[52]) developed this point further by arguing that the architecture could be remade in a way which didn't merely *facilitate* state enforcement but itself *effected* that enforcement. That is, the software or "code" underlying the network can function as a type of self-executing law, one which makes targeted behaviour either difficult or impossible, and thus minimises or entirely does away with the need for traditional legal enforcement mechanisms such as police and courts. By analogy with the offline world one might consider the speed camera versus the speed bump: both devices aimed at changing driver behaviour, but the latter having the advantage of being self-enforcing, physically preventing drivers from speeding without the need for follow up police or judicial action.[53]

This analysis drew on an existing literature from within criminology on situational crime prevention[54] and, insofar as it promised more effective enforcement of the law, had an obvious appeal.[55] Reidenberg, for example, went so far as to say that states had an *obligation* to use this type of regulation (which he described as *lex informatica*) where necessary to achieve an important public policy goal.[56] Similarly, in the context of CAI Taylor and Quayle argued that the use of technical controls could balance what they

[50] Lessig, *Code*.
[51] Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors'.
[52] Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review* 76, no. 3 (1998): 553.
[53] Lessig, *Code: Version 2.0*, 128.
[54] On which see e.g. Andrew von Hirsch, David Garland, and Alison Wakefield, eds., *Ethical and Social Perspectives on Situational Crime Prevention*, Studies in Penal Theory and Penal Ethics (Oxford: Hart Publishing, 2000).
[55] On its proposed use for child abuse images see in particular Max Taylor and Ethel Quayle, 'The Internet and Abuse Images of Children: Search, Precriminal Situations and Opportunity', in *Situational Prevention of Child Sexual Abuse*, ed. Richard Wortley and Stephen Smallbone, vol. 19, Crime Prevention Studies (Monsey, N.Y.: Criminal Justice Press, 2006); Richard Wortley, 'Situational Prevention of Child Sexual Abuse in the New Technologies' (presented at the G8 Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children, Chapel Hill, North Carolina, 2009).
[56] Reidenberg, 'States and Internet Enforcement'.

described as the extraordinary ease of committing the crime of viewing or downloading images.[57]

In addition, code as law also appeared to address a number of cyber-libertarian claims about legitimacy and legislative overspill – by using tools such as geolocation and filtering, states could ensure that regulation mapped more closely onto geographic boundaries.[58] More generally, it might also be argued (as with situational crime prevention generally) that regulation by code is a more humane form of regulation compared with traditional law enforcement – that insofar as it prevents crime it spares the prospective offender from the stigma and punishment that would be associated with a criminal conviction.

Others, however, were warier, and (led by Lessig) have identified risks with this type of regulation: many of which have manifested themselves in the context of Cleanfeed.

(ii) Indirection and opacity

> [A]fter 1948 local communities shifted their techniques for preserving segregation. Rather than covenants, they used architecture... No longer able to effect segregation directly, they used zoning laws – geographical architecture, or real space code – to effect it indirectly... Here the government is regulating indirectly... [and] gets an effect at no political cost. It gets the benefits of what would clearly be an illegal and controversial regulation without even having to admit any regulation exists.
>
> – Lawrence Lessig, 2006[59]

A key criticism of code as law is that it permits governments to regulate indirectly, bypassing the legal constraints or political costs which would otherwise apply to their actions. In Lessig's example, by controlling the built environment governments could attempt to preserve racial segregation in a way which would otherwise be denied to them

[57] Taylor and Quayle, 'The Internet and Abuse Images of Children: Search, Precriminal Situations and Opportunity'; Max Taylor and Ethel Quayle, 'Criminogenic Qualities of the Internet in the Collection and Distribution of Abuse Images of Children', *Irish Journal of Psychology* 29, no. 1–2 (2008): 119.
[58] See e.g. Dan Jerker B Svantesson, 'How Does the Accuracy of Geo-Location Technologies Affect the Law', *Masaryk University Journal of Law & Technology* 2 (2008): 11.
[59] Lessig, *Code: Version 2.0*, 135.

by law, and which would provoke public anger if known. Similarly, in the online environment Lessig saw a risk that governments could seek to build in controls into the network in such a way that users would experience these restrictions as inherent in the technology rather than as the result of deliberate choices.[60]

Closely related to the notion of indirection is a further concern – that code as law is inherently more opaque than other modalities of regulation.[61] The contrast here is especially striking when we consider attempts to control speech. Traditional forms of censorship have generally involved at least some elements of transparency. In some cases this takes the form of a public index of banned books (such as the infamous *Index Librorum Prohibitorum*[62]); in others, legislation of general application enforced with public trials or forfeiture hearings. In each case, however, the fact that a work was prohibited was not itself a secret, nor was the source of the power which brought about that result, and the operation of the censorship mechanism could be expected to result in some publicity.[63]

In the case of regulation by code, however, it becomes possible to control content in a way which bypasses these mechanisms of transparency. Users can, for example, be presented with a deceptive error page which conceals from them the fact that access to a particular website has been blocked. Even when users are aware that a block is in place, they may often be unaware as to which part of the network chain is responsible for the blocking: a library user, for example, might not know whether to blame the library itself, the ISP providing connectivity to that library, or some entity further upstream again. As a result, accountability becomes difficult where the user is unable to determine who is responsible. This is especially true if (as is increasingly common) multiple internet filters are in use concurrently.

---

[60] Ibid., chap. 12.
[61] Ibid.
[62] Francis J. Connell, 'Censorship and the Prohibition of Books in Catholic Church Law', *Columbia Law Review* 54 (1954): 699.
[63] For a general survey of censorship in the UK see e.g. Donald Thomas, *Freedom's Frontier: Censorship in Modern Britain* (London: John Murray, 2007).

To what extent are these criticisms borne out in the case of Cleanfeed? To answer this question it must be remembered that Cleanfeed is a system rather than a single entity – as a result there may be differing levels of transparency in respect of different parts of the system.

In relation to the IWF itself, it is fair to say that it is generally transparent in its operations. Board minutes and operating policies are all available on its website. In relation to the Child Abuse Image Content (CAIC) URL list the IWF is open as to the criteria which must be met in order for a URL to be added to that list and the manner in which it is periodically reviewed, and from time to time reports on the number of URLs on that list.[64] More recently, the IWF has also begun to publish a list of companies which receive the list and have voluntarily committed to filtering[65] and has taken steps to promote transparency elsewhere in the system by encouraging those companies to use splash pages where material is blocked.[66] The main exception to this general rule of transparency is in relation to the URL list itself, which is understandably kept confidential.[67]

Turning away from the IWF itself, however, there has been little transparency in the other parts of the Cleanfeed system. The individual ISPs which receive the URL list and block access using that list have been very poor at notifying users of the fact that they are doing so. This can be seen most clearly when we consider the use of block pages which indicate to users that a particular page has been blocked to them. In this regard, the Wikipedia "Virgin Killer" incident acted as a natural experiment which provides us with a valuable source of data, in the form of the Wikipedia administrators' page which

[64] Internet Watch Foundation, 'Child Sexual Abuse Content URL List'; Internet Watch Foundation, 'Blocking of Child Sexual Abuse Websites', 18 June 2009, http://www.iwf.org.uk/public/page.148.htm; Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative', *Internet Watch Foundation,* 4 January 2010, http://www.iwf.org.uk/public/page.148.437.htm; Internet Watch Foundation, 'IWF URL List Policy and Procedures'.
[65] Internet Watch Foundation, 'IWF URL List Recipients'.
[66] Internet Watch Foundation, 'Internet Watch Foundation (IWF) Brand Guidelines'.
[67] Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative'.

recorded how UK users were affected by the blocking.[68] That page gives us a snapshot of how UK ISPs implemented blocking in 2008, summarised below:

ISP	Error type	Users informed of block?	IWF role identified?
3 UK	"Site blocked"	✓	x
Be Unlimited	404 error	x	x
BT	404 error	x	x
Demon Internet	Stop page	✓	✓
Eclipse Internet	404 error	x	x
PlusNet	TCP RST	x	x
TalkTalk	404 error	x	x
Telefónica 02 UK	404 error	x	x
Tesco.net	Unknown	x	x
UK Online	404 error	x	x
Virgin Media / NTL	TCP RST / 502	x	x
Vodafone	Block page	✓	✓
Sky	404 error	x	x
T-mobile	Redirect to IWF site	✓	✓

Figure 4 - ISP implementation of Wikipedia blocking

From this, we can see that of 15 ISPs only four notified users that their access was being deliberately blocked, with the remaining 11 presenting users with deliberately deceptive results intended to create the impression of access being prevented by technical errors. In turn, of the four who notified users of the existence of blocking only three explained that the IWF was behind the decision to block. Indeed, these figures substantially understate the position – three of the four providers who indicated that a block was in place were mobile broadband providers and the only fixed line ISP (Demon) had a relatively small market share. Consequently, at the time of the Wikipedia block the overwhelming majority of UK internet users were being presented with error messages which deliberately concealed the blocking system being used, leaving them ignorant as to why material was blocked, by whom and what they could do about it if they believed it to be wrongfully blocked.

[68] 'Administrators' noticeboard/2008 IWF Action'.

At the outset, this approach was justified by BT on the basis that any other approach would enable the blacklist to be reverse-engineered.[69] This justification appears to fall down, however, when we consider that some ISPs do serve indications that pages have been blocked and indeed in other jurisdictions the use of block pages is well established. Other concerns have been cited as justifying a failure to display a block page – for example industry representatives have cited a fear that the technical implementation of a block page might be defamatory if a site was wrongfully blocked, might serve to worry customers, might identify the wrong ISP (where an ISP was reselling connectivity) or indeed might generate log files which could subsequently be accessed by police as an intelligence tool.[70] Nevertheless it is striking to note that in 2009 Cleanfeed had not even matched the level of transparency in the Saudi Arabia national filtering system which had since 2002 presented users with a page explaining any block and a form to seek unblocking.[71]

[69] Truman, Telephone interview.
[70] Andrew McCormack, Telephone Interview, 30 July 2009.
[71] Nart Villeneuve, 'The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace', *First Monday* 11, no. 1 (2006), http://firstmonday.org/ojs/index.php/fm/article/view/1307/1227.

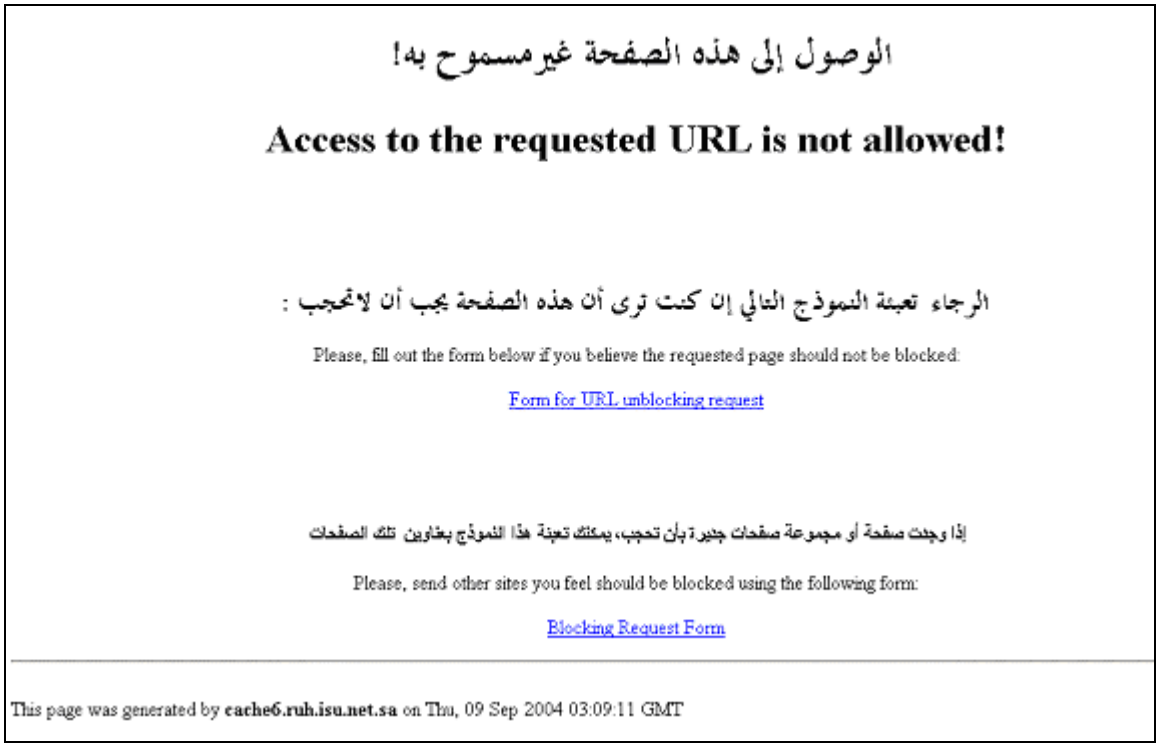

Figure 5 - Saudi Arabia block page, http://cache6.ruh.isu.net.sa[72]

Finally, it must also be remembered that there is a substantial state involvement in the adoption of the Cleanfeed system which must also be assessed for transparency. Although this is considered further in Chapter 5, it should be noted at this stage that the key department – the Home Office – has been shy in addressing questions regarding its relationship with the IWF: for example, in the wake of the Wikipedia incident declining to give an interview on the Cleanfeed system while also refusing numerous Freedom of Information requests on the basis that it had no "formal" relationship with the IWF.[73]

(iii) Overblocking

Another complaint often levelled against regulation by code is that it is prone to false positives. In the case of filtering, this manifests itself as overblocking – that is,

[72] Image taken from OpenNet Initiative, 'Internet Filtering in Saudi Arabia in 2004', *Berkman Center for Internet and Society*, 2004, https://opennet.net/studies/saudi.
[73] See Chapter 5, section 4(iv).

preventing users from accessing material which falls outside the legitimate remit of a particular system.[74] This is not an inevitable feature of filtering – as hash value based blocking systems have shown, it is possible to have a filtering system which is sufficiently precise that it will only block the transmission of a file which is identical in every regard to the file intended to be blocked.[75] Such systems are, however, computationally demanding and have yet to be deployed in respect of web browsing. Instead, the majority of web blocking systems follow the approach of blocking access to particular addresses, based on a finding that prohibited files are to be found there.[76]

This approach risks two main types of overblocking. The first relates to the specificity of the address which is blocked. Just as a postcode is less precise than the address of a particular house, so too a system which blocks at the level of the domain name (preventing access to everything hosted at example.com) will be less precise than one which blocks at the level of the full URL (blocking access to http://example.com/users/johndoe/lolita.jpg, while still permitting access to legitimate material elsewhere on that site). In this case, the principle of proportionality would generally not be met. The second form of overblocking relates to timing, and depends on how often the list of blocked material is updated – in this situation there is a risk that a website which previously contained child pornography will continue to be blocked even after the offending material has been removed.

Both types of overblocking have proved to be very common in the implementation of child pornography blocking systems elsewhere. In one well-known early example, *Centre for Democracy and Technology v. Pappert*[77], US ISPs required to cut off access to approximately 400 child pornography sites ultimately blocked approximately 1.2

[74] See e.g. Lambers, 'Code and Speech'.
[75] For an example of such a system operated by AOL see Don Colcolough, 'Investigating and Prosecuting Computer Facilitated Crimes Against Children: An AOL Perspective', 28 May 2009, http://www.childrensmn.org/web/mrcac/handouts/184933.pdf.
[76] Callanan et al., *Internet Blocking*, chap. 5.
[77] 337 F. Supp. 2d 606 (E.D. Pa. 2004).

million websites in the course of complying.[78] Similarly, the EU funded CIRCAMP blocking systems have deliberately chosen to use domain name blocking notwithstanding the collateral damage which this causes to legitimate content hosted on the same domain, viewing this as a means of incentivising domain owners to police their users.[79]

How does the IWF CAIC URL list fare in comparison? First, it must be noted that its subject matter is very narrow and limited to the most serious forms of illegal content. It is restricted to potentially illegal "indecent images of children, advertisements for or links to such content" and generally contains just 500-800 URLs.[80] It includes pseudo-photographs, but does not, for example, include non-photographic images of children (such as cartoons)[81] notwithstanding that these are now also illegal to possess.[82] IWF procedures have been modified after the Wikipedia case so as to no longer automatically include borderline images – particularly those that would be classed as level one according to the UK Sentencing Guidelines Council.[83] Also, unlike other entirely automated systems of filtering this relatively narrow scope enables it to rely entirely on manual intervention and human judgment to designate a URL to be blocked, and makes it possible to regularly review each URL. Finally, the blocking list has, since its inception, operated at the level of full URLs rather than domain names, allowing ISPs to reduce collateral damage.

In relation to the specific content sought to be blocked, therefore, it may be difficult to argue that the system is not proportionate and from the outset it has been designed to minimise overblocking. As against that, however, the manner in which blocking has

[78] See the discussion in Kreimer, 'Censorship by Proxy'.
[79] McIntyre, 'Blocking Child Pornography on the Internet'.
[80] Internet Watch Foundation, 'Blocking of Child Sexual Abuse Websites'.
[81] Internet Watch Foundation, 'Board Minutes 29 September 2009', 29 September 2009.
[82] Chapter 2, Part 2 of the Coroners and Justice Act 2009.
[83] Ozimek, 'IWF Takes "Pragmatic" Stance on Level One Images'; Internet Watch Foundation, 'IWF URL List Policy and Procedures'.

been implemented suggests that there are problems which in practice mean that overblocking is an issue.

In relation to the IWF list itself, the relatively small number of pages on the list and the manner in which they are updated suggest that overblocking is unlikely. That said, the Wikipedia incident exposed a flaw in that text pages relating to the album were being blocked, while the image files themselves were going unblocked. This appears to have been due to a technical misunderstanding on the part of IWF staff, who inadvertently listed text pages while intending to list images.[84]

Turning from the IWF list itself to its implementation by ISPs, more significant problems appear. Hybrid blocking systems, such as those pioneered by BT, are sufficiently granular so as to filter at the level of the individual URL.[85] However, not all systems are this sophisticated, and some ISPs have claimed that hybrid filtering of this sort can be too expensive to implement.

Consequently at least one ISP, apparently unwilling or unable to incur the cost associated with a BT-style hybrid blocking system, has implemented the CAIC list by 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.[86] Others – notably mobile broadband providers such as O2 – have taken a similarly crude approach and have used the CAIC list as the basis for DNS blocking, resulting in substantial blocking of unrelated content on image hosting sites.[87] These examples highlight the point examined later in this chapter that intermediaries, faced with

[84] Clayton, 'Technical Aspects of the Censoring of Wikipedia'.
[85] See e.g. Clayton, 'Anonymity and Traceability in Cyberspace'.
[86] Sebastien Lahtinen, 'Be Unlimited Causes Stir in Effort of Blocking Child Abuse Images', *Thinkbroadband.com*, 11 October 2007, http://www.thinkbroadband.com/news/3235-be-unlimited-causes-stir-in-effort-of-blocking-child-abuse-images.html.
[87] 'O2 Now Blocking Sites', *O2 Forum*, 17 September 2009, http://forums.o2online.ie/forums/showthread.php?6034-O2-now-blocking-sites&p=74137&viewfull=1#post74137; GSMA Mobile Alliance Against Child Sexual Abuse Content, 'Implementation of Filtering'.

difficulties in complying with regulatory demands, will systematically overblock where this is the least cost option open to them.

Similarly, not long after the Wikipedia block a further issue arose when numerous ISPs blocked any access to the entire of the Internet Archive's Wayback Machine (a site which lets users view web pages as they existed in the past) – cutting off UK users from a valuable research tool containing approximately 85 billion web pages.[88] In this case, as with the Wikipedia incident, the overblocking was the result of an unexpected technical interaction between the ISPs' proxy servers and the Internet Archive itself – rather than being a deliberate decision.[89] Consequently, it was not something which could be laid directly at the door of the IWF. Nevertheless, it illustrates how even a system designed to minimise collateral damage can inadvertently operate in a disproportionate manner.

(iv) Eliminating feedback

Another concern which has been expressed about regulation by code generally is that it may eliminate elements of feedback which are vital to good governance. This argument has a number of dimensions.

The first is a dignitarian one, which suggests that automated enforcement of rules objectifies individuals by failing to engage with their moral reasoning. This is an old concern in the field of situational crime prevention (SCP), summarised by Smith who notes that:

> The usual criticism of SCP is that it changes situations without changing people, and is therefore superficial and amoral. It is said to be like hiding the tin of sweets from the children, as opposed to teaching them not to eat more sweets than is good for them.[90]

[88] Metz, 'Brit Porn Filter Censors 13 Years of Net History'.
[89] Metz, 'Demon Ends Porn-Less Internet Archive Block'.
[90] David J Smith, 'Changing Situations and Changing People', in *Ethical and Social Perspectives on Situational Crime Prevention*, ed. Andrew von Hirsch, David Garland, and Alison Wakefield, Studies in Penal Theory and Penal Ethics (Oxford: Hart Publishing, 2000), 154.

A variant of this is a fear that automated enforcement may erode self-control by depriving individuals of the opportunity to exercise moral judgment[91] and perhaps even encouraging them to push boundaries knowing that automated controls will intervene to prevent them going too far.

Both of these concerns have been carried over from the real world into the virtual world, and Brownsword in particular has examined whether this use of code might, in his words, corrode moral community.[92] Without entering too deeply into this debate, it can be seen that it may have some application to filtering – and indeed Zittrain has suggested that where filters are in place then users might be absolved of liability for material which escapes the filtering system:

> The notion that some content is so harmful as to render its transmission, and even reception, actionable – true for certain categories of both intellectual property and pornographic material – means that certain clicks on a mouse can subject a user to intense sanctions. Consumers of information in traditional media are alerted to the potential illegality of particular content by its very rarity; if a magazine or CD is available in a retail store its contents are likely legal to possess. The Internet severs much of that signaling, and the ease with which one can execute an Internet search and encounter illegal content puts users in a vulnerable position. Perhaps the implementation of destination ISP-based filtering, if pressed, could be coupled with immunity for users for most categories of that which they can get to online in the natural course of surfing.[93]

While one can see the strength of this point, it does tend to establish the truth of Brownsword's fear that a community in which behaviour is channelled is also one in which individuals lose touch with the consequences of choices. Interestingly, prominent researchers in the field of child pornography have touched on the same point: Taylor and Quayle have expressed support for code based controls which will prevent access to child pornography, but also wish to see technology used to "alert the conscience" of viewers in order to help them manage change their behaviour.[94]

---

[91] Ibid., 160.
[92] Roger Brownsword, 'Code, Control, and Choice: Why East Is East and West Is West', *Legal Studies* 25 (2005): 1; Brownsword, *Rights, Regulation, and the Technological Revolution*.
[93] Zittrain, 'Internet Points of Control', 36.
[94] Taylor and Quayle, 'Criminogenic Qualities of the Internet in the Collection and Distribution of Abuse Images of Children', 127–128.

If we are to take these points seriously, then the deceptive error messages used by some ISPs are wrong in principle – at the least, stop pages should explain to viewers why their browsing was interrupted. Indeed, the CIRCAMP project has expressed support for stop pages for similar grounds – that they help to instil a sense of responsibility in viewers, as well as alerting them to the fact that the internet is a place which is policed in the same way as the real world.[95]

Another, more prosaic aspect of feedback relates to outcomes – assessing how automated enforcement systems are actually working. Here Grimmelman has pointed out that when we regulate by software we run the risk of creating systems that fail without any human review which can detect that failure.[96] Tien has similarly pointed out that architectural regulation may take away the public process associated with both making and applying legal rules.[97] When considered together, these considerations may mean that regulation by software may lose the feedback – from regulator to regulatee and *vice versa* – which is necessary to maintain and improve a system.

In the context of Cleanfeed, is this concern borne out? There is some feedback within the system in respect of false negatives – where the IWF does not block a particular page containing child pornography then a user who encounters that page may submit a report to the IWF via its hotline service seeking to have it blocked. There is not necessarily, however, the same feedback in respect of false positives – as we have seen, this depends on whether a particular ISP has chosen to implement stop pages. The result may be that wrongful blocking goes unnoticed. The Wikipedia blocking was unusual in that the high profile of the site affected and the technical side effects guaranteed that blocking would be detected by users. The same may not be true of less famous sites.

---

[95] CIRCAMP, 'CIRCAMP Overview', *CIRCAMP*, accessed 27 March 2010, http://circamp.eu/index.php?option=com_content&view=article&id=11:circamp-overview&catid=1:project&Itemid=2; CIRCAMP, 'CIRCAMP Fact Sheet English', *CIRCAMP*, accessed 20 July 2010, http://circamp.eu/index.php?option=com_content&view=article&id=15:circamp-fact-sheet-english&catid=1:project&Itemid=2.

[96] James Grimmelmann, 'Regulation by Software', *Yale Law Journal* 114 (2005): 1719.

[97] Lee Tien, 'Architectural Regulation and the Evolution of Social Norms', *Yale Journal of Law and Technology* 7 (2005): 1.

The Wikipedia case also illustrates a further consequence of a lack of feedback. In that case, the IWF asserted – correctly – that the image in question was "potentially illegal" under English law and therefore properly blocked under its guidelines as they stood.[98] What this failed to recognise, however, was a significant public consensus that the image was harmless; and a crisis for the IWF resulted when it was suddenly faced with this contrary view, forcing it to abandon this particular block. It might well be the case that more transparency – such as the use of stop pages – would have allowed for greater public feedback in respect of level one images before 2008, potentially allowing for an earlier change in policy and avoiding an incident which did significant damage to the IWF.[99]

(v) Function Creep

A common objection to regulation by code generally, and filtering in particular, is that it lends itself to function creep – that is, expansion beyond its original remit.[100] The risk is colourfully described by Tambini, *et al.*:

> Clearly the presence of an institution invites all sorts of 'Christmas Tree' dangers whereby more and more categories of content are 'hung from' the existing list of illegal content the IWF should remove, 'because it is there'.[101]

This is true to some extent of the IWF itself, which has taken on a reporting and notice and take down role in relation to the new offence of extreme pornography[102] – although

[98] Internet Watch Foundation, 'Board Minutes 9 December 2008'; Internet Watch Foundation, 'Board Minutes 27 January 2009'.
[99] Ozimek, 'Scorpions Tale Leaves IWF Exposed'.
[100] Callanan et al., *Internet Blocking*, 129.
[101] Tambini, Leonardi, and Marsden, *Codifying Cyberspace*, 296.
[102] See e.g. Internet Watch Foundation, 'Board Minutes 25 Nov 2008', *Internet Watch Foundation*, 25 November 2008, http://iwf.org.uk/corporate/page.200.htm.

it has also shed its functions in relation to racist material.[103] But is it also true of the Cleanfeed system specifically?

There has certainly been a great deal of discussion about extending the remit of the system. For example, in 2008 the Home Secretary suggested that "terrorist" sites should be blocked[104] while in 2010 the Home Office *Sexualisation of Young People Review* recommended that pro-anorexia sites should also be blocked.[105] Indeed, Roger Darlington – a former Chair of the IWF – has gone so far as to suggest that *all* harmful content (which he describes as content "the creation of which or the viewing of which involves or is likely to cause actual physical or possible psychological harm") should be voluntarily blocked by ISPs.[106] There has been some public support for the suggestion that ISPs should track access to child pornography sites for police purposes.[107] In the 2011 review of the *Prevent* counter-terrorism strategy the Home Office has reverted to its 2008 thinking and has stated that it wants to:

> explore the potential for violent and unlawful URL lists to be voluntarily incorporated into independent national blocking lists, including the list operated by the Internet Watch Foundation.[108]

Despite these suggestions, however, the IWF blacklist has not (with one very minor exception which will be considered later) been expanded beyond its original function. Even where the IWF has adopted a takedown role in relation to other illegal content such as extreme pornography, it has not been prepared to add that content to the CAIC list.[109]

---

[103] Internet Watch Foundation, 'Incitement to Racial Hatred Removed from IWF's Remit', *Internet Watch Foundation*, 11 April 2011, http://www.iwf.org.uk/about-iwf/news/post/302-incitement-to-racial-hatred-removed-from-iwfs-remit.
[104] Helene Mulholland, 'Government to Stamp down on Terror "Grooming" Websites', *The Guardian*, 17 January 2008, http://www.guardian.co.uk/politics/2008/jan/17/uksecurity.terrorism.
[105] Linda Papadopoulos, *Sexualisation of Young People Review* (Home Office, 2010).
[106] Roger Darlington, 'How the Internet Could Be Regulated', 7 January 2009, http://www.rogerdarlington.co.uk/Internetregulation.html.
[107] Malcolm Hutty, '89% Say ISPs Should Track Access to Paedophile Sites', *LINX Public Affairs*, 16 March 2005, https://publicaffairs.linx.net/news/?p=281.
[108] Home Office, *Prevent Strategy* (London: HMSO, 2011), 79.
[109] On extreme pornography see Internet Watch Foundation, 'Board Minutes 25 Nov 2008'.

In fact, not all "child pornography" is blocked – non photographic images ("virtual" child pornography) are not included on the CAIC list.[110]

Why has the remit of the blocking list not been expanded? It is difficult to give a complete answer, but a number of factors appear to play a role. First, notwithstanding the Wikipedia incident, child abuse images are for the most part uncontentious both in the sense that there is a wide public consensus that they should be illegal[111] and also in the sense that there will often be little room for debate as to whether a particular image is, in fact, illegal. Other material does not share these attributes, which in the case of extreme pornography caused the IWF Board to be nervous of an "increased likelihood of challenges from content owners which may damage IWF's reputation".[112]

Secondly, there are resource implications for the IWF in any expansion of its remit generally. In relation to both extreme pornography and non-photographic images the Board expressed concern that any expansion of the IWF role could take additional staff time and impose additional costs in a way which might undermine the priority given to child abuse images.[113] This may be particularly so given that one would expect those images to be much more common. Consequently, children's groups – who are well represented on the IWF board – are strongly against expansion of the IWF remit.[114]

Resource issues are also implicated in a third reason – the industry simply does not wish to pay for the costs associated with a wider function. This point has been made by a number of interviewees who have indicated that industry funding acts as a natural check on IWF function creep.[115]

---

[110] Internet Watch Foundation, 'Board Minutes 29 September 2009', 29 September 2009.
[111] A point made by former IWF Chief Executive Peter Robbins . See John Ozimek, 'IWF Chief: We Don't Need Crusaders', *The Register*, 8 September 2009, http://www.theregister.co.uk/2009/09/08/iwf_perter_robbins_interview/.
[112] Internet Watch Foundation, 'Board Minutes 25 Nov 2008'.
[113] Ibid.; Internet Watch Foundation, 'Board Minutes 29 September 2009', 29 September 2009.
[114] John Carr, Telephone interview, 16 November 2009; John Carr, 'Submission Regarding Communications Bill', 10 June 2002, http://www.chis.org.uk/uploads/55.pdf.
[115] See e.g. Peter Sommer, Telephone interview, 2 November 2009.

Consequently, the point has been forcefully made by many observers that a co-regulatory model such as that of the IWF may be more rather than less resistant to function creep as compared with a system which operated in the public sphere on a legislative basis – that the involvement of industry ensures greater restraint.[116]

As already mentioned, there has been one case in which the CAIC list was used for a different purpose - the IWF board minutes from January 2007 indicate that the list was used in one case as an "intelligence tool" involving "the monitoring of school networks to identify devices where an attempt was made to access a URL on the CAIC list". The Board, however, on being briefed expressed concern that this "could lead to the identification of potential offenders" and on that basis the IWF withdrew from the project.[117]

This tends to confirm the point that the IWF structure is resistant to function creep – when brought to the Board the response was negative, despite the obvious possible value of the system for law enforcement, and the two IWF members concerned were prevented from using the list for that purpose in future. It should also be pointed out that the IWF members who deploy blocking have generally designed their systems in a way which minimises logging of user data and thus the possibility that the logs might be used by police to identify attempted viewers.[118]

That said, the very existence of the Cleanfeed system has acted as a proof of concept which has encouraged blocking generally in the UK – even if it takes place outside the IWF structure. Two examples are particularly important. First, in the recent debates on the Digital Economy Bill the perceived success of Cleanfeed was used to justify the

[116] Ibid.
[117] Internet Watch Foundation, 'Minutes of Board Meeting'.
[118] Truman, Telephone interview.

blocking of sites for alleged copyright infringement – see e.g. the comments of Lord Clement-Jones[119] who in introducing an amendment providing for blocking said that:

> site blocking already exists. It is perfectly legitimate to do that. This is not a novel concept. There are sites that are identified as being blocked in various fields. I am not saying child pornography is equivalent to copyright infringement... If you're infringing somebody's copyright on the web, it's something that should not be taking place.

It would not be fair, however, to describe this as function creep on the part of the IWF itself – if anything, it tends to reinforce the point that the IWF is resistant to function creep, insofar as it involves an entirely different mechanism being used to achieve blocking.

The second example, however, is more significant and the decision of the High Court in *Twentieth Century Fox v. BT*[120] (better known as "Newzbin2") proves the truth of concerns about function creep in relation to particular filtering technologies deployed by ISPs. In this case, an action brought by the movie industry succeeded in obtaining a High Court judgment requiring BT to use its Cleanfeed system to block access to a particular website – Newzbin2 – which they say infringes their copyright.

To appreciate the impact of this judgment, one must go back somewhat. In 2004 – when BT initially adopted Cleanfeed – it was obvious even then that there was a risk of function creep and in particular that copyright holders would seek to use the system. At the time, however, BT believed that it was unlikely to be sued and that it could mitigate this risk by discontinuing the use of Cleanfeed if function creep became a reality.[121] According to a contemporaneous briefing to LINX members, BT's views were as follows:

[119] 'Lib Dem Peer on Why Site Blocking Is Needed'.
[120] [2011] EWHC 1981 (Ch).
[121] Hutty, 'Cleanfeed: The Facts'.

> Scope creep is a serious risk
>
> The Home Office originally indicated to BT that Cleanfeed might be employed to block access to other undesirable content.
>
> Wannadoo has already been approached by the British Phonographic Industry (BPI) about implementing a system similar to Cleanfeed so as to block access to works allegedly infringing copyright.
>
> BT says that if the pressure to extend the scope of Cleanfeed became too great it would simply cancel the project...
>
> BT is unlikely to be the defendant of choice for a copyright holder or other party attempting to hold an ISP legally responsible for Internet traffic.

The ruling in *Newzbin2*, however, showed the flaws in this reasoning. Once the Cleanfeed system had provided the technical proof that the blocking requested by the plaintiffs could be achieved, BT became a natural target for copyright plaintiffs. Indeed, according to a representative of the movie industry: "BT was chosen because it's the largest and already has the technology in place, through its Cleanfeed system, to block the site".[122] At this point, the idea that the idea that BT could unilaterally turn off the blocking system became unrealistic. To the contrary, the court in *Newzbin2* laid great emphasis on the fact that:

> the order sought by the Studios is clear and precise; it merely requires BT to implement an existing technical solution which BT already employs for a different purpose; implementing that solution is accepted by BT to be technically feasible; the cost is not suggested by BT to be excessive.[123]

Does *Newzbin2* therefore prove the truth of concerns about function creep in the context of Cleanfeed? The answer is both yes and no. Almost all critics who expressed concern about function creep predicted that the executive would exert pressure on the IWF to expand the scope of its URL list.[124] As we have seen, however, despite government

[122] Chris Williams, 'Hollywood Studios Ask High Court to Block Film Website', *The Telegraph*, 27 June 2011, http://www.telegraph.co.uk/technology/news/8597596/Hollywood-studios-ask-High-Court-to-block-film-website.html.
[123] Para. 177.
[124] Edwards, 'From Child Porn to China, in One Cleanfeed'.

leanings in this direction the IWF has not expanded its blocking function and is unlikely to do so. In this regard, fears of function creep by the IWF itself have been misplaced and did not give adequate weight to the incentives faced by industry and the IWF and the manner in which these have been a buffer against further expansion of state control over the internet.

On the other hand, the decision in *Newzbin2* proves that the filtering technologies implemented by ISPs can be co-opted for other purposes even if the IWF itself is not. In this wider sense fears of function creep have been proved correct in relation to filesharing – and it seems likely that plaintiffs will seek to expand blocking to other areas such as defamation and privacy claims.[125] Indeed Max Mosley has already argued that blocking should be used against news sites which breach press standards. Mr. Mosley is best known as the victim of press intrusion involving the videoing of a sex session[126] and is suing Google in a number of jurisdictions seeking a filter to proactively block images from that session from search results.[127] In testimony to the Culture, Sport and Media Committee following the Leveson Inquiry he has claimed that filtering should also apply at the ISP level, urging that ISPs be required to "cut the wire" to offshore news sites which do not abide by a UK code of practice.[128] Whether or not he is successful in this particular claim it nevertheless illustrates the point that once a technology of control is in place there will be numerous parties seeking to use it.[129]

---

[125] Though note that in *Newzbin2* Arnold J. suggests that filtering may not be available as a remedy in such cases: "Counsel for BT also suggested that applications would be made in respect of websites alleged to contain defamatory allegations or private information. In my view applications in respect of websites of those kinds would be likely to raise separate issues to the present application, as well as common ones, and would require separate consideration. Even if the present application succeeds, it does not automatically follow that applications in respect of such websites would succeed." (Para. 188)

[126] Gavin Phillipson, 'Max Mosley Goes to Strasbourg: Article 8, Claimant Notification and Interim Injunctions', *Journal of Media Law* 1, no. 1 (2009): 73.

[127] Michael Stothard, 'Mosley Takes Google Privacy Battle to French Court', *Financial Times*, 4 September 2013, http://www.ft.com/intl/cms/s/0/23705a3c-1581-11e3-950a-00144feabdc0.html?siteedition=intl.

[128] 'Max Mosley Wants Websites Closed down If They Flout New Press Watchdog Rules', *The Mirror*, 19 March 2013, http://www.mirror.co.uk/news/uk-news/max-mosley-wants-websites-closed-1773836.

[129] It has, for example, been suggested that the Icelandic Modern Media Initiative might lead to Icelandic media being blocked in other jurisdictions: Rachael Craufurd Smith, 'Reflections on the Icelandic Modern

5. Gatekeeper regulation

(i) Reintermediation

The cyber-libertarian promise of disintermediation was, according to the cyber-paternalists, somewhat oversold. While acknowledging that the internet has resulted in some disintermediation, theorists pointed to the growth of entirely new intermediaries, who often enjoyed greater capacity to control the actions of their users. In relation to private communications, for example, the Post Office may be replaced by ISPs or webmail providers who will (as a practical matter) have a greater technical capability to screen communications, and may be exempt from older laws prohibiting this.

In addition, the nature of the internet gives rise to a need for new intermediaries. The search engine, for example, has no exact counterpart in the offline world, but without a listing in a search engine a site might as well cease to exist for many users. Similarly, transactions which in the real world could be carried out anonymously and directly by cash become impossible online, leading to a situation where the use of payment services becomes necessary.[130] Noting this, cyber-paternalists such as Zittrain pointed to ISPs, search engines, hosting providers, domain name providers and other intermediaries as new "Internet points of control" and developed theories of gatekeeper regulation to assess how states might use these points of control to regulate user behaviour.[131]

Media Initiative: A Template for Modern Media Law Reform?', *Journal of Media Law* 2, no. 2 (1 December 2010): 210.

[130] Mann and Belzley, 'The Promise of Internet Intermediary Liability'.

[131] On gatekeeper theory see in particular Reinier Kraakman, 'Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy', *Journal of Law, Economics and Organization* 2, no. 1 (1 January 1986): 53.

(ii) From mice to elephants: shifting the focus of regulation

The attraction for states of gatekeeper regulation is noted by Swire who uses the analogy of elephants and mice in assessing how difficult it is to control behaviour. In short, he points out that problems with tackling numerous internet users or individual sites ("mice") can be avoided if states turn their enforcement powers against the relatively small number of large, immobile and easily targeted intermediaries such as ISPs or payment providers ("elephants") – requiring them in turn to devise ways to control their users.[132]

This approach is justified by some on economic grounds, with Mann and Belzley in particular suggesting that liability should be imposed on intermediaries for the wrongful conduct of their users where it can be shown that the intermediary is the least cost avoider. In that context, they argued for legislation which would force ISPs and payment providers to take active steps to prevent their users from viewing or paying for child pornography, saying that:

> [G]atekeeper liability is systematically more likely to be effective in the modern internet environment than it has been in traditional offline environments... [It is] increasingly cost-effective for intermediaries to monitor more closely the activities of those that use their networks. As it becomes cheaper to monitor activity more closely, it ineluctably becomes *relatively* more desirable to rely on such monitoring as the least expensive way to eradicate undesirable activity.[133]

(iii) Censorship by proxy? Criticisms of gatekeeper regulation

Against this strategy, others have claimed that intermediary regulation is particularly prone to damaging freedom of expression. Kreimer, for example, has expressed concerns about what he terms "censorship by proxy" online, arguing that it changes the dynamic of censorship.[134] Unlike traditional forms of content control – which generally

[132] Swire, 'Of Elephants, Mice, and Privacy'.
[133] Mann and Belzley, 'The Promise of Internet Intermediary Liability', 21.
[134] Kreimer, 'Censorship by Proxy'.

target either the speaker or the recipient of speech – intermediary regulation targets someone who usually does not have any direct interest in the speech. As a result, that intermediary will often lack any incentive to notify either the speaker or the user of the fact of censorship – and may similarly lack any incentive to minimise the collateral damage caused by the censorship. The experience of ISPs deploying Cleanfeed bears out this point, showing that ISPs have tended to act in a way which both conceals the fact of blocking and also overblocks.[135]

6. Effectiveness

(i) Objectives

When BT initially introduced filtering, they were clear that it was intended to serve a relatively modest goal – to "prevent casual web access to URLs listed on the Internet Watch Foundation's "Child Abuse Images" database"[136] and also "unintentional" or accidental access. Their representatives were keen to stress that it "won't stop a hardened paedophile and we're not saying that".[137]

The IWF, on its own website, describes the goal as follows:

> This initiative is designed to reduce the occasions when innocent internet users might be exposed to traumatic and unlawful images, however it may also help to:
>
> - Diminish the re-victimisation of children by restricting opportunities to view their sexual abuse.
> - Disrupt the accessibility and supply of content to those who may seek out such images.
> - Disrupt the dissemination of images to UK internet users for commercial gain by criminal organisations.[138]

[135] See sections 4(ii) and 4(iii) of this chapter.
[136] Hutty, 'Cleanfeed: The Facts'.
[137] Leyden, 'BT's Modest Plan to Clean up the Net'.
[138] Internet Watch Foundation, 'Blocking of Child Sexual Abuse Websites'.

Despite some political confusion (which tends to oversell the capabilities of blocking), this has remained the consistent position of the IWF and technically knowledgeable advocates. As Carr puts it: "It was intended to block the guy in his office at home one night, pi**ed, mildly curious, who could get himself into jail by going off and looking for it. It's meant to stop the accidental exposure".[139]

While this goal is expressed in a way which focuses on the wellbeing of the viewer, it appears to be closely tied with a concern that viewers will ultimately go on to commit "real-world" offences against children – that is, that accidental or casual exposure to child pornography will contribute to further offending. Again, Carr has made this argument in the UK context:

> Many of those who start looking at child abuse images on the internet, or who start collecting images they have obtained from the internet, may already have a direct sexual interest in children of which they were aware, or they may believe their interest is limited only to looking and collecting. For others, the internet will provide their first ever introduction to the idea of having sex with children or to child abuse images... The key point is that many of those who come to it for the first time, and even many of those with a pre-existing interest, would almost certainly never have got involved with the images in the real world, perhaps for a mixture of reasons but probably mainly because the amount of effort needed to obtain such images would be a major disincentive, or because of their fear of getting caught…
>
> [I]s it really possible to say that, having had their sexual interest in children stimulated, extended or created by the kind of exposure to the images the internet allows, some of these same people will, in turn, go on to abuse children directly because of that? If it is, the implication is clear: but for those prior processes, any children thus abused would have been spared.[140]

It must be noted, however, that the literature is not conclusive as to whether exposure to child pornography does in fact cause "real world" offending. While some authors – such as Russell and Purcell[141] and Bourke and Hernandez[142] – make a strong argument that it does, there appears to be no definitive study.[143]

---

[139] Barry Collins, 'Charity: Child Abuse Filters Save Men from Themselves', *PC Pro*, 23 February 2009, http://www.pcpro.co.uk/news/248117/charity-child-abuse-filters-save-men-from-themselves/print.
[140] Carr, *Child Abuse, Child Pornography and the Internet*, 7.
[141] 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.

Consequently, if we take the goal as being to protect users and thereby indirectly to protect children – has Cleanfeed been effective in achieving this goal?

Here we are hampered by an almost complete lack of data. In the first instance, there does not appear to be any evidence that accidental exposure has been a problem in need of a solution. In a recent Dutch study Stol *et al.* were not able to find any credible reports of accidental exposure, noting that:

> Where internetters use a spam filter, are not searching for sex sites, do not participate in sexual news groups or panels and do not take notice of obscure messages that always seem to pass despite safety precautions, the chance of encountering child pornography seems minimal... No interviewed expert, authority or other person involved was able to refer to a case in which a 'decent' internetter was unexpectedly or incidentally confronted with child pornography on a website.[144]

It may be more likely that what Carr describes as casual viewing has been a problem – again, however, we appear to have very little evidence, except for the statistics generated by the Cleanfeed system itself. After BT implemented the Cleanfeed system, media coverage indicated it was blocking "20,000 hits per day". By 2009 that figure had been raised to 45,000 hits per day.[145] This headline figure was taken by mainstream media to indicate that the system was a substantial success[146] – but was soon challenged by the ISPA on the basis that a substantial portion of this traffic appeared to be generated by

---

[142] Michael Bourke and Andres Hernandez, 'The "Butner Study" Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders', *Journal of Family Violence* 24, no. 3 (1 April 2009): 183.

[143] See e.g. the review of the literature in O'Donnell and Milner, *Child Pornography: Crime, Computers and Society*, 74–77; Child Exploitation and Online Protection Centre, 'A Picture of Abuse: A Thematic Assessment of the Risk of Contact Child Sexual Abuse Posed by Those Who Possess Indecent Images of Children', June 2012, http://ceop.police.uk/Documents/ceopdocs/CEOP%20IIOCTA%20Executive%20Summary.pdf.

[144] Stol et al., 'Governmental Filtering of Websites', 254.

[145] Nick Truman, 'The Experience of BT in Online Child Protection' (presented at the Effective Strategies for the Prevention on Child Online Trafficking Pornography and Abuse, Bahrain, 9 May 2009), http://www.befreecenter.org/Upload/Conference/papers/BT.ppt.

[146] Hutty, 'Cleanfeed: The Facts'.

spam, pop-ups and other sources rather than deliberate attempts to access child pornography.[147]

The technical approach used by BT has ensured that no conclusive analysis of their figures can be carried out. That said, many of those hits appear to be due to foreign internet users taking advantage of open proxies situated within the UK – undermining arguments that UK users are being protected or that viewing is being deterred.[148] It should be acknowledged at this point that this data is fragmentary and somewhat anecdotal – but it also must be said that these limitations are inherent in the nature of the system. By shifting enforcement to private ISPs the Cleanfeed system may escape the mechanisms (such as regulatory impact assessments and freedom of information oversight) which might enable such a system to be the subject of more rigorous assessment if publicly operated.

In assessing the effectiveness of filtering systems we must also consider underblocking – that is, the extent to which a particular filtering system fails to achieve its regulatory goal, by allowing the targeted content to be accessed.[149] Here, the very limited scope of Cleanfeed must be noted. It filters only web traffic and critics have pointed out that it fails to deal with equally accessible CAI via IRC, instant messaging or peer to peer sources.[150] Jim Gamble – former chief executive of Ceop – has reported that Cleanfeed was a "fabulous success" but that it was essentially limited to inadvertent or novice access and ineffective against "hardcore predators". Instead, he stated that the problem had largely moved on from websites and towards peer to peer networks, so that he was unconvinced of the need to further expand the system.[151]

---

[147] Richardson, 'ISPA Seeks Analysis of BT's "Cleanfeed" Stats'; Richardson, 'BT on Child Porn Stats'.
[148] Truman, Telephone interview; Truman, 'The Experience of BT in Online Child Protection'.
[149] Derek Bambauer, 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering', 2008, http://ssrn.com/paper=1143582.
[150] Wendy Grossman, 'IWF Reforms Could Pave Way for UK Net Censorship', *The Register*, 29 December 2006, http://www.theregister.co.uk/2006/12/29/iwf_feature/.
[151] Williams, 'New Web Filter Laws Questioned by Top Child Abuse Cop'.

Even in relation to web browsing, however, the system may be of less value than might first appear. The IWF block list usually contains approximately 500-800 URLs.[152] The list is, however, passive. It is based solely on reports received via the hotline and not on any proactive searching by IWF analysts.[153] Consequently, it is not clear to what extent the IWF list covers the full range of websites which might be accessed by the "casual viewer". Do the URLs blocked cover the majority of this content, or only a minority? Edwards has suggested that the block list may catch less than twenty per cent of child pornography sites, though she gives no source for this estimate.[154] There appears to be no detailed research on this point – and the legal prohibitions on the viewing and possession of child pornography would appear to rule out most methods for carrying out such research. The result is that there is little evidence one way or the other as to whether Cleanfeed is effective at its stated goal of blocking casual viewing.

(ii) Circumvention

Internet regulation is dynamic rather than static and the regulatory target may seek to avoid regulation by changing their tactics in response.[155] In the case of filtering, this may be done by using technical means which will allow particular forms of filtering to be circumvented. In considering the effectiveness of Cleanfeed, therefore, we must answer two questions: how easily can ISP filtering systems be circumvented, and are users aware of those means of circumvention?

Experts have for some time pointed out that web blocking is easily evaded and indeed a report published by Ofcom in 2011 confirms this, saying "[f]or all blocking methods

[152] Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative'.
[153] Though there are proposals to move towards proactive searching. See Department for Culture, Media and Sport, 'Tackling Illegal Images - New Proactive Approach to Seek out Child Sexual Abuse Content', *GOV.UK*, 18 June 2013, https://www.gov.uk/government/news/tackling-illegal-images-new-proactive-approach-to-seek-out-child-sexual-abuse-content.
[154] Lilian Edwards, 'Pornography, Censorship and the Internet', in *Law and the Internet*, ed. Lilian Edwards and Charlotte Waelde, 3rd ed. (Oxford: Hart Publishing, 2009), 667.
[155] Andrew Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Abingdon: GlassHouse, 2007).

circumvention by site operators and internet users is technically possible and would be relatively straightforward by determined users".[156]

This, of course, is not the full story. The fact that blocking can be circumvented does not necessarily mean that it will be circumvented – this depends on the motivation and knowledge of the affected users. However a 2010 study of convicted child pornography offenders in Sweden revealed that all the offenders questioned were aware of the existing filtering systems and how to bypass them – significantly, even those who were initially unaware of how to do so soon learned under the tutelage of more experienced users.[157] Awareness of techniques such as proxy servers and alternative DNS providers was high – both of which would also serve to defeat the UK implementations of blocking.

Perhaps ironically, function creep within the UK will ensure the further spread of knowledge as to how to circumvent blocking. There is already a growing level of awareness amongst internet users of technical controls on their behaviour and how to circumvent them. For example, expatriates who wish to view the BBC iPlayer have learned how to use VPNs or proxy servers for the purpose of defeating geolocation technologies.[158] The *Newzbin2* decision and the cases which followed it have provoked a backlash from users who have developed tools to circumvent copyright blocking – tools which will then be readily transferable to accessing sites blocked as containing child pornography.[159]

---

[156] Ofcom, *'Site Blocking' to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act* (London, 2011), 4.
[157] Marie Eneman, 'Internet Service Provider (ISP) Filtering of Child-Abusive Material: A Critical Reflection of Its Effectiveness', *Journal of Sexual Aggression: An International, Interdisciplinary Forum for Research, Theory and Practice* 16, no. 2 (2010): 223.
[158] For background see Svantesson, 'How Does the Accuracy of Geo-Location Technologies Affect the Law'.
[159] See e.g. Mark Jackson, 'Banned Piracy Website Expands BT Circumvention Tool to Include The Pirate Bay', *ISP Review*, 6 October 2011, http://www.ispreview.co.uk/story/2011/10/06/banned-piracy-website-expands-bt-circumvention-tool-to-include-the-pirate-bay.html.

7. Conclusion

This chapter has outlined the predictions of both cyber-libertarians (as to factors that will limit state regulation of the internet) – and cyber-paternalists (as to the regulatory strategies which states may use in response, and the risks which these might pose) and considered the UK situation in light of these predictions. In doing so, it has shown that many of the cyber-paternalists' predictions have been borne out in the context of Cleanfeed which by deploying both code as law and gatekeeper regulation has established a system which is opaque, prone to overblocking, and is capable of being captured for other uses also.

It also, however, illustrates that only some of the risks identified by the cyber-paternalists have manifested themselves. In particular, it is striking that concerns about function creep, overblocking and transparency have come true – but more so at the level of the ISP rather than the level of the IWF itself. This suggests that in some cases the cyber-paternalist predictions have not been sufficiently nuanced, and may need to be modified to consider in more detail the incentives faced by intermediaries. Many interviewees have suggested that the IWF and Cleanfeed have between them been "the saviour of the UK internet from further regulation"[160] and have argued that governmental schemes are "massively less transparent".[161] From this perspective, intermediary self-regulation in the form of the IWF may in fact help to maximise transparency and prevent function creep, as compared with direct legislative intervention. This point will be taken up further in the next chapter.

[160] Truman, Telephone interview.
[161] Perry, Telephone Interview.

Chapter 5 – Self-regulation

1. Introduction

> Self-regulation is the principle on which the IWF's operations and structures are founded; it is also the government and internet industry's preferred method of regulating internet content in the UK. Self-regulation and multi-stakeholder partnerships are at the core of the IWF's model, operations and success.
>
> – Internet Watch Foundation, 2011[1]

The previous chapter identified three regulatory strategies which have been promoted by cyber-paternalists as enabling greater state control of internet content, and examined how the Cleanfeed system has made use of the first two of these: code as law and gatekeeper regulation. This chapter considers the third strategy – self-regulation (along with the closely related concept of co-regulation). It outlines the literature on self- and co-regulation, describing its possible advantages and risks when applied to internet regulation. It then assesses the operation of the Cleanfeed system against this background and considers how it exemplifies both the desirable and undesirable aspects of self-regulation.

In particular, this chapter will:

- Introduce self- and co-regulation in the context of the internet and discuss difficulties in defining and applying the concepts;
- Discuss the attractions of self-regulation as a regulatory strategy online and the criticisms which have been levelled against it;
- Outline UK government policy favouring self-regulation on the internet, with particular reference to the IWF and Cleanfeed; and

[1] Internet Watch Foundation, 'Self-Regulation', *Internet Watch Foundation*, accessed 2 November 2011, https://www.iwf.org.uk/members/self-regulation.

- Consider whether the experience of the IWF and Cleanfeed can be used to validate, refute or refine predictions regarding the operation of self- and co-regulation.

2. Defining self- and co-regulation

(i) What do we mean by regulation?

> The contrast between the care taken to regulate content broadcast using traditional means—through dedicated regulators, codes and sanctions—and the near absence of control over access to Internet content is striking.
>
> – Select Committee on Culture, Media and Sport, 2008[2]

Before we attempt to define self- and co-regulation, we might first ask a preliminary question – what do we mean by regulation itself? In the quotation which starts this section the Select Committee on Culture, Media and Sport claims to have identified a "near absence of control over access to Internet content" in the United Kingdom. Given, however, that the Select Committee discusses elsewhere in its report the extensive role played by bodies such as the IWF and controls such as parental filtering, it seems that the Select Committee was in that sentence implicitly adopting a traditional view of regulation, one which is both "state-centric" and "rule-centric"[3] – that is, one which privileges the role of the state and which assumes that control should be mediated through a system of rules as commands.[4]

Such a view, however, would be challenged by many as tending to give an inadequate picture of regulation in general and internet regulation in particular. Johnson and Post,

---

[2] Select Committee on Culture, Media and Sport, *Harmful Content on the Internet and in Video Games* (London: HMSO, 2008), para. 77, http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/35302.htm.

[3] Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge: Cambridge University Press, 2007), 4.

[4] This emphasis on *state* intervention is all too common in discussion of media regulation – see Mike Feintuck and Mike Varney, *Media Regulation, Public Interest and the Law*, 2nd ed. (Edinburgh: Edinburgh University Press, 2006), 202–206.

for example, would dispute the state-centric aspect, arguing that "the community of online users and service providers is up to the task of developing a self-governance system".[5] Lessig has suggested that a rule-centric approach tends to obscure the role played by code and architecture as modalities of regulation – modalities which can be much more effective and pervasive than traditional rules which rely on the obedience of those to whom they are directed.[6] Yeung has similarly pointed to successful means of regulation by communication – termed by her "disclosure", "exhortation", "explanation" and "exclamation and excoriation" – which may be successful in promoting a desired end but which need not always rely on state involvement.[7]

For those reasons, it seems desirable to adopt a wider view of regulation, and for the purposes of this chapter the definition of regulation offered by Hood, Rothstein and Baldwin will be followed, where they suggest that regulation is characterised by the presence of three factors:

> There must be some capacity for *standard setting*, to allow a distinction to be made between more or less preferred states of the system. There must also be some capacity for *information gathering* or monitoring to produce knowledge about current or changing states of the system. On top of that must be some capacity for *behaviour-modification* to change the state of the system.[8]

This definition, focusing as it does on the *operation* of regulation rather than either the regulatory *actors* or the regulatory *tools*, appears to be more apt to cover the range of regulatory interventions which have characterised the control of internet content in the UK.

[5] Johnson and Post, 'Law and Borders - The Rise of Law in Cyberspace'.
[6] Lessig, *Code*.
[7] Karen Yeung, 'Government by Publicity Management: Sunlight or Spin?', *Public Law*, 2005, 360.
[8] Christopher Hood, Henry Rothstein, and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford: Oxford University Press, 2004), 23.

(ii) Introducing self-regulation

We can now consider what we mean when we speak of self-regulation. This is not an easy question to answer – as Price and Verhulst note "[t]he initial problem of every approach to self-regulation pertains to definition and semantics" in respect of a term which is used "almost indiscriminately".[9] In addition, the terms self-regulation and co-regulation have acquired specialised and technical meanings in European law, which often differ from national understandings.[10] Nevertheless, the term self-regulation remains in common usage and is helpful as describing an approach to regulation which is marked by an avoidance of direct government or legislative control, and instead places responsibility for rule making and enforcement on the group regulated.

In a general sense we can begin to define self-regulation by contrasting it with state-centric modes of governing. In particular, self-regulation can be compared with its supposed antithesis of command and control regulation which (in its crudest conceptions) involves public authorities issuing orders to individuals or corporations, on threat of punishment if those orders are disobeyed. By contrast, the essence of self-regulation is that it relies on consent and consensus to implement a system whereby private entities themselves devise and apply rules and standards to govern their own conduct.[11] As Koops, *et al.* put it:

> In its most extensive form, self-regulation implies that private actors themselves implement the applicable norms and rules and, ideally, monitor compliance and enforce the rules in case of non-compliance. Self-regulation is therefore often used as an argument in proposing a system that is different from formal regulation by national governments or international regulatory bodies[12]

This comparison between command and control and self-regulation is, however, apt to be misleading. By setting up a false dichotomy between the two forms of regulation, it

[9] Price and Verhulst, *Self-Regulation and the Internet*, 3.
[10] Linda Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?', *Electronic Journal of Comparative Law* 9, no. 1 (2004).
[11] Julia Black, 'Constitutionalising Self Regulation', *Modern Law Review* 59 (1996): 27.
[12] Koops et al., 'Should Self-Regulation Be the Starting Point?'.

encourages us to think of each in artificial and idealised terms. Instead, it has often been argued that self-regulation is better understood as an umbrella term which covers a range of activities with varying mixes of private and state involvement.[13] For example, in an influential taxonomy Black has identified four possible types of state involvement in self-regulatory systems:

> *mandated* self-regulation, in which a collective group, an industry or profession for example, is required or designated by the government to formulate and enforce norms within a framework defined by the government, usually in broad terms;
> *sanctioned* self-regulation, in which the collective group itself formulates the regulation, which is then subjected to government approval;
> *coerced* self-regulation, in which the industry itself formulates and imposes regulation but in response to threats by the government that if it does not the government will impose statutory regulation; and
> *voluntary* self-regulation, where there is no active state involvement, direct or indirect, in promoting or mandating self-regulation.[14]

While Black did not have the internet in mind in devising this classification, it has been extended and applied to the internet by others such as Price and Verhulst[15] and more recently Mifsud Bonnici who describes self regulation as encompassing "statutory self-regulation", "mandated or delegated self-regulation" and "coerced self-regulation" where the state respectively either requires private groups to engage in self-regulation, delegates rulemaking and enforcement powers to private groups, or uses political pressure to coerce private groups into self-regulation.[16]

(iii) From self-regulation to co-regulation

These definitions of self-regulation have not, however, been universally followed. In particular, what Black terms "mandated" or "sanctioned" self-regulation – those cases

[13] See generally e.g. Darren Sinclair, 'Self-Regulation versus Command and Control? Beyond False Dichotomies', *Law & Policy* 19, no. 4 (1997): 529.
[14] Black, 'Constitutionalising Self Regulation', 27.
[15] Price and Verhulst, *Self-Regulation and the Internet*, 11–12.
[16] Mifsud Bonnici, *Self-Regulation in Cyberspace*, chap. 3.

where there is formal state involvement in the establishment of regulation – would now more often be described as examples of "co-regulation".[17]

The origins of this term have been traced by Marsden to late 1980s Australia where it was first used to describe a hybrid of state and self-regulation.[18] Since then, it has become more prominent in the regulatory and legal literature – particularly in Europe, following the 2003 European Union adoption of definitions of self- and co-regulation and guidelines as to when each will be an appropriate means of achieving a particular goal.[19]

At first glance, this might seem to be a merely semantic difference, one which simply changes the label applied to what is otherwise the same activity. There have, however, been strong arguments made that the term helps with the analysis of structures in this area. Prosser, for example, has argued that the terms self-regulation and command and control have come to be used as crude political slogans for or against certain outcomes, while in reality there is no such thing as pure self-regulation or pure command and control.[20] Instead, he argues that the concept of co-regulation offers a more sophisticated and balanced basis for analysis. In the same way, it can be said that the term co-regulation better draws our attention to the cooperation and interaction which is present in those systems where the state is directly involved, rather than focusing our attention on merely one part of the system.[21]

Notwithstanding these disagreements as to terminology, there is consensus on a more general concept – that there is a continuum from purely private regulation towards

[17] See e.g. Tony Prosser, 'Self-Regulation, Co-Regulation and the Audio-Visual Media Services Directive', *Journal of Consumer Policy* 31 (2008): 99; Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law'; Tambini, Leonardi, and Marsden, *Codifying Cyberspace*.
[18] Marsden, 'Internet Co-Regulation and Constitutionalism', 213.
[19] Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law'.
[20] Prosser, 'Self-Regulation, Co-Regulation and the Audio-Visual Media Services Directive'.
[21] See also the discussion of terminology in Ian Bartle and Peter Vass, *Self-Regulation and the Regulatory State - a Survey of Policy and Practice* (Bath: Centre for the Study of Regulated Industries, 2005), http://www.bath.ac.uk/management/cri/pubpdf/Research_Reports/17_Bartle_Vass.pdf.

regulation characterised by a greater degree of state involvement. This continuum is sometimes simplified to focus on a single variable, as in this National Consumer Council visualisation from 2000 which focuses on the *origin* of the rules which govern conduct[22]:

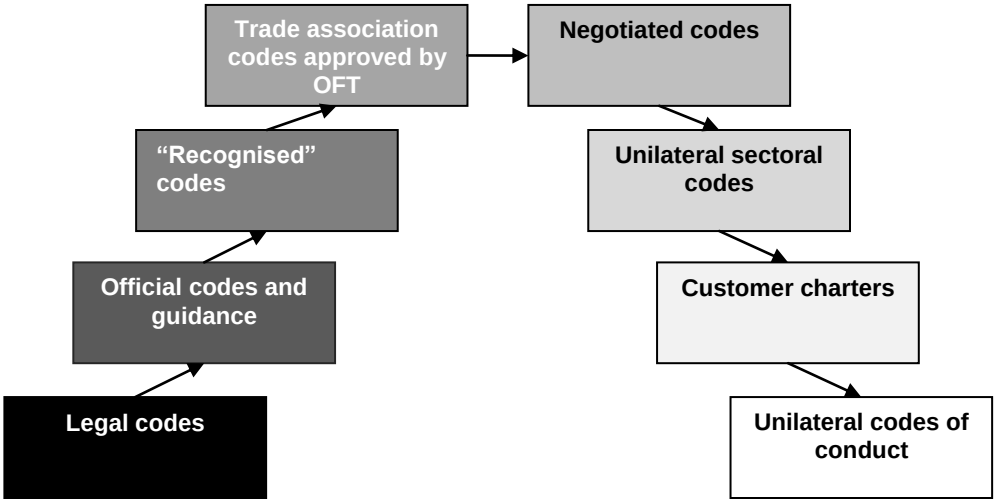

Figure 6 - National Consumer Council models of self-regulation

A more sophisticated visualisation can be found in recent work by Millwood-Hargrave and in the following diagram she illustrates the possible degrees of state involvement in relation to three variables – the *source* of the rules or "code" governing a particular sector, the *body* responsible for enforcement of those rules and the *enforcement mechanisms* which incentivise or enforce compliance[23]:

[22] National Consumer Council, *Models of Self-Regulation: An Overview of Models in Business and the Professions*, 2000, http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.
[23] Quoted in Marsden et al., *Options for and Effectiveness of Internet Self- and Co-Regulation Phase 1 Report*, 3.

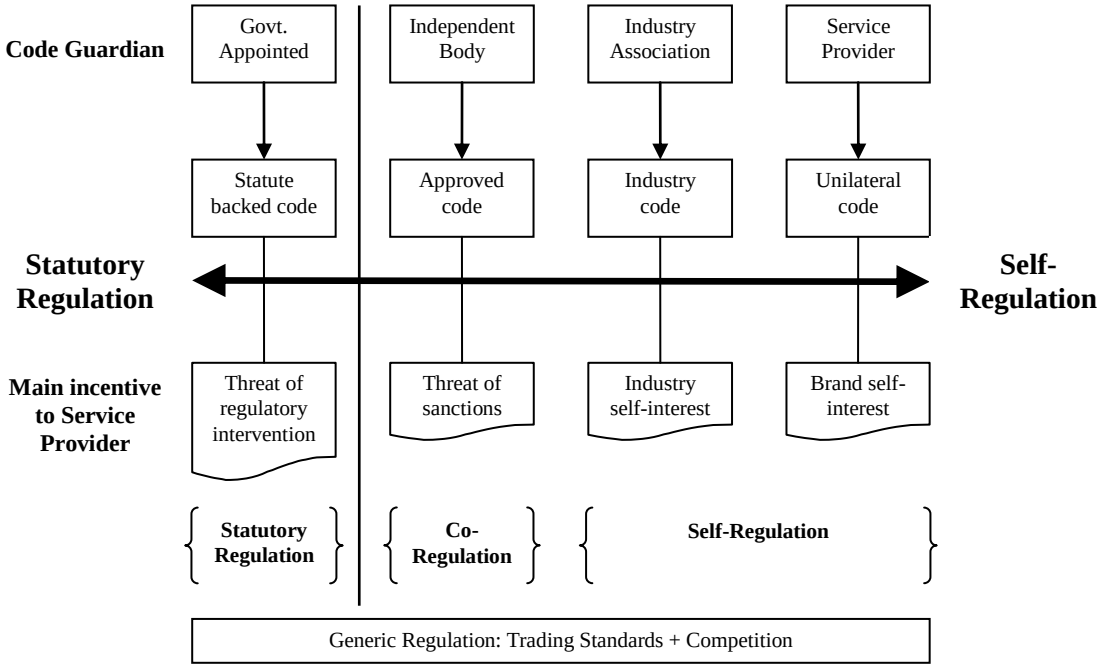

Figure 7 - Millwood-Hargrave diagram of SROs, regulatory type and incentive structure

Even this diagram, however, only begins to capture the complexity of the possible types of regulatory structures. Particularly online, there is a remarkable variety of arrangements in place. Marsden has extensively surveyed internet governance arrangements and has identified twelve types of systems on the self- and co-regulatory continuum based on the extent and nature of state involvement:[24]

[24] Marsden, 'Internet Co-Regulation and Constitutionalism', 216.

Regulatory scheme	Illustrative example	Scale	Government involvement
'Pure' unenforced self-organization	SecondLife	0	Informal interchange only – evolving partial industry forum building on players' own terms
Acknowledged self	Bebo Creative Commons	1	Discussion but no formal recognition/approval
Ex post standardized self	W3C	2	*Ex post* approval of standards
Standardized self	IETF	3	Formal approval of standards
Discussed self	IMCB	4	*Ex ante* informal consultation – but no sanction/approval/process audit
Recognized self	ISP Associations	5	Recognition of body – informal policy role
Co-founded self	FOSI	6	*Ex ante* negotiation of body; no outcome role
Sanctioned self	PEGI	7	Recognition of body – formal policy role (contact committee/process)
Approved self	IWF	8	*Ex ante* informal negotiation with government –with recognition/approval
Approved compulsory co-regulatory	ICANN	9	*Ex ante* negotiation with government –with sanction/approval/process audit
Scrutinized co-regulatory	NICAM ATVOD	10	As 9 with annual budget/process approval
Independent Body (stakeholder forum)	PhonePayPlus NOMINET	11	Government imposed and co-regulated with taxation/compulsory levy

Figure 8 - Twelve ideal types of self- and co-regulation

(iv) UK and EU definitions

It will be evident from the foregoing that there is considerable debate as to terminology: both in relation to the term self-regulation itself and also in relation to where the line between self- and co-regulation should be drawn.

Academic disagreement aside, however, the UK government has generally used these terms in a reasonably consistent way. This is exemplified by the DTI and Department for Culture, Media and Sport 2000 White Paper *A New Future for Telecommunications.*[25] That paper identified co-regulation (as distinct from self-regulation) as existing where

[25] Department for Trade and Industry and Department for Culture, Media and Sport, *A New Future for Communications* (London: HMSO, 2000).

self-regulation is accompanied by the active involvement of a governmental regulatory body to ensure that a desired regulatory objective was met – which would include situations where that body enjoyed a legislative role in setting objectives or imposing sanctions where those objectives fail to be met.

This UK governmental understanding can be found in e.g. the 2008 policy document *Identifying appropriate regulatory solutions*, where Ofcom offers the following typology of regulation:

> **No regulation:**
> Markets are able to deliver required outcomes. Citizens and consumers are empowered to take full advantage of the products and services and to avoid harm.
>
> **Self-regulation:**
> Industry collectively administers a solution to address citizen or consumer issues, or other regulatory objectives, without formal oversight from government or regulator. There are no explicit *ex ante* legal backstops in relation to rules agreed by the scheme (although general obligations may still apply to providers in this area).
>
> **Co-regulation:**
> Schemes that involve elements of self- and statutory regulation, with public authorities and industry collectively administering a solution to an identified issue. The split of responsibilities may vary, but typically government or regulators have legal backstop powers to secure desired objectives.
>
> **Statutory regulation:**
> Objectives and rules of engagement are defined by legislation, government or regulator, including the processes and specific requirements on companies, with enforcement carried out by public authorities.[26]

An example of co-regulation under this typology is the way in which Ofcom has "contracted out" aspects of the regulation of broadcast advertising to the independent and non-statutory Advertising Standards Authority (ASA) – subject, however, to a legislative "backstop" where Ofcom retains a statutory power to impose sanctions should regulation via the ASA not meet the desired standard of effectiveness.[27]

---

[26] Ofcom, 'Identifying Appropriate Regulatory Solutions: Principles for Analysing Self- and Co-Regulation', 10 December 2008, http://stakeholders.ofcom.org.uk/consultations/coregulation/.
[27] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (Oxford: Oxford University Press, 2006), chap. 11; Prosser, 'Self-Regulation, Co-Regulation and the Audio-Visual Media Services Directive', 101–102.

This meaning of co-regulation, as distinct from self-regulation, focuses on the existence of some statutory involvement, usually in the form of a backstop or residual power to intervene on the part of state authorities to ensure that certain aims are achieved. As such it echoes the predominant approach at European level where self-regulation has been defined in the 2003 *Interinstitutional Agreement on Better Law-Making* as:

> the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt *amongst themselves and for themselves* common guidelines at European level (particularly codes of practice or sectoral agreements) [emphasis added].[28]

While co-regulation is defined as requiring some *legislative* intervention, being:

> the mechanism whereby a Community *legislative act* entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations) [emphasis added].[29]

These understandings of self- and co-regulation, though they remain open to criticism, provide a workable approach for the assessment of domestic practice and will be used throughout this chapter.[30]

(v) Situating Cleanfeed on the self-/co-regulatory continuum

Given these definitions, where should we place the Cleanfeed system on the continuum from state regulation to self-regulation? Is it best described as being an example of self- or co-regulation? The IWF generally labels itself as a "self-regulatory" body though it goes on to describe a close partnership with state authorities:

---

[28] European Parliament, Council and Commission, 'Interinstitutional Agreement on Better Law-Making'[2003] OJ C321/1.

[29] This agreement and these definitions are discussed in detail in Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law'.

[30] For analysis of the European definitions of co-regulation see in particular Eva Lievens, Jos Dumortier, and Patrick S. Ryan, 'The Co-Protection of Minors in New Media: A European Approach to Co-Regulation', *UC Davis Journal of Juvenile Law & Policy* 10 (2006): 97.

> We operate independently of Government, but are closely supported by the Home Office, the Department for Business, Innovation and Skills (BIS) and the Ministry of Justice as well as working with the Department for Education and the Department for Culture, Media and Sport (DCMS) and a number of Parliamentarians, Peers and MEPs who take an interest in our work.[31]

It is unlikely, however, that the IWF has any clear or consistent view as to what it means by this term, particularly as in some cases it has gone further and described itself as operating in a co-regulatory way. For example, in evidence to the Select Committee on European Union in 2000 and again in evidence to the Byron Review in 2007 it described its activities as "co-regulation", working in cooperation with industry and law enforcement.[32] In addition, its understanding of itself as a public body for the purposes of the Human Rights Act suggests an unresolved internal uncertainty as to its nature.[33]

Of course, the label which the IWF chooses for itself is not conclusive, and some have argued that the extensive involvement of government in its activities (particularly when we consider the possibility of appeal against IWF decisions to the police) means that it should be regarded as co-regulatory.[34] Marsden in particular has identified a shift in the nature of the IWF from its formation, which he describes as a "deliberate and quite transparent change... from a self-regulatory ISP-based body to a more co-regulatory police cooperation body".[35]

However, when we separate out the Cleanfeed system from the IWF generally, it becomes impossible to describe the system as co-regulatory using our narrower definitions of co-regulation as requiring some "legislative act" (the Interinstitutional Agreement) or some "legislative backstop" (the Ofcom schema). The IWF's role in advising ISPs to take down material they host might be regarded as co-regulation under

[31] There is a useful discussion in Laidlaw, 'The Responsibilities of Free Speech Regulators', 13–15.
[32] Internet Watch Foundation, 'Written Evidence to the Select Committee on European Union', 20 February 2000, http://www.publications.parliament.uk/pa/ld199900/ldselect/ldeucom/95/95we35.htm; Internet Watch Foundation, 'IWF Response to the Byron Review', 2007, http://www.iwf.org.uk/accountability/consultations/byron-review-2007.
[33] See Akdeniz, *Internet Child Pornography and the Law*, 264.
[34] See e.g. Sommer, 'Re: Cleanfeed and Wikipedia', 9 December 2008.
[35] Marsden, *Internet Co-Regulation*, 177.

the Ofcom analysis insofar as there is a legislative backstop in place, as ISPs may be prosecuted should they ignore reports of child pornography reported to them by the IWF. In the case of blocking, however, there is neither a legislative basis for blocking, nor any backstop in the form of legal consequences for ISPs who choose not to block, and consequently the blocking scheme could not be called co-regulation.

This result might seem counterintuitive, given the extensive links between the state and the IWF in relation to blocking, but highlights one advantage of the narrower definitions of co-regulation – by demanding a legislative basis before a system can be described as co-regulatory these definitions place the focus on issues of legitimacy and parliamentary oversight and deny the rhetorical advantage of "co-regulation" to those systems which rely on informal and therefore unenforceable links with the state.

3. The lure of self-regulation

(i) A presumptive starting point

Self-regulation has become increasingly pervasive as a form of internet governance, to the point where Koops *et al.* have concluded that it has become the presumptive starting point.[36] From the late 1990s onwards governments have adopted policies which favour self-regulation where possible.[37] Indeed, in 2002 the Vatican went so far as to say that "[r]egulation of the Internet is desirable, and in principle industry self-regulation is best".[38]

In the United Kingdom, this approach was most notably set out in the 2001 e-Policy Principles, issued by the Cabinet Office's "e-Envoy", which established eight principles

[36] Koops et al., 'Should Self-Regulation Be the Starting Point?'.
[37] See e.g. Price and Verhulst, *Self-Regulation and the Internet*; Tambini, Leonardi, and Marsden, *Codifying Cyberspace*.
[38] Pontifical Council for Social Communications, 'Ethics in Internet', 22 February 2002, http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_en.html.

intended to guide policy makers throughout central government.[39] The third of these established a general presumption in favour of self-regulation, on the basis that this "generally provide[s] a more rapid and flexible means of responding to changing market needs, and achieving international consensus, than is possible through legislation". The e-Policy Principles explicitly cited the IWF in making this recommendation – by 2001 the IWF had already become, in the official mind, an example of best practice.

This recommendation was, however, nothing new in the UK context. As we have already seen in chapter 3, from the early days of the internet the government had pursued a consistent policy of "legislative forbearance" in relation to internet content – i.e. a reluctance to legislate in a way which would create a new regulatory regime – instead preferring to promote self-regulatory solutions.[40] This policy – a deliberately "light touch"[41] on the part of the state – had been frequently articulated and applied even before the e-Policy Principles were adopted.

At the outset, as the establishment of the IWF shows, government policy towards internet content was very different from existing policy towards traditional audio-visual (broadcast, film or video) content. Traditional audio-visual content was generally regulated in detail by sector-specific legislation.[42] In the case of the internet, however, a preference was expressly stated for "voluntary" industry regulation over statutory intervention, and for application of the general law rather than sector-specific rules.[43]

---

[39] Office of the e-Envoy, 'E-Policy Principles: A Policymakers Guide to the Internet', December 2001, http://tna.europarchive.org/20050311005439/http://www.cabinetoffice.gov.uk/regulation/ria-guidance/documents/pdf/epolicy.pdf.

[40] It should be noted that the treatment of content differs from other aspects of cyberspace which have not always benefited from similar light touch regulation. The regulation of encryption in the UK, for example, has been marked by the adoption of legislation – in the form of Part III of the Regulation of Investigatory Powers Act 2000 – which has been characterised as undermining civil rights, highly intrusive and damaging to online businesses. See e.g. Walden, *Computer Crimes and Digital Investigations*, 282–295.

[41] Douglas Vick, 'Regulatory Convergence?', *Legal Studies* 26, no. 1 (2006): 26.

[42] In respect of which see e.g. Geoffrey Robertson and Andrew Nicol, *Media Law*, 4th ed. (London: Penguin, 2002), chap. 15 and 16.

[43] For explicit statements of this policy see e.g. House of Commons, Select Committee on Culture, Media and Sport, *The Multi-Media Revolution* (London: HMSO, 1998), 106.; DTI, 'DTI Press Release P/96/636'.

In 2000, for example, the White Paper *A New Future for Telecommunications* recognised that the proposed super-regulator Ofcom might have a role to play in relation to internet content, but rejected the suggestion that it should be given statutory powers comparable to those which it would enjoy in respect of content on the broadcast media, stating:

> OFCOM should ensure continuing and effective mechanisms for tackling illegal material on the Internet, such as those being pursued under the auspices of the Internet Watch Foundation. It will also promote rating and filtering systems that help Internet users control the content they and their children will see… [I]t is important that there are effective ways of tackling illegal material on the Internet and that users are aware of the tools available, such as rating and filtering systems, that help them control what they and their children will see on the Internet. Research suggests that this is what people want in relation to the Internet, rather than third party regulation.[44]

This model was adopted in the Communications Act 2003, which was carefully drafted to ensure that regulation of internet content was not brought within Ofcom's scope.[45]

This national approach has also been paralleled at EU level where, since 1996, there has been a strong preference towards self-regulation in relation to online content generally and child pornography in particular.[46] Consequently the series of Safer Internet Programmes adopted from 1999 onwards have focused on self-regulation – and indeed have provided significant funding to the IWF as well as other national self-regulatory bodies.[47]

---

[44] Department for Trade and Industry and Department for Culture, Media and Sport, *A New Future for Communications*, para. 6.34–6.10.1.
[45] Richard Collins, 'Networks, Markets and Hierarchies: Governance and Regulation of the UK Internet', *Parliamentary Affairs* 59, no. 2 (1 April 2006): 319.
[46] Cooke, 'Controlling the Net'; McIntyre, 'Blocking Child Pornography on the Internet'.
[47] The IWF was successful in receiving European funding from the very outset. See e.g. Internet Watch Foundation, '2000 Annual Report'.

(ii) Practicability

Why did self-regulation achieve such prominence, both in the UK and internationally, as a favoured regulatory tool? When we assess the cyber-libertarian/cyber-paternalist debate outlined in Chapter 4 we see that two linked objections were made to state regulation of the internet – that it was both impracticable and illegitimate. On the face of it, the use of self-regulation appeared to address both dimensions of that debate by apparently providing a method of regulation which was both effective and was legitimated by the involvement and consent of those governed. In this section we will first consider the practicability claim.

To begin, it might be helpful to look more closely at the e-Policy principles document as this provides us with a typical governmental perspective as to the benefits of self-regulation.[48] In its references to actors "closest to the market" enabling "rapid and flexible means of responding to changing market needs" and "achieving international consensus" we see the key pragmatic arguments in favour of self-regulation: that it captures the expertise of industry participants, that it enables regulation which is more responsive to changing conditions and technologies, and that it enables norms to be drawn up and enforced on an international basis, not merely limited to a particular jurisdiction. These points do, however, need to be examined more closely.

(a) Flexibility

At the heart of almost every argument in favour of self-regulation is the argument that it enables faster and more responsive regulation.[49] At its crudest, this tends to rely on the argument that the pace of change online has outrun the conventional lawmaking process – if regulation is to keep up, so the argument goes, then non-statutory measures must be

[48] Office of the e-Envoy, 'E-Policy Principles: A Policymakers Guide to the Internet'.
[49] See e.g. International Telecommunication Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, 42, http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/policy_makers/policy_makers.pdf.

taken. This is not, however, an argument which is new in the context of the internet – Baldwin and Cave, for example, identify it as one of the arguments behind self-regulation generally – and in more nuanced versions of this argument it is often claimed that self-regulation allows for changes in conditions to be responded to by means of incremental and evolutionary change rather than the intermittent step changes which are associated with legislative intervention.[50] The comments of Darlington, a former chair of the IWF, are typical of many in the UK industry:

> My personal position is totally opposed to all forms of state blocking of generic categories of material on the Internet. I am most uncomfortable with the use of a constitution or statute to regulate such a fast-moving and complex medium as the Internet. My strong preference is for co-regulation by industry bodies with government support...[51]

A further variant of this argument notes that self-regulation tends to focus on outcomes rather than particular processes, thus providing participants with flexibility to choose the most effective means available to achieve the mandated goals. In an environmental law context, for example, Sinclair has noted that historically command and control regulation has often been overly prescriptive and inflexible regarding particular technical systems with the result that "regulators may have inadvertently prevented the development of more effective technological solutions".[52] By comparison, self-regulatory solutions may leave provide participants with greater choice as to how to solve a particular problem, thus promoting more innovative responses. This flexibility can be seen in the context of the IWF URL list itself where, as we have seen, industry participation has led to steady incremental development: from an internal database for IWF use only, to use for site blocking by ISPs, to use in parental and school filtering software and, more recently, to filtering of search results by companies such as Google.[53]

---

[50] Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy and Practice* (Oxford: Oxford University Press, 1999), 127.
[51] Roger Darlington, 'Should the Internet Be Regulated?', 25 February 2010, http://www.rogerdarlington.me.uk/regulation.html.
[52] Sinclair, 'Self-Regulation versus Command and Control?', 539.
[53] Internet Watch Foundation, 'IWF URL List Recipients'; Committee on Energy and Commerce, *Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites.*

(b) Specialist knowledge

Closely related to the flexibility argument is one based on specialist knowledge – that self-regulation harnesses industry expertise and therefore addresses the objection that governments lacked the knowledge necessary to regulate the internet. This argument is common throughout self-regulation generally, usually coupled with the argument that the skill set necessary to regulate a particular industry cannot simply be "bought in" but must be based on continued direct involvement with the sector.[54] This argument has particular weight in the case of the IWF where its position at the intersection of industry, child protection and law enforcement has led to internationally recognised expertise in relation to child abuse material and matters such as hosting, payment services and even commercial brands of abuse material.[55]

(c) Internalisation of objectives

By encouraging industry to participate in the drawing up of standards self-regulation has also been said to cause industry to internalise the values being promoted, encouraging voluntary compliance and thereby reducing the need for enforcement.[56] As compared with legislation, the argument runs, self-regulation is more likely to cause industry to feel a sense of ownership of rules and to implement them with an enthusiasm which goes beyond mere grudging compliance.[57] This point was accepted by the All Party Parliamentary Communications Group in relation to the IWF and in October 2009 it concluded that compulsory blocking against the IWF URL list should be avoided lest future industry cooperation be jeopardised.[58]

---

[54] Baldwin and Cave, *Understanding Regulation*, 127.
[55] See e.g. Internet Watch Foundation, '2010 Annual Report', 8–9.
[56] See e.g. Sinclair, 'Self-Regulation versus Command and Control?', 545.
[57] Compare Baldwin and Cave, *Understanding Regulation*, 126–127.
[58] All Party Parliamentary Communications Group, *Can We Keep Our Hands off the Net? Report of an Inquiry by the All Party Parliamentary Communications Group*, para. 55.

(d) Cost reduction

A central part of the appeal of self-regulation is the perception that it can result in lower costs for both the state and industry participants. In the case of the state, self-regulation offers the possibility of outsourcing the costs associated with the generation and enforcement of norms. These can be significant, particularly when we consider not merely the direct financial costs of information gathering, rule creation and enforcement but also the intangible costs in e.g. parliamentary time and political capital. This has, unsurprisingly, encouraged governments to prioritise self-regulation.[59]

In the same way, industry has also generally welcomed self-regulatory initiatives on cost grounds, notwithstanding the way in which it can shift costs from the state. In part this will be because the industry itself is better placed to engage in information gathering and rule formation and can do so at lower cost than the state. More generally, however, the cost/benefit analysis will often be seen to favour self-regulation as offering a light touch regulatory regime which might serve to ward off more intrusive and costly legislative intervention – an industry sponsored body will naturally devise rules which it sees as workable, in a way which legislators might not.[60]

(e) Uniform international outcomes

One of the key cyber-libertarian arguments was that national regulations could easily be avoided by jurisdictional or regulatory arbitrage: that is, by users simply moving to services and sites based beyond the reach of particular national laws. This mobility, it was argued, meant that attempts to control internet content would require difficult and coordinated international action at state level, thus hindering enforcement efforts, or else would require states to block access to foreign sites.[61]

---

[59] Koops et al., 'Should Self-Regulation Be the Starting Point?', 124.
[60] Ibid., 109.
[61] Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power', *Modern Law Review* 65, no. 4 (2002): 494–495.

By contrast, as self-regulation can be adopted on an international basis it appears to have substantial practical advantages over legislation: it can achieve comparable outcomes between nations with very different legal systems, minimising the possibilities for jurisdictional arbitrage without the need for time consuming and politically difficult harmonisation of laws, and reducing the perceived need for the use of geolocation, blocking or other technologies which may segment the internet along national lines.[62]

This argument is less important in the context of CAI, where substantial international harmonisation has already taken place. Nevertheless, it is interesting to note that the IWF URL list has (without any apparent conscious design on the part of the IWF) already achieved substantial international take up in a way which confirms the validity of this point. Among the international users of the list are mobile providers who use the IWF list in jurisdictions where there is no domestic blocking list, search engines such as Google, and home and school filtering software.[63] Consequently, even though the URL list was devised and is administered with UK law in mind, in practice it has become a remarkably pervasive international standard.

(iii) Legitimacy

(a) Consent of the governed

Turning from practicability to legitimacy, self-regulation seemed (at least in part) to answer the arguments of those who claimed that cyberspace was properly a separate place beyond the legitimate control of any government.[64] Self-regulation – though it might be promoted by governments – allowed for the possibility of governance by

[62] These perceived benefits are discussed extensively in Koops et al., 'Should Self-Regulation Be the Starting Point?'.
[63] GSMA Mobile Alliance Against Child Sexual Abuse Content, 'Implementation of Filtering'; Internet Watch Foundation, 'IWF URL List Recipients'.
[64] Barlow, 'A Declaration of the Independence of Cyberspace'.

internet actors themselves in a way which appeared to meet Barlow's promise that "[w]here there are real conflicts, where there are wrongs, we will identify them and address them by our means". In doing so, it also appeared to offer an inbuilt safeguard by allowing users the ability to vote with their feet – by moving to a different online community – in the event that they disagreed with particular developments.[65]

Can this point be made in relation to the Cleanfeed system, given the government pressure on ISPs to deploy the system or face legislative intervention? The argument might be made that notwithstanding government pressure it is still voluntary, as demonstrated by the few, smaller ISPs who have yet to deploy the technology. Consequently some would say that as with other forms of self-regulation the system is legitimated by the consent of those who participate in it – and that it is more desirable than legislative intervention for those who mistrust the role of the state in controlling speech.[66] This reflects arguments commonly made in the context of other bodies such as the Press Complaints Commission – that by serving as a buffer against direct state regulation they preserve rather than undermine freedom of expression.[67]

(b) Decoupling governance from individual jurisdictions

As we have already discussed, online self-regulation decoupled governance from national legislation, and allowed new regulatory systems to develop on an international basis. As such it arguably had a legitimating as well as a practical effect. It appeared to minimise (at least in part) the conflict of laws and legislative overspill arguments which were so convincing to early authors such as Johnson and Post.[68] In principle, at least, in a self-regulatory system the issue of conflicting obligations may be less likely to arise and similar results can be achieved internationally notwithstanding the laws of different

[65] See e.g. Mueller, *Networks and States*.
[66] Ozimek leans in this direction, arguing that the IWF approach is less threatening than that adopted elsewhere: John Ozimek, 'A Censorship Model', *The Guardian*, 2 August 2009, http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/02/internet-censor.
[67] See e.g. Tambini, Leonardi, and Marsden, *Codifying Cyberspace*, chap. 11.
[68] Johnson and Post, 'Law and Borders - The Rise of Law in Cyberspace'.

countries. Likewise, if a self-regulatory system is not founded in national law then it is less vulnerable to the cyber-libertarian complaint that online regulation involves states in improperly extending their reach beyond national territory.

(iv) Resistance to function creep

A common libertarian view is that self-regulatory forms of content regulation are preferable as restricting the ability of states to add new categories of content to be censored. Mueller, for example, has identified the "saving grace of privatised governance" as the "ability of users and suppliers to vote with their feet", suggesting that if blocking is put on a statutory basis it is likely to become more rather than less pervasive. Instead, he argues, voluntary utilisation decisions can establish effective accountability for bodies engaged in blocking, giving blacklists created by anti-spam activists as an example.[69] From a different perspective Zittrain and Palfrey nevertheless reach a similar conclusion when they argue that collective self-regulation enables the industry to present a united front to excessive state demands, limiting the ability of governments to pick off individual firms one by one.[70]

The question of function creep was already considered in chapter 4, where we noted that predictions of function creep have only partially been borne out in the case of the Cleanfeed filtering system. Despite frequent kite-flying by politicians who propose expanding the system, the URL list itself remains limited to its original purpose. In chapter 4 we identified one reason for this as being the self-regulatory nature of the system, which has led to three distinct constraints on any expansion of the remit of the system: IWF fears of reputational damage, industry resistance to funding any expansion and, significantly, fears on the part of children's groups that any expansion would undermine child protection. This has been the case from quite early on in the history of

[69] Mueller, *Networks and States*, 213–214.
[70] Jonathan Zittrain and John Palfrey, 'Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet', in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J Deibert et al. (Cambridge, Mass: MIT Press, 2008), 122.

the IWF – for example, during the 1998 review of the structure of the IWF Childnet was very clear in its submission that:

> IWF's terms of reference should maintain an absolute priority on protecting children. Specifically they should not be extended to include civil matters. IWF should only take responsibility for any other illegal content or activity if there is a specific additional budget sufficient for the extra staff resources required.[71]

For these reasons, it seems fair to say that in this case self-regulation has in fact resulted in function creep being avoided for the reasons which Mueller and Zittrain and Palfrey have identified. This is a view echoed by Edwards, who has argued that more generally:

> by mediating, and providing a central hotline for, complaints about internet content, the IWF effectively protects ISPs from having to deal with complaints from the public about pornography and hate speech... as part of daily business, and from being distracted by frivolous or unfounded ones. In this context, the IWF might well actually act in defence of free speech, since the IWF will (one hopes) have the sense and experience to throw out complaints about entirely legal Internet images or content, where a small ISP, lacking legal advice and as best-practice risk management, might simply give in and remove the item in question.[72]

4. Criticisms of self-regulation

These claims in favour of self-regulation have not, however, gone unchallenged and internet self-regulation of content brings to the fore concerns regarding accountability and the blurring of the public/private divide. Particularly from the mid-1980s onwards, UK public lawyers have paid special attention to these issues which Page summarised in 1986 as having three aspects:

> First, there is the idea that these authorities, or some of them at least, wield significant powers which may be abused to the detriment of their own members, third parties or the public at large: they may be exploited, or their interests may be otherwise insufficiently taken into account...
>
> Secondly, there is the recognition, documented more fully below, that government has resorted to self-regulation on an increasing scale as an alternative to direct regulation by itself. This recognition engenders a number of reactions. The first, and perhaps most important, is that resort to self-regulation somehow involves government in sliding out from what properly ought to be its

[71] Nigel William, 'Review of the Internet Watch Foundation: Submission from Childnet International to the Review Team', October 1998, para. 5.1, http://www.childnet-int.org/downloads/iwf.pdf.
[72] Edwards, 'Pornography, Censorship and the Internet', 656.

> own responsibilities, responsibilities which cannot be discharged effectively by anyone else... The increasing resort on the part of government to self-regulation gives rise to two other fears. First, because its role as sponsor of self-regulation may conflict with its role as guardian of the public interest, the fear that self-regulation may be subject to less external supervision and control than it ought to be; secondly, the contradictory fear, that resort to self-regulation may mean that government is able to deny responsibility for the control which it may in fact exercise...
>
> The final idea to be distinguished is that some associations, quite apart from their relationship with government, exercise governmental functions and should therefore, like government itself, be accountable in respect of them. [73]

Some of these points have been answered, at least in part, by the widening scope of judicial review following the decision in *R. v. Panel on Takeovers and Mergers, ex p. Datafin*[74] which established the potential reviewability of bodies with no "visible means of legal support" and the extent to which the IWF may be subject to judicial review or other public law remedies will be considered in chapter 6. In this section the wider issues presented by self-regulation will be addressed.

(i) Who is the "self" in self-regulation?

The most fundamental criticism of self-regulation is that it may not involve genuine self-governance, but merely a different form of hierarchical regulation in which third parties find their activities controlled by industry actors. Despite this, however, analysis of self-regulation has tended to focus on the business sector alone, neglecting the role (if any) played by the individual user.[75]

This criticism is not unique to the online environment, but is especially significant in that context given the freedom of expression and privacy issues at stake. Consequently, one might ask whether internet content regulation in the UK should properly be termed "self" regulation at all, characterised as it is by intermediaries such as ISPs regulating what users can publish or access, with limited input from users themselves whether

[73] Alan C. Page, 'Self-Regulation: The Constitutional Dimension', *Modern Law Review* 49 (1986): 143–144.
[74] [1987] 2 WLR 699.
[75] Price and Verhulst, *Self-Regulation and the Internet*, chap. 2.

collectively or individually. Cleanfeed therefore triggers the legitimacy concerns identified by Ogus[76] who notes that:

> The capacity of [*a self regulatory authority*] to make rules governing the activities of an association or profession may itself constitute an abuse if it lacks democratic legitimacy in relation to members of the association or profession. The potential for abuse becomes intolerable if, and to the extent that, the rules affect third parties.[77]

In expressing this concern, Ogus is typical of a wider set of theorists in the mid 1990s who observed with some trepidation the growth of self-regulation in the UK and argued that a shifting of power from the state was taking place in an environment of limited controls on self-regulatory bodies. This was perhaps best articulated by Black who argued for the need to "constitutionalise" self-regulation, ensuring respect for public law values in the private enforcement of power.[78]

(a) Consent from users?

We have already noted the argument that self-regulation can be legitimated by the consent of the participants. In the internet context, however, there is a crucial difference from other self-regulatory systems: here, the speech being regulated is not just that of the ISPs themselves but also that of their users and third parties. Consequently, we cannot simply rely on the consent of the ISP, but must also examine whether those most directly affected – the users – also consent.

In principle, one might say that consent is possible through market mechanisms – as where users have a choice between competing providers where some operate filters and some do not. But it is not possible to say that there is any real consent on the part of UK internet users when the system lacks the transparency which would make consent

[76] Ogus, 'Rethinking Self-Regulation', 98–99.
[77] See also the observations in Peter Grabosky, 'Using Non-Governmental Resources to Foster Regulatory Compliance', *Governance* 8, no. 4 (1995): 527.
[78] Black, 'Constitutionalising Self Regulation'. It should also be noted that Black identified a need to preserve the rightful autonomy of non-state bodies, arguing that too much intervention by public law may also be harmful to wider social values.

possible. In particular, we have seen that Ofcom does not require that the use of Cleanfeed be revealed by ISPs[79] and that it is only since 2010 that the IWF has published a list of members which use the URL list.[80] Even now, however, there is still no guarantee of transparency as to *how* a particular member may be using the list – for example, whether it is blocking at the URL level or merely using a crude DNS or IP blocking approach – and consequently users are not in a position to make an informed choice between ISPs.

In any event, given that the overwhelming majority of UK ISPs use the Cleanfeed system, even those users who might be aware of the system and which ISPs participate in it may have no choice but to use those ISPs regardless. The theoretical possibility of choice is unrealistic when the user is faced with both an opaque system and an almost entirely homogenous market.[81]

(b) User and civil rights representation in the Cleanfeed system?

It might also be argued that self-regulatory schemes could be legitimated with regard to users in a different way – by ensuring greater representation in the bodies responsible for drawing up and enforcing rules. Indeed many of the earlier approaches to internet governance assumed that this would be the norm. An example is the 2001 Council of Europe *Recommendation on Self-Regulation Concerning Cyber Content.*[82] This document did not see self-regulation as a threat to fundamental rights, but rather as primarily protective of fundamental rights by safeguarding users against illegal and harmful content. Consequently, it recommended that:

[79] Chapter 2, section 5(iv).
[80] Internet Watch Foundation, '2010 Annual Report'.
[81] Compare Kreimer, 'Censorship by Proxy', 35–36.
[82] Committee of Ministers of the Council of Europe, 'Recommendation Rec(2001)8 on Self-Regulation Concerning Cyber Content (self-Regulation and User Protection against Illegal or Harmful Content on New Communications and Information Services)', 5 September 2001, https://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2001)8.

> 1. Member states should encourage the establishment of organisations which are representative of Internet actors, for example Internet service providers, content providers and users.
>
> 2. Member states should encourage such organisations to establish regulatory mechanisms within their remit, in particular with regard to the establishment of codes of conduct and the monitoring of compliance with these codes.
>
> 3. Member states should encourage those organisations in the media field with self-regulatory standards to apply them, as far as possible, to the new communications and information services.
>
> 4. Member states should encourage such organisations to participate in relevant legislative processes, for instance through consultations, hearings and expert opinions, and in the implementation of relevant norms, in particular by monitoring compliance with these norms.
>
> 5. Member states should encourage Europe-wide and international co-operation between such organisations.

Notably absent from these recommendations were any measures to safeguard against abuses of power by self-regulatory organisations themselves, which seem to have been overlooked. By contrast, later recommendations of the Council of Europe have paid significantly more attention to this point.[83]

The reference in the recommendations to "organisations which are representative of Internet actors" including "content providers" and "users" is important in a UK context, where self-regulation in the guise of the IWF has developed in an entirely different manner so that the involvement of users is essentially limited to the function of reporting illegal content via the hotline function.[84] While the precise governance of the IWF has varied over time, its core structure has in substance remained the same since 2000 and involves governance by a board of ten comprising an independent chair, six independent

[83] Most recently, see the 2012 recommendation on search engines which cautions that 'Member States should work with search engine providers so that they ensure that any necessary filtering or blocking is transparent to the user. The blocking of all search results for certain keywords should not be included or promoted in self- and co-regulatory frameworks for search engines. Self- and co-regulatory regimes should not hinder individuals' freedom of expression and right to seek, receive and impart information, ideas and content through any media. As regards the content that has been defined in a democratic process as harmful for certain categories of users, Member States should avoid general de-indexation which renders such content inaccessible to other categories of users. In many cases, encouraging search engines to offer adequate voluntary individual filter mechanisms may suffice to protect those groups". Committee of Ministers of the Council of Europe, 'Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines', 4 April 2002, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)3.

[84] On this, see Internet Watch Foundation, 'The Hotline and the Law', 10 December 2007, http://www.iwf.org.uk/public/page.31.htm.

trustees and three industry trustees. The industry trustees are in turn elected by the Funding Council, comprising all industry members who fund the IWF.[85] Examining this structure against the recommendations of the Council of Europe reveals a significant gap: within the IWF there is no provision for representation of users as such.[86] Instead, the role of the IWF and its industry roots suggest that internet content regulation is viewed as a matter to be negotiated between business and children's groups rather than as something which affects all citizens.[87]

In addition, while the independent trustees come from a range of backgrounds there is no current trustee representing user or civil liberties interests[88] and only one past board member – Malcolm Hutty[89] – could be described as fitting this category.[90] It is also striking that it was during the brief tenure of Malcolm Hutty that many of the fundamental rights safeguards were adopted – for example, the commitment of the IWF to be treated as a public body.[91] It is deeply undesirable that user rights should be left to be represented in this essentially *ad hoc* way.[92] This is particularly so given that (at the time of writing) three of the five independent members have a policing or prosecution

[85] Internet Watch Foundation, 'IWF Governance', *Internet Watch Foundation*, 14 December 2009, http://www.iwf.org.uk/public/page.103.550.htm.
[86] There is also a gap as regards content providers, though a lesser one as a small number of content creators such as the BBC are members of the IWF and thus enjoy input through the Funding Council.
[87] Beattie has made a similar point in respect of Australian internet regulation: "At present the Internet Industry Association (IIA) has adopted the 'professional body' role for pragmatic reasons, but this may eventually lead to the IIA emerging as a state sanctioned authority similar to a law society or medical association, simply because it is easier to replicate these existing organisational roles than it is to develop new ones. Inevitably, this also contributes to the assumption that the Internet is primarily a business interest and the matter of Internet regulation is one of constraining businesses rather than private communications. This is in keeping with Government policy presuming communications to be fundamentally concerned with commerce." Scott Beattie, *Community, Space and Online Censorship: Regulating Pornotopia* (Farnham: Ashgate, 2009), 54.
[88] For details of the current board members see Internet Watch Foundation, 'Internet Watch Foundation Trustees', accessed 8 December 2013, http://www.iwf.org.uk/accountability/governance/board-biographies.
[89] In the early days of the IWF Malcolm Hutty joined as a civil liberties representative. See the comments at footnotes 54 and 58 in Heins, *Not in Front of the Children*, 347–348.
[90] Although it should be said that Mark Stephens - a prominent civil liberties solicitor - was nominated to the IWF by Liberty but not as its representative. See ibid., 214–216.
[91] Internet Watch Foundation, 'Board Minutes 25 April 2001'.
[92] Akdeniz has made this point as far back as 1997: Yaman Akdeniz, 'Internet Content Regulation: UK Government and the Control of Internet Content', *Computer Law & Security Report* 17, no. 5 (30 September 2001): 303.

background, making it difficult to describe them as truly independent of the state and their former colleagues.[93]

Granted, the amorphous nature of internet use means that it may be difficult to identify user representatives – and the near universal use of the internet means that user interests might be viewed as aligned with those of the wider population. Nevertheless, it is striking that there is no formal representation within the IWF for e.g. the Open Rights Group as an organisation dedicated to fundamental rights issues in an online context. There are undoubtedly competing interests and conflicting rights at stake in relation to decisions being made by the IWF and these do not appear to be adequately represented at board level. While industry members may share many of the interests of users generally, experience has shown that there are areas (such as transparency in blocking) where they are diametrically opposed.

(ii) Removing regulation from public law scrutiny

Another core criticism is that self-regulatory systems may enable governments to establish systems for controlling speech which (by operating through private law) evade the constitutional constraints and judicial scrutiny which would limit state action.[94] These criticisms are especially strong in relation to what Mifsud Bonnici terms

[93] Catherine Crawford is a former Chief Executive of the Metropolitan Police Authority; Philip Geering is a former Director of Policy at the CPS and Director at the Independent Police Complaints Commission; Peter Neyroud was formerly Chief Constable of Thames Valley and Chief Executive of the National Policing Improvement Agency. See Internet Watch Foundation, 'Catherine Crawford OBE', accessed 8 December 2013, https://www.iwf.org.uk/accountability/governance/board-biographies/catherine-crawford; Internet Watch Foundation, 'Philip Geering', accessed 8 December 2013, https://www.iwf.org.uk/accountability/governance/board-biographies/philip-geering; Internet Watch Foundation, 'Peter Neyroud CBE, QPM', accessed 8 December 2013, https://www.iwf.org.uk/accountability/governance/board-biographies/peter-neyroud-cbe-qpm.

[94] Birnhack and Elkin-Koren, 'The Invisible Handshake'; Angela Daly, 'Private Power and New Media: The Case of the Corporate Suppression of WikiLeaks and Its Implications for the Exercise of Fundamental Rights on the Internet', in *Human Rights and Risks in the Digital Era*, ed. Christina M. Akrivopoulou and Nicolaos Garipidis (IGI Global, 2012).

"mandated" or "coerced" self-regulation – that is, systems adopted and applied in response to government pressure but without any legislative underpinning.[95]

Lambers, for example, describes this as "tilting" where the "classical vertical state-citizen relationship on which... freedom of speech is founded, is short circuited since a second private party shifts between the state and the user: the ISP". He graphically represents this "tilt" as follows:

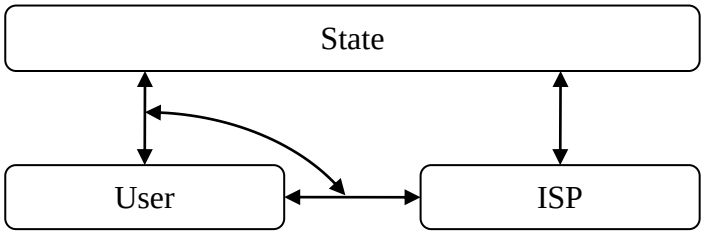

Figure 9 - Lambers' model of "tilting" legal relationships

Consequently, he argues, the relationship between state and citizen becomes instead a relationship between ISP and user – one which is governed by private law only, to the exclusion of constitutional rights to freedom of expression.[96]

A particularly good illustration of his argument comes from the Dutch system, adopted in 2007, which involved ISPs voluntarily blocking access to domains designated by the police, using DNS blocking. A study commissioned by the government found that this was unlawful and contrary to Article 10 ECHR in that it lacked any specific legal basis – ultimately forcing it to be abandoned.[97] Remarkably, however, the response of the Dutch government was not to provide a legal basis, but instead to try to further privatise

[95] Mifsud Bonnici, *Self-Regulation in Cyberspace*.
[96] Lambers, 'Code and Speech'.
[97] Stol et al., 'Governmental Filtering of Websites'; Wouter Stol et al., 'Filtering Child Pornography on the Intenet: An Investigation of National and International Techniques and Regulations' (CyREN – Cybersafety Research and Education Network, 26 May 2008), http://www.wodc.nl/onderzoeksdatabase/internetfilters-tegen-kinderporno.aspx?cp=44&cs=6780.

blocking. The tactic adopted was to seek to persuade ISPs to develop a purely self-regulatory scheme – in which the sites to be blocked would be designated by a private body rather than by the police – thus deliberately avoiding the safeguards which would apply to a state run system.[98]

Is this criticism valid in relation to Cleanfeed? The IWF is conscious of these concerns and despite its nominally private status, it 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.[99] 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. This argument would rely on the well developed line of caselaw to the effect that certain formally private bodies will nevertheless be subject to judicial review where they carry out a public law function – a principle which has been applied to self-regulatory schemes which affect third parties.[100] It would also be reinforced by the separate but largely parallel provisions of the Human Rights Act 1998, which in section 6(3)(b) imposes obligations on "any person certain of whose functions are functions of a public nature".[101] This point will be considered further in chapter 6 where it will be examined within the broader context of the availability of judicial review as against the IWF and the positive obligations of the state under Article 10 ECHR.[102]

(iii) Accountability and legitimacy

> We consider the IWF to be both an accountable and a transparent organisation. We have put in place a whole series of procedures and mechanisms to ensure utmost accountability and

[98] Bits of Freedom, 'Dutch Providers Abandon "ineffective" Web Blocking', 7 March 2011, https://www.bof.nl/2011/03/07/dutch-providers-abandon-ineffective-web-blocking/.
[99] See the Minutes of IWF Board Meeting 25 April 2001, discussed in Akdeniz, *Internet Child Pornography and the Law*, 264.
[100] *R. v. Panel on Takeovers and Mergers, ex p. Datafin* [1987] 2 WLR 699.
[101] On this point see e.g. Dawn Oliver, 'England and Wales: The Human Rights Act and the Private Sphere', in *Human Rights and the Private Sphere: A Comparative Study*, ed. Dawn Oliver and Jörg Fedtke (Abingdon: Routledge-Cavendish, 2007).
[102] See Chapter 6, section 3(v).

> transparency. The Board comprises a majority of non-industry members. The Chair is an independent appointee. We have in place good governance arrangements; we are a charitable organisation, and therefore are subject to the jurisdiction of the Charity Commission; we have regularly engaged independent experts to examine our processes and procedures; and taken together, those set of mechanisms we think provide for a high degree of accountability and transparency.[103]
>
> – Ian Walden, 2009

> The IWF dislikes being called a censor, and, strictly speaking, it isn't one. But, on the other hand, there cannot be the slightest doubt that it is involved in a process whose end result is self-censorship by ISPs understandably terrified of being accused of distributing child pornography… [A]lthough it was originally set up and now operates with strong governmental support, its workings have never been the subject of any sustained parliamentary or public scrutiny or debate. But, there again, why should they be? The IWF does not enjoy even the dubious status of a quango, and indeed takes considerable pains to stress that it is a purely private body. The problem, however, is that as such it lacks any kind of democratic legitimacy and authority for its actions.[104]
>
> – Julian Petley, 2009

A related complaint levelled at self-regulatory systems is that they often lack accountability and legitimacy. In some cases this overlaps with complaints about transparency and openness – as in Lessig's concerns about "truth in blocking"[105] – with critics concerned that users will not know what is being blocked, by whom, or how. In other cases, however, the concern is not that citizens will be unaware of particular actions or decisions, but rather that they will have no input into those actions nor methods to challenge them.

This line of criticism generally focuses on the shifting source of regulation – away from public bodies which are bound by constitutional constraints and subject to judicial review and towards private bodies such as ISPs which are exempt from these restrictions – and we have already mentioned the issues which this presents.

However, accountability through traditional administrative law mechanisms such as judicial review is merely one variety of accountability. Freeman, for example, has

[103] 'apComms Inquiry into Internet Traffic: Third Oral Evidence Session', 7 July 2009, http://www.apcomms.org.uk/uploads/090707_apComms_Oral_Evidence_-_3.doc.
[104] Julian Petley, 'Web Control', *Index on Censorship* 38, no. 1 (2009): 87.
[105] Lessig, *Code: Version 2.0*, 258.

pointed out that accountability may be ensured in relation to "private" actors by other mechanisms which might in some cases be adequate alternatives:

> Importantly, private actors are often already constrained by alternative accountability mechanisms that go largely unrecognized in administrative law. A private decision maker's internal procedural rules, market pressures, informal norms of compliance, third party oversight and the background threat of agency enforcement might hold private actors to account for their performance, even in what seem to be voluntary, self-regulatory systems. Although these forms of accountability may not satisfy the traditional administrative law demand for accountability to an elected body, they nonetheless may play an important role in legitimizing, or rendering acceptable, a particular regulatory regime.[106]

If we take this wider view, it might at first seem that there are significant and effective alternative accountability mechanisms in place for the IWF and the Cleanfeed system. There is certainly very significant accountability to the industry. Although only a minority of the IWF's board represent the internet industry, the industry ultimately controls the purse strings. Membership of the IWF is voluntary, as is deployment of the Cleanfeed system: dissatisfied ISPs are free to disengage if they are unhappy with the direction taken. Other mechanisms have also been used within the IWF to ensure accountability – one of the most significant is the carrying out of a regular independent audit.[107]

There is also substantial *de facto* accountability to different arms of the state. The IWF is crucially dependent on official recognition and support to enable it to carry out its functions. Were any of these to be withdrawn it is hard to see how it could continue to function. For example, its legal basis for exemption from liability for possession of child pornography relies on a 2004 Memorandum of Understanding between the Crown

[106] Jody Freeman, 'Private Parties, Public Functions and the New Administrative Law', *Administrative Law Review* 52, no. 3 (2000): 6.
[107] On this see e.g. Tom Espiner, 'IWF Chief: Why Wikipedia Block Went Wrong', *ZDNet.co.uk*, 20 February 2009, http://news.zdnet.co.uk/internet/0,1000000097,39616171,00.htm; Internet Watch Foundation, 'Board Minutes 8 July 2008', *Internet Watch Foundation*, 8 July 2008, http://www.iwf.org.uk/corporate/page.203.595.htm; Sommer, 'Re: Cleanfeed and Wikipedia', 9 December 2008.

Prosecution Service and the Association of Chief Police Officers.[108] Without this the legal risks to the IWF could render its work impossible. Similarly, in order to vet staff the IWF was obliged to approach the Home Office for the ability to seek enhanced disclosures (CRB checks) under Part 5 of the Police Act 1997. As Walden points out, since reorganising as a charity in 2004 the IWF is subject to the oversight of the Charity Commission. In addition, the IWF is in receipt of very substantial funding from official sources – in 2008/09 for example the Hotline function was subsidised by an EU grant under the Safer Internet Plus Programme to a total of €450,000.[109]

There is a noticeable absence here however: there is no apparent mechanism in place to ensure accountability to the affected *users* except indirectly, insofar as they might be heard via ISPs or via the state. As already mentioned, there is not a single trustee who could be described as representing a user or civil rights perspective.

A similar complaint can be made about processes within the IWF. Laidlaw has examined other aspects of IWF governance and has concluded that human rights oversight is lacking, noting that not one of the annual reports, strategic plans, and board minutes available to her mentions human rights.[110] Similarly, she points out that human rights issues do not feature in the audit process relied upon by the IWF as establishing its legitimacy. Consequently she argues that, even considered simply as a private company, the IWF would not meet the Ruggie principles to meet its responsibility to protect human rights.[111]

---

[108] Crown Prosecution Service and Association of Chief Police Officers, 'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003'.
[109] Project reference SIP-2007-HL-111702.
[110] Laidlaw, 'The Responsibilities of Free Speech Regulators', 29–30 In fairness to the IWF it should be said that there were several discussions of the Human Rights Act at board meetings in 2000-2001.
[111] As to which see John Ruggie, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (United Nations Human Rights Council, 2011), http://www.business-humanrights.org/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf.

Interestingly, the IWF was particularly stung by her criticism and in reply commissioned a human rights audit of its practices.[112] This *ad hoc* response – while desirable in itself – does however tend to reinforce her wider point that human rights compliance should be built in at a structural level and not merely addressed in an *ad hoc* or haphazard way. The audit was carried out by former DPP Ken Macdonald (now Lord Macdonald) but has yet to be published.[113]

The question of legitimacy also merits further attention. Thus far we have been assessing legitimacy primarily in relation to legal validity and in accordance with constitutional and human rights norms. Black, however, has suggested that this approach is often unsuitable for assessing new patterns of governance.[114] She notes that:

> Where regulatory regimes are largely non-legal and where, as in transnational regimes, infusing them with law is problematic, using only a legal concept of legitimacy will lead us to a dead end: such regimes will necessarily lack legitimacy and any potential for legitimacy in legal terms. They may, however, still be regarded as perfectly legitimate by others. The Forest Stewardship Council or Responsible Care, for example, are seen as legitimate by a number of market actors in the forestry and chemical industries respectively, but they have no legal basis.[115]

This point applies with equal force in the context of the IWF and the Cleanfeed system, both of which are undoubtedly regarded as legitimate by many observers, notwithstanding the problems we have already discussed. Black argues, therefore, that we should understand legitimacy not just in normative terms but also in sociological terms – to recognise that "[l]egitimacy means social credibility and acceptability" so that

[112] Internet Watch Foundation, 'Board Minutes 16 October 2012', 16 October 2012, https://www.iwf.org.uk/assets/media/accountability/board/Minutes%2016%20October%202012%20Web.pdf; Internet Watch Foundation, 'Board Minutes 20 November 2012', 20 November 2012, https://www.iwf.org.uk/assets/media/accountability/board/IWF%20Board%20Meeting%20Minutes%2020%20November%202012.pdf.
[113] Malcolm Hutty, 'IWF Human Rights Review', *LINX Public Affairs*, 26 November 2013, https://publicaffairs.linx.net/news/?cat=20.
[114] Julia Black, 'Legitimacy and the Competition for Regulatory Share', 23 June 2009, http://ssrn.com/abstract=1424654.
[115] Ibid., 9.

an organisation is legitimate if it is "perceived as having a right to govern both by those it seeks to govern and those on whose behalf it purports to govern".[116]

If we apply her reasoning to Cleanfeed, we end up with a more empirical and pragmatic approach to legitimacy, one which would ask in our case whether the IWF has succeeded in earning and maintaining perceptions of legitimacy amongst the communities (government, ISPs and internet users) it serves – an approach which might help us understand the potential harm to the IWF's reputation and legitimacy caused by e.g. the Wikipedia blocking. Using this form of analysis also helps to draw out the point that legitimacy is not necessarily something measured along a single dimension only – government agencies, ISPs and users may have very different views of the legitimacy of the Cleanfeed system.

On that point, it has to be noted that a perceived lack of legitimacy will itself hamper the work of the IWF. The Mobile Broadband Group made this point in submissions to the All Party Parliamentary Communications Group, noting the backlash which resulted from the Wikipedia incident and arguing that actions which were resented by the public could be expected to be ineffective:

> There have been discussions with the Home Office, for example, about the use of blocking for radicalisation sites. It was concluded that such an approach would be just too contentious and actually counter-productive, when there is no consensus among the wider population as to the legitimacy of blocking. By way of illustration, the IWF has had recent experience of the public objecting to the blocking of an image (albeit Level 1 illegal) that had been in the public domain for 30 years. The IWF's action led to the image being posted many many times, perhaps thousands of times, more. Whatever the rights and wrongs of that particular incident, it was a very clear demonstration of how power has shifted from government and corporations to the individual. It is very easy for actions taken for the best of motives to be completely counterproductive.[117]

For that reason, we see a very significant incentive for the IWF to ensure legitimacy at least in the sense outlined by Black – without public support, blocking is likely to be

[116] Ibid.
[117] All Party Parliamentary Communications Group, *Can We Keep Our Hands off the Net? Report of an Inquiry by the All Party Parliamentary Communications Group*, para. 45.

counterproductive. This has led to an extremely cautious approach on its part regarding the expansion of the blocking initiative.

(iv) Transparency

In Chapter 4 we considered the complaint that regulation by code resulted in a lack of transparency in relation to the operation of the Cleanfeed system and we examined how the technical and practical operation of the system was opaque to UK users. A similar complaint can be made that self-regulation masks the state role in the system. This is strikingly borne out in the case of Cleanfeed by a recent response from the Home Office to a freedom of information request regarding its involvement with the IWF:

> I regret to inform you that the Home Office does not hold the information that you have requested regarding the relationship between the IWF and the Home Office. The IWF is a self regulatory, independent charity that has no formal links with the Home Office.[118]

This response – that there are no "formal" links – may be true in a very narrow sense, but is belied by the very close relationship between the Home Office and the IWF. As we have seen in chapter 3, the Home Office was the midwife to the birth of the IWF, commissioned the report which led to its restructuring in 1999, led the push for mandatory blocking against the IWF URL list, and recently asked the IWF to expand its reporting mechanisms to cover "extreme pornography" under s.63 of the Criminal Justice and Immigration Act 2008. Given these links, the Home Office reply to the freedom of information request is disingenuous and is typical of other responses by the Home Office to attempts to scrutinise its relationship with the IWF.[119] While there is significant information publicly available about that relationship, it is striking that it is the IWF itself which makes that information available (through, for example, its public board minutes) rather than the Home Office. Consequently – and ironically – it is the

[118] Home Office, 'Response to Freedom of Information Act Request Re the Relationship between the Home Office and the IWF', *What Do They Know?*, 1 January 2009, https://www.whatdotheyknow.com/request/relationship_between_the_home_of.
[119] See e.g. Davies, 'The Hidden Censors of the Internet'.

self-regulatory body which better meets the spirit of freedom of information laws, supporting the argument that self-regulation can be the more transparent approach.[120]

(v) Compliance with the Interinstitutional Agreement on Better Law Making

A number of these concerns regarding self-regulation have received special treatment in EU law. Senden has charted the development of a "better regulation" agenda within the EU which, over the approximate period from 1998 to 2003, moved towards greater use of self- and co-regulatory policy tools.[121] This process led to a number of different policies being adopted – notably the July 2001 White Paper on European Governance and the June 2002 Action Plan "Simplifying and Improving the Regulatory Environment" – but for our purposes the most significant of these is the December 2003 Interinstitutional Agreement on Better Law-Making.[122] This agreement between the Parliament, the Council and the Commission established for the first time general criteria as to when self- and co-regulation should be used as policy instruments. It explicitly recognised a need to ensure democratic legitimacy and transparency and therefore provided in Article 17:

> 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.

This is an important provision – by its references to transparency, publicity of agreements and representativeness of parties it sets high standards for self-regulatory mechanisms generally but also expressly rules out the use of self- or co-regulatory mechanisms where "fundamental rights... are at stake". It is striking, however, that it has not influenced European policy towards internet content which has continued to rely

[120] Perry, Telephone Interview.
[121] Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law'.
[122] European Parliament, Council and Commission, 'Interinstitutional Agreement on Better Law-Making'[2003] OJ C321/1.

heavily on self-regulation – and indeed recently has moved even further in this direction.[123] The criticism here is that content regulation of its very nature involves restrictions of freedom of expression but is not being assessed against the standards set out in the Interinstitutional Agreement.[124] The point is particularly acute in relation to Directive 2011/93/EU which promotes self-regulatory blocking in a way which the Commission had previously found likely to breach Article 10 ECHR.[125] Consequently, there is a strong argument that European involvement in this area – particularly Directive 2011/93/EU – has the effect of facilitating blocking in a way which does not meet the requirements of the Interinstitutional Agreement.[126]

5. Conclusion

In the previous chapter we examined the cyber-libertarian/cyber-paternalist debate and we considered two of the regulatory tactics which were said by cyber-paternalists to enable greater state control of internet content. We concluded that those two tactics – code as law and gatekeeper regulation – when used in the context of Cleanfeed had manifested only some of the risks identified for them, and that the incentives faced by ISPs and in particular the IWF shaped the application of these tactics in a way which was not always recognised in the literature.

In this chapter we examined the third tactic in this regulatory triad – self regulation – and the way in which it has been used in the context of the Cleanfeed system. We

[123] Cooke, 'Controlling the Net'.
[124] For a summary of recent developments see e.g. Joe McNamee, 'Privatised Online Enforcement Series: Abandonment of the Rule of Law', *EDRi: European Digital Rights*, 23 March 2011, http://www.edri.org/edrigram/number9.6/abandonment-rule-of-law.
[125] See McIntyre, 'Blocking Child Pornography on the Internet', 214.
[126] This is supported by Lievens et al. who take a narrow view of the requirements of the Interinstitutional Agreement, suggesting that it would permit co-regulatory solutions, but agree that it rules out self-regulatory solutions: 'this constraint does not preclude the use of co-regulation in the media sector, so long as a sensible balance is sought between protecting freedom of expression to the greatest extent possible (through the provision of certain democratic government guarantees) and establishing a flexible, effective, and enforceable system of co-regulation.' See Lievens, Dumortier, and Ryan, 'The Co-Protection of Minors in New Media', 147.

assessed how many of the same criticisms in relation to code as law and gatekeeper regulation (notably the possible effect on transparency, legitimacy and accountability) may apply to self-regulation, but also identified benefits to self regulation and in particular considered how the requirement for industry participation acts as a check on the IWF and therefore indirectly on state action. Consequently, it might again be concluded that the incentives of industry actors can operate to minimise the risks associated with self-regulation.

Given the deficiencies in accountability and transparency we identified in both chapters, there appears to be a clear need for reform of the Cleanfeed system, though this chapter cautions against a rush to greater state involvement in the operation of the IWF. However, the extent to which reform must take place and the nature of reform required will depend on the legal obligations which already apply to ISPs, the IWF and the state. The next chapter will consider these obligations and in particular will consider to what extent public law can already intervene to control the operation of the Cleanfeed system, both as a matter of domestic law and international legal obligations.

Chapter 6 – Public Law and Positive Obligations

1. Introduction

In previous chapters we outlined the way in which the UK government has promoted self- and co- regulatory solutions in the online space, reflecting a deliberate policy choice to minimise the use of legislation. We also saw claims that this approach – especially where coupled with the use of gatekeeper regulation and technological enforcement tools – tends to undermine constitutional values by restricting fundamental rights while also insulating regulation from legal scrutiny. In this chapter we examine those claims by assessing the extent to which the law might enforce fundamental rights and public law norms as against the IWF, ISPs and the state itself.

We begin by considering the threshold question as to whether and how English law might regard the IWF and the Cleanfeed system as having a public dimension. In particular, we will consider whether the IWF may exercise a "public function" for the purposes of judicial review; whether it might be considered a "public authority" under the Human Rights Act 1998; and whether it could amount to an "emanation of the state" for the purposes of European Union law. Following this we then consider the extent to which the UK faces a positive obligation under the ECHR which may require it to safeguard freedom of expression in the context of the Cleanfeed system.[1]

2. Research context

> Because, as a technical matter, the government in such cases is not technically mandating such speech restrictions and because such restrictions are "voluntarily" undertaken by private ISPs at the behest of the government in cooperation with "private" organizations like the IWF, these speech restrictive actions are technically outside the scope of applicable national laws protecting citizens' free speech rights, like the UK's Human Rights Act.
>
> – Dawn Nunziato, 2011[2]

[1] For discussion of state liability for non-state actors under other instruments see in particular Cheung and Weber, 'Internet Governance and the Responsibility of Internet Service Providers'.
[2] Nunziato, 'How (not) to Censor', 1138.

The literature on internet freedom sometimes paints with a very broad brush, making generalised claims about technological and governance trends without adequately considering national conditions. Nunziato exemplifies this with her assertion that the Cleanfeed system exists beyond the scope of the Human Rights Act – a claim that is not supported by any analysis of English law and which, it will be argued later in this chapter, is inconsistent with the authorities. Such a wide approach may be necessary when considering the international picture as a whole. However, when applied to particular national contexts it can mean that arguments for reform neglect the actual conditions on the ground. Nunziato, for example, argues for the export of the First Amendment "state action" doctrine to the UK while entirely overlooking the considerable domestic jurisprudence which already exists regarding the attribution of responsibility to the state for "private" actors.[3]

It is desirable, therefore, to test the general predictions which have been made about internet freedoms with a view to seeing whether these predictions have been borne out in the English context. This requires us to consider whether the use of self-regulation has in fact resulted in the Cleanfeed system being insulated from judicial challenge by looking in more detail at the availability of remedies. When we do so, it becomes striking how little has been written on this point – or indeed on the wider question of judicial oversight of internet self-regulation in England.

[3] As to which see e.g. Oliver, 'England and Wales: The Human Rights Act and the Private Sphere'; Colin D. Campbell, 'The Nature of Power as Public in English Judicial Review', *The Cambridge Law Journal* 68, no. 01 (2009): 90; Tony Prosser, 'Constitutional Guarantees in the Light of Privatisation: The UK Experience' (presented at the VII World Congress of the International Association of Constitutional Law, Athens, 11 June 2007), http://www.enelsyn.gr/papers/w10/Paper%20by%20Prof.%20Tony%20Prosser.pdf; Richard Mumford and Jaime Arancibia, *Self-Regulation in England and Wales*, NewGov: New Modes of Governance Project (Florence: European University Institute, 2007), http://www.eu-newgov.org/database/DELIV/DLTFIbD09a_Final_Chapters_on_self-regulation_England_and_Wales.pdf.

Most of the leading pieces on the IWF and Cleanfeed, for example, note that challenges to the actions of the IWF may be problematic but do not discuss this point further.[4] Indeed, on a close examination of the literature only four authors appear to have considered in detail the ways in which the English courts might apply public law norms or fundamental rights as against internet self-regulatory schemes.[5]

Why is this? A lack of source material may play a part. To date there is no English case law regarding the application of public law norms to internet self-regulation. There has been no litigation regarding the IWF, while the only attempt to judicially review Nominet failed at the leave stage – though apparently on the basis of failure to exhaust remedies rather than amenability to judicial review – leaving us without the benefit of a determination on its public or private status.[6] Another possible reason is the IWF concession that it is a public body for the purposes of the Human Rights Act, discussed further below, which may have discouraged detailed consideration of its status.

In any event, this chapter will address this gap in the literature by considering in more detail whether the Cleanfeed system should be understood as being already within the realm of public law. It should be noted, however, that the focus of this chapter will be on the *application* of public law norms – for example, whether the IWF will be subject to judicial review. The *content* of those norms – for example, whether a right to be heard might be required before a blocking decision is made or whether overblocking might result in a breach of Article 10 ECHR – will be considered in chapter 7.

[4] See e.g. Akdeniz, *Internet Child Pornography and the Law*, 263–267; Edwards, 'Pornography, Censorship and the Internet', 655–658; Petley, 'Web Control'.
[5] See Mark Gould, 'An Island in the Net: Domain Naming and English Administrative Law', *John Marshall Journal of Computer & Information Law* 15 (1997): 493; Mac Sithigh, 'Datafin to Virgin Killer'; Marsden, 'Internet Co-Regulation and Constitutionalism'; Marsden, *Internet Co-Regulation*, chap. 2; Laidlaw, 'The Responsibilities of Free Speech Regulators'.
[6] 'Nominet Wins iTunes.co.uk Decision', *OUT-LAW.COM*, 5 August 2005, http://www.out-law.com/page-5979.

3. Applying public law

(i) Background

> In the United Kingdom, as in other liberal democracies, the last decade has been a period of quiet revolution in public administration. Successive governments elected on political platforms promising to "roll back the state" have presided over changes in the mode of governance which have transformed the relation between public and private... Activities previously subject to close administrative controls have been deregulated, and other activities formerly carried out directly by public bodies have been "contracted out" to the private sector...
>
> – Murray Hunt, 1997[7]

To understand the way in which the law might control the operation of the Cleanfeed system it will be helpful to begin by setting it within a wider context. Since the early years of the Thatcher government, public law in the United Kingdom has had to deal with significant changes in the nature of the state. Trends such as privatisation, outsourcing and deregulation have led to a "contracting state" – "contracting" in the sense of shrinking, in the sense of contracting out functions to the private sector and also in the sense of using contracts as a tool of governance.[8] More recently these have been characterised as leading to a new form of "decentred governance" or a "post-regulatory state" in which the state and legislation are no longer necessarily viewed as central to regulation and where more emphasis is placed on approaches such as self-regulation, soft law and non-state rulemaking.[9]

Against this background the UK preference for online self-regulation is not an outlier but instead exemplifies a more general approach whereby the state has withdrawn from

---

[7] Murray Hunt, 'Constitutionalism and the Contractualisation of Government in the United Kingdom', in *The Province of Administrative Law*, ed. Michael Taggart (Oxford: Hart Publishing, 1997), 21.
[8] See generally Terence Daintith, 'Regulation by Contract: The New Prerogative', *Current Legal Problems*, 1979, 41; Ian Harden, *The Contracting State* (Buckingham: Open University Press, 1992); Hunt, 'Constitutionalism and the Contractualisation of Government in the United Kingdom'; Jody Freeman, 'The Contracting State', *Florida State University Law Review* 28 (2000): 155.
[9] See in particular Colin Scott, 'Regulation in the Age of Governance: The Rise of the Post-Regulatory State', in *The Politics of Regulation: Examining Regulatory Institutions and Instruments in the Age of Governance*, ed. Jacint Jordana and David Levi-Faur (Cheltenham: Edward Elgar, 2004); however, note the limitations identified in Adam Crawford, 'Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security', *Theoretical Criminology* 10, no. 4 (November 2006): 449–79.

the delivery (though not necessarily the oversight) of a wide range of functions.[10] In particular, the work of the IWF in assessing legality might be said to reflect a move towards "bottom-up" privatisation – one where a governmental activity is taken on by a private actor without any formal transfer taking place.[11]

Following these trends and their blurring of the public/private divide, one of the most difficult questions in English law has come to be that of deciding when public law standards (and through them fundamental rights) should be applied to functions which might be described as governmental but are placed in the hands of private actors. This is particularly challenging in the context of self-regulation where the law has struggled to develop a principled basis to reconcile the need to regulate abuses of power with the rightful autonomy of private bodies.[12]

Surveying this much-litigated area, we can say that there are three distinct but related approaches which will determine whether the actions of a private body can be attributed to the state, depending on the type of right which is asserted and the type of remedy sought.[13] The first is judicial review, as a freestanding remedy available in respect of the exercise of "public functions" even by an otherwise private body. Second, the Human Rights Act 1998 makes available a cause of action against a "public authority" which acts in a way which is incompatible with a Convention right, where the term public authority is defined to include "any person certain of whose functions are of a public nature".[14] Third, under European Union law it may be possible to enforce certain rights as against an "emanation of the state" under the principle set out in *Foster v. British Gas.*[15] Each of these will be outlined in turn before being applied to the case of the IWF.

[10] Collins, 'Networks, Markets and Hierarchies'.
[11] The terminology is taken from Catherine Donnelly, 'Positive Obligations and Privatisation', *Northern Ireland Legal Quarterly* 61 (2010): 209.
[12] See e.g. Black, 'Constitutionalising Self Regulation'.
[13] For a comprehensive review of the caselaw see Campbell, 'The Nature of Power as Public in English Judicial Review'.
[14] Section 6.
[15] Case C-188/89 *Foster v. British Gas* [1990] ECR I-3313.

(ii) Judicial review and public functions

> In one sense, then, there is no 'constitutional' background to the protection of human rights in the private sphere in England. England's is a legal system in which areas where Parliament has not occupied the field (and where European Community law does not apply), including much of the private sphere, are regulated – or not regulated – by the common law and equity. At least in the private sphere everyone enjoys freedom to do as they will unless there is a positive law to the contrary.
>
> – Dawn Oliver, 2007[16]

One of the most significant aspects of English law, highlighted by Oliver, is that it does not have a general doctrine whereby human rights are enforceable as between private actors unless there is some pre-existing legal relationship between them. This is so notwithstanding that a body may exercise significant power over an individual or even an entire industry. Instead the dominant position remains that fundamental rights have vertical effect only – amounting to a check on the power of the state – rather than having horizontal effect so as to restrict the actions of other individuals or private bodies.[17]

Given this fact, one of the few mechanisms open to an individual who claims that their rights have been violated by a private body has been to argue that the body should be regarded as carrying out a "public function" within the meaning of Part 54 of the Civil Procedure Rules, which defines a "claim for judicial review" to include "a claim to review the lawfulness of... a decision, action or failure to act in relation to the exercise of a public function".[18] This concept, as applied by a line of case law from *R. v. Panel on Takeovers and Mergers, ex parte Datafin*[19] onwards, will determine when such an exercise of power is reviewable as a matter of public law. This will enable a challenge on the basis of illegality, irrationality or procedural impropriety and – more recently –

[16] Oliver, 'England and Wales: The Human Rights Act and the Private Sphere', 63.
[17] See e.g. Colm O'Cinneide, 'Taking Horizontal Effect Seriously: Private Law, Constitutional Rights and the European Convention on Human Rights', *Hibernian Law Journal* 4, no. 1 (2003): 77.
[18] On the 'new' rules in Part 54 and the ways in which they differ from the old rules in O.53 RSC see generally Tom Cornford, 'The New Rules of Procedure for Judicial Review', *Web Journal of Current Legal Issues* 5 (2000), http://webjcli.ncl.ac.uk/2000/issue5/cornford5.html.
[19] [1987] QB 815.

also on the developing[20] grounds of good administration[21] and proportionality.[22] These grounds – while they do not themselves directly provide for the enforcement of fundamental rights – do protect procedural rights and enable the court to assess whether other rights were properly taken into account in the decision making process.[23]

When, then, can it be said that a body exercises a "public function" so as to make it amenable to judicial review? Until relatively recently the law focused solely on the *source* of the power exercised by the body, asking whether it was rooted in statute or the prerogative. The result, in the case of industry self-regulatory bodies, was that they were viewed as creatures of private agreement which therefore fell outside the scope of judicial review. As Parker CJ put it in *R. v. Criminal Injuries Compensation Board, ex parte Lain:* "Private or domestic tribunals have always been outside the scope of *certiorari* since their authority is derived solely from contract, that is, from the agreement of the parties concerned".[24]

This approach was modified in 1986 by *Datafin.* In that case the Court of Appeal found that the function of the City Panel on Takeovers and Mergers, a non-governmental and self-described "self-regulatory" body, was nevertheless amenable to judicial review. In a judgment which expressed considerable concern about unfettered private power Sir John Donaldson MR began by noting that the term self-regulation was a loaded one, which very often comprised the regulation of others:

---

[20] As to the developing grounds see e.g. Dawn Oliver, 'What, If Any, Public-Private Divides Exist in English Law?', in *The Public-Private Law Divide: Potential for Transformation?*, ed. Matthias Ruffert (London: British Institute of International and Comparative Law, 2009), 7; Andrew Le Sueur, 'Courts, Tribunals, Ombudsmen, ADR: Administrative Justice, Constitutionalism and Informality', in *The Changing Constitution*, ed. Jeffrey Jowell and Dawn Oliver, 6th ed. (Oxford: Oxford University Press, 2007), 336–337.

[21] *R. (Nadarajah) v. Secretary of State for the Home Department* [2005] EWCA Civ 1363.

[22] *O'Reilly v. Mackman* [1983] 2 AC 237.

[23] This is, however, a significantly lower standard of review than that which applies in an action under the Human Rights Act 1998. *Per* Baroness Hale in *Belfast City Council v. Miss Behavin' Ltd* [2007] UKHL 19, para. 31: "The role of the court in human rights adjudication is quite different from the role of the court in an ordinary judicial review of administrative action. In human rights adjudication, the court is concerned with whether the human rights of the claimant have in fact been infringed, not with whether the administrative decision-maker properly took them into account."

[24] [1967] 2 QB 864, 882.

> "Self-regulation" is an emotive term. It is also ambiguous. An individual who voluntarily regulates his life in accordance with stated principles, because he believes that this is morally right and also, perhaps, in his own long term interests, or a group of individuals who do so, are practising self-regulation. But it can mean something quite different. It can connote a system whereby a group of people, acting in concert, use their collective power to force themselves and others to comply with a code of conduct of their own devising. This is not necessarily morally wrong or contrary to the public interest, unlawful or even undesirable. But it is very different.[25]

The Master of the Rolls then turned to look at the considerable *de facto* power exercised by the Panel, notwithstanding its lack of any "visible means of legal support"[26], and took a wide view of the decision in *Lain* as articulating a functional test towards judicial review – one which looks to the *nature* of the power being exercised.[27] In determining whether a power is subject to judicial review the Master of the Rolls identified the only essential points as being (a) that there should be a "public element" and (b) that judicial review is excluded in relation to "bodies whose sole source of power is a consensual submission to its [*sic*] jurisdiction".[28] Beyond these, the Master of the Rolls described the case law as enumerating a number of factors determining amenability to judicial review but stated that these factors are not exclusive, nor is it essential that all these factors be present.[29]

Using this analysis the court determined that the Panel was amenable to judicial review, finding that it performed an important public duty, exercised "immense power" over citizens whether or not they had technically assented to its jurisdiction and was obliged to act judicially but was beyond the effective control of private law remedies. Most importantly, the court noted that the Panel was backed up by considerable indirect statutory recognition and support so that it could be said to form part of a wider governmental regulatory system. According to the Master of the Rolls:

[25] [1987] QB 815, 826.
[26] 824.
[27] 838.
[28] 838.
[29] 838.

> As an act of government it was decided that, in relation to takeovers, there should be a central self-regulatory body which would be supported and sustained by a periphery of statutory powers and penalties wherever non-statutory powers and penalties were insufficient or non-existent or where EEC requirements called for statutory provisions.
>
> No one could have been in the least surprised if the panel had been instituted and operated under the direct authority of statute law, since it operates wholly in the public domain. Its jurisdiction extends throughout the United Kingdom. Its code and rulings apply equally to all who wish to make take-over bids or promote mergers, whether or not they are members of bodies represented on the panel. Its lack of a direct statutory base is a complete anomaly, judged by the experience of other comparable markets world wide… [T]he position has already been reached in which central government has incorporated the panel into its own regulatory network built up under the Prevention of Fraud (Investments) Act 1958 and allied statutes, such as the Banking Act 1979.[30]

The limits of the "regulatory network" approach in *Datafin* can be seen in *R. v. Disciplinary Committee of the Jockey Club, ex parte Aga Khan*.[31] That case was in some ways very similar to *Datafin,* in that it involved a self-regulatory body which exercised effective control over an important industry, where those wishing to take part in horseracing had no realistic alternative but to submit to the Club's Rules of Racing and its Disciplinary Committee. Here, however, the Court of Appeal held that these factors were not sufficient. Central to this finding was a distinction between powers which affect the public and governmental powers – the latter requiring some greater element of state involvement. Sir Thomas Bingham MR could therefore characterise the Club as not being subject to judicial review despite the fact that it regulated a "significant national activity" so that if it did not exist "the government would probably be driven to create a public body to do so".[32] Despite this, the Master of the Rolls held that the necessary degree of state participation was lacking – unlike the Takeover Panel, the Jockey Club had not been incorporated into a wider governmental scheme nor given statutory support for its powers:

> But the Jockey Club is not in its origin, its history, its constitution or (least of all) its membership a public body. While the grant of a Royal Charter was no doubt a mark of official approval, this did not in any way alter its essential nature, functions or standing. Statute provides for its representation on the Horseracing Betting Levy Board, no doubt as a body with an obvious interest in racing, but it has otherwise escaped mention in the statute book. It has not been woven into any system of governmental control of horseracing, perhaps because it has itself controlled

[30] 835-836.
[31] [1993] 1 WLR 909.
[32] 923.

> horseracing so successfully that there has been no need for any such governmental system and such does not therefore exist. This has the result that while the Jockey Club's powers may be described as, in many ways, public they are in no sense governmental.[33]

Hoffman LJ likewise differentiated the decision in *Datafin* and other cases regarding the judicial review of self-regulatory bodies on the basis that those cases involved "a privatisation of the business of government itself... [by] private bodies established by the industry but integrated into a system of statutory regulation".[34]

The *Aga Khan* decision also confirmed that *Datafin* had not established a purely functional test for judicial review – the *source* of power remained important insofar as the applicant had a contractual relationship with the Club which afforded him an adequate private law remedy in cases of abuse of power (though the members of the court reserved their position as to whether a public law remedy should be made available if private law remedies were inadequate). As a result, the test for judicial review remains a relatively narrow one which requires significant government involvement – the fact that a respondent exercises considerable private power, even over an entire industry, is not enough. In the words of Hoffman LJ, the courts remain reluctant to "patch up the remedies available against domestic bodies by pretending that they are organs of government".[35]

(iii) Public authorities under the Human Rights Act 1998

The limits of *Datafin* and its progeny were a cause for some concern when the Labour government delivered on its commitment to "bring rights home" through the incorporation of the European Convention on Human Rights into domestic law. In particular, the narrow scope of judicial review left it unclear whether traditional state

[33] 923.
[34] 931-932.
[35] 933.

functions (such as the provision of healthcare) would be subject to human rights guarantees where outsourced to charitable or commercial entities.[36]

Section 6 of the Human Rights Act 1998 addressed this point by attempting to clarify the human rights obligations of non-state bodies. Section 6(1) introduced the new concept of a "public authority" and provides that it is unlawful for a public authority to act in a way which is incompatible with Convention rights. The term public authority is not fully defined, but section 6(3)(b) includes in the concept "any person certain of whose functions are functions of a public nature".

As explained by the House of Lords in *Aston Cantlow and Wilmcote PCC v. Wallbank*[37] this creates a twofold classification. On one side are bodies such as government departments, local authorities, the police and armed forces which are so closely identified with the state as to amount to "core" public authorities. These are governed by section 6(1) without reference to section 6(3)(b) and thus are subject to the requirements of the Convention in everything they do.[38] On the other side the House of Lords identified section 6(3)(b) as creating a category of "hybrid" public authorities – those which exercise both public functions and non-public functions. Such bodies are also obliged to respect Convention rights under section 6(1), but only when carrying out a public function – under section 6(5) such a person is not a public authority in relation to a particular act "if the nature of the act is private".

At first glance, this appeared to create a statutory scheme which resembled the post-*Datafin* case law on judicial review of private bodies, with a similar focus on the public nature of a particular function, and indeed the Court of Appeal in *Aston Cantlow* itself relied heavily on that case law for guidance. In the House of Lords, however, this was criticised on the basis that it neglected the international law origins of the rights

[36] See e.g. Elizabeth Palmer, 'Should Public Health Be a Private Concern? Developing a Public Service Paradigm in English Law', *Oxford Journal of Legal Studies* 22, no. 4 (2002): 663.
[37] [2003] UKHL 37.
[38] See in particular the speech of Lord Nicholls, paras. 8-11.

protected in the 1998 Act. In particular, their Lordships took the view that the test to be applied was one which mirrored the approach which would be taken in Strasbourg with regard to state liability – as Lord Rodger put it, one must look "behind the Act to the Convention itself".[39] He went on to say that the intention of the Act "was to make provision in our domestic law to ensure that the bodies carrying out the functions of government in the United Kingdom observed the rights and freedoms set out in the Convention" and therefore "the essential characteristic of a public authority is that it carries out a function of government which would engage the responsibility of the United Kingdom before the Strasbourg organs".[40]

That is not to say that the judicial review case law is of no use in this context, and indeed Lord Hope explicitly noted that it might well be helpful as to whether a particular power constitutes "a function of a public nature".[41] It does, however, mean that the 1998 Act by no means parallels the *Datafin* test.

Lord Nicholls expanded on the approach to be taken under the 1998 Act by identifying four particular factors which would identify a "governmental" function for the purposes of the ECHR, holding that:

> [T]he statute does not amplify what the expression "public" and its counterpart "private" mean in this context. But, here also, given the statutory context already mentioned and the repetition of the description "public", essentially the contrast being drawn is between functions of a governmental nature and functions, or acts, which are not of that nature. I stress, however, that this is no more than a useful guide. The phrase used in the Act is public function, not governmental function...
>
> What, then, is the touchstone to be used in deciding whether a function is public for this purpose? Clearly there is no single test of universal application. There cannot be, given the diverse nature of governmental functions and the variety of means by which these functions are discharged today. *Factors to be taken into account include the extent to which in carrying out the relevant function the body is publicly funded, or is exercising statutory powers, or is taking the place of central government or local authorities, or is providing a public service* [emphasis added].[42]

[39] Para. 157.
[40] Para. 160.
[41] Para. 52.
[42] Paras. 9-12.

Applying these factors the House of Lords held (by a majority) that the plaintiff parochial church council was not acting as a public authority when it served a notice on the defendants calling on them to repair the chancel of the parish church but rather was merely acting to enforce a private law liability.

The House of Lords has elaborated further on this test in *YL v. Birmingham City Council*[43]. In this case Birmingham City Council was under a statutory duty to make arrangements for the provision of care and accommodation for YL, who suffered from Alzheimer's disease. It did so under a contract with Southern Cross Healthcare Ltd., a private business operating a residential care home. Ultimately the relationship between YL's family and staff in the home broke down, at which point Southern Cross sought to terminate YL's right to remain. The question then arose whether YL could assert the Article 8 right to a family life as against Southern Cross.

This question – in essence, whether Southern Cross should be treated as a hybrid public authority – was tried as a preliminary issue and decided in the negative by a 3-2 majority. While the majority and the minority were agreed that the presence of coercive, disciplinary or regulatory functions were strong indications that a body is a public authority, they differed when it came to the more difficult case of outsourced service delivery where these factors tend not to be present.[44] In deciding that Southern Cross was not a section 6(3)(b) public authority, the majority placed most emphasis on the commercial nature of the enterprise and the contractual nature of its relationship with the Council. In an oft-quoted passage, Lord Scott summarised these points by noting that:

> Southern Cross is a company carrying on a socially useful business for profit. It is neither a charity nor a philanthropist. It enters into private law contracts with the residents in its care homes and with the local authorities with whom it does business. It receives no public funding, enjoys no special statutory powers, and is at liberty to accept or reject residents as it chooses (subject, of course, to anti-discrimination legislation which affects everyone who offers a service to the public) and to charge whatever fees in its commercial judgment it thinks suitable. It is operating in a commercial market with commercial competitors... [T]he fees charged by Southern

[43] [2007] UKHL 27.
[44] See in particular paras. 28, 101, 121, 166 and 167.

> Cross and paid by local or health authorities are charged and paid for a service. There is no element whatsoever of subsidy from public funds.[45]

Lord Mance similarly placed reliance on the effect which a public authority finding would have on the ability of Southern Cross to run its business, suggesting that the duties which might arise as a result would fit uneasily with "the ordinary private law freedom to carry on operations under agreed contractual terms".[46]

By contrast, Lord Bingham and Baroness Hale would have held that Southern Cross was a hybrid public authority, seeing those in residential care as particularly vulnerable to human rights abuses and the outsourcing of this type of formerly public function as precisely the type of case which section 6(3)(b) of the 1998 Act was intended to capture. Indeed, the dissenters went so far as to describe the approach of the majority in separating the (public) *arrangement* of care by the Council from the (private) *delivery* of care by Southern Cross as being "artificial and legalistic".[47]

In any event, the particular outcome in *YL* was promptly reversed, with legislation passed to deem a private care home under contract with a local authority to be exercising "a function of a public nature".[48] However, *YL* remains the subject of significant criticism, not least because it appears to reject a clear Parliamentary intention in relation to outsourced public functions. The Joint Committee on Human Rights has since called for wider legislative change to restore what it describes as "the original intention of Parliament, that all private bodies exercising public functions should be subject to the duty to act compatibly with human rights".[49]

---

[45] Paras. 26-27.
[46] Para. 116.
[47] See in particular the comments of Lord Bingham at paras. 19-20 and those of Baroness Hale at paras. 61-72.
[48] Section 145 of the Health and Social Care Act 2008.
[49] See e.g. John McGarry, '"Functions of a Public Nature" under the Human Rights Act 1998: The Decision of the House of Lords in YL v Birmingham City Council', *Web Journal of Current Legal Issues* 5 (2007), http://webjcli.ncl.ac.uk/2007/issue5/mcgarry5.html; Stephanie Palmer, 'Public, Private and the Human Rights Act 1998: An Ideological Divide', *Cambridge Law Journal* 66 (2007): 559; Mac Sithigh, 'Datafin to Virgin Killer'; Joint Committee on Human Rights, *Any of Our Business? Human Rights and the UK Private Sector* (London: HMSO, 2009), para. 136.

There has been surprisingly little litigation since *YL* considering whether a particular body is a hybrid public authority for the purposes of the 1998 Act, with the only reported decision being that of the Court of Appeal in *R. (Weaver) v. London & Quadrant Housing Trust.*[50] In that case a divided court (Rix LJ dissenting) found a private residential social landlord (RSL) to be a hybrid public authority which was carrying out a public function in deciding to terminate a tenancy for rent arrears. Despite some similarities to *YL* the majority (Collins LJ and Elias LJ) held that the earlier case could be distinguished – while this was also a case of outsourced delivery of a service, they took the view that it was removed from the private law and commercial context of *YL*. Specifically, the majority held that the RSL was a non-profit, charitable body which by delivering *subsidised* housing was engaged in an inherently public function. They stressed the fact that payments to the RSL were subsidies, not merely payments for services, and noted that the RSL worked very closely with local government and was subject to very close statutory regulation in matters such as the allocation and management of properties. Consequently, the termination of the tenancy was held to be so bound up in the public function of the provision of social housing that it must also be seen as a public act.[51] This result, along with the judicial divisions in both *Weaver* and *YL* itself, highlights the fact sensitive nature of the test established by *Aston Cantlow* and the continued difficulties which the courts face in applying it.

(iv) Emanation of the state and European Union law

The final way in which the actions of the IWF might be treated as having a public law character is through the European law doctrine of direct effect. As is well known, a Member State may not rely on its own failure to perform its obligations under a directive and consequently an individual may be able to assert rights conferred by an

[50] [2010] 1 WLR 375.
[51] See e.g. Justin Leslie, 'Approaches to Section 6 HRA: Lessons from Weaver v. London and Quadrant Housing Trust', *Judicial Review* 14, no. 4 (2009): 327–332.

unimplemented directive against the state. This vertical direct effect will in turn apply not just against central government but also against a wider set of public bodies.[52] In English law these are usually referred to as "emanations of the state", though this phrase is not one endorsed by the ECJ and has been criticised as potentially misleading.[53] This doctrine of direct effect, established in *Marshall v. Southampton Area Health Authority*[54], differs very substantially from both judicial review and the Human Rights Act in that once a body is regarded as an emanation of the state then it is subject to direct effect in relation to all its functions, public and private alike. It therefore ensures that an individual can rely on a directive against the state "regardless of the capacity in which the latter is acting, whether employer or public authority".[55]

Whether a body will be treated as part of the state for the purposes of direct effect is a matter of European law primarily determined by *Foster v. British Gas*.[56] In that case the ECJ set out a wide understanding of the state, holding in paragraph 20 that:

> a body, whatever its legal form, which has been made responsible, pursuant to a measure adopted by the State, for providing a public service under the control of the State and has for that purpose special powers beyond those which result from the normal rules applicable in relations between individuals is included in any event among the bodies against which the provisions of a directive capable of having direct effect may be relied upon.[57]

In *Foster* itself, therefore, the House of Lords ultimately held that British Gas fell within this test so as to be bound by European equality law in relation to retirement ages, on the basis that British Gas provided a public service, did so under the control of the state which was entitled to dictate its policies and benefit from its surpluses, and enjoyed special powers in that it held a monopoly on the supply of gas within the United Kingdom.[58]

---

[52] See e.g. Paul Craig, 'The Legal Effect of Directives: Policy, Rules and Exceptions', *European Law Review* 34, no. 3 (2009): 349.
[53] See e.g. the comments of Mustill LJ in *Rolls-Royce Plc v. Doughty* [1992] ICR 538.
[54] Case C-152/84, *Marshall v. Southampton Area Health Authority* [1986] ECR 723.
[55] Para. 49.
[56] Case C-188/89 *Foster v. British Gas* [1990] ECR I-3313.
[57] Para. 20.
[58] [1991] 2 AC 306.

The test in *Foster* is not, however, the only basis on which a body can be treated as an emanation of the state. The language in paragraph 20 – stating that such a body "is *included* in any event among the bodies [against which direct effect may be relied upon]"[59] – suggests that other factors may also have the effect of causing a body to be treated as an emanation of the state. This has been accepted by the Court of Appeal in *Rolls-Royce Plc v. Doughty*[60] where Mustill LJ held that *Foster* "was not intended to provide the answer to every category of case. The words 'is included among'... make this clear enough". Notwithstanding this, Mustill LJ went on to say that in most cases the *Foster* test would be decisive:

> Nevertheless, at least in a case of the same general type as *Foster* the Court's formulation must always be the starting point, and will usually be the finishing point. If all the factors identified by the Court are present it is likely to require something very unusual to produce the result that an entity is not to be identified with the state. Conversely, although the absence of a factor will not necessarily be fatal, it will need the addition of something else, not contemplated by the formula, before [direct effect] has a prospect of being brought into play.

In that case Rolls Royce was found not to be subject to direct effect. Despite being entirely state owned, the Court of Appeal took the view that it was a commercial undertaking, trading with the state at arm's length rather than providing a public service, and did not enjoy any special powers of the type referred to in *Foster*.

By contrast, in *National Union of Teachers v. St. Mary's Church of England (Aided) Junior School*[61] Schieman LJ for a unanimous Court of Appeal held that a voluntary aided school had to be regarded as an emanation of the state because it was responsible for providing a public service on foot of a statutory instrument and was under the control of the state insofar as its activities were closely regulated by both the Secretary of State and the relevant Local Education Authority. While the court accepted that the school did not enjoy any "special powers beyond those which apply between individuals", this was held not to be an absolute requirement where other *indicia* of public status were present.

[59] Emphasis added.
[60] [1991] EWCA Civ 15.
[61] [1996] EWCA Civ 1194.

The earlier decisions in *Foster* and *Rolls-Royce* were distinguished on the basis that both involved commercial undertakings in which the state held a stake – not the provision of an inherently public service such as education – though in neither of those cases had the court relied upon this factor.

(v) Assessing the public status of the IWF

> [W]e have, at most, some separate substantive and adjectival public *laws*, but we do not have a coherent divide between public and private law or laws.
>
> – Dawn Oliver, 2009[62]

From our brief survey of the different tests used in the context of judicial review, the Human Rights Act and direct effect it will be clear that there is no single method by which to determine whether the courts would treat the actions of the IWF in administering the Cleanfeed system as being public in nature.[63] This is, perhaps, to be expected. Each test has evolved to serve a very different purpose: there are substantial differences between the narrow Diceyan concept of legality served by judicial review[64], the Human Rights Act aim of ensuring compliance with international legal obligations[65] and the doctrine of direct effect whether conceived as a form of estoppel against the state or simply a means of ensuring the effectiveness of EU law.[66]

Nevertheless, there are significant overlaps between the tests which make it appropriate that we should consider them together. As Woolf CJ noted in *Poplar Housing and Regeneration Community Association Ltd v. Donoghue*[67], in borderline cases such as this "there is no clear demarcation line which can be drawn between public and private

[62] Oliver, 'What, If Any, Public-Private Divides Exist in English Law?' Emphasis in original.
[63] Campbell goes somewhat further and argues that the tests are not merely inconsistent with each other but are internally incoherent. See Campbell, 'The Nature of Power as Public in English Judicial Review'.
[64] See e.g. Hunt, 'Constitutionalism and the Contractualisation of Government in the United Kingdom'.
[65] See in particular the comments of Lord Mance in *YL* stating that section 6 has a "different rationale, linked to the scope of State responsibility in Strasbourg." (Para. 87.)
[66] See e.g. Craig, 'The Legal Effect of Directives', 356.
[67] [2001] EWCA Civ 595.

bodies and functions… the decision is very much one of fact and degree".[68] It will be helpful to carry out a holistic assessment of the public status of the IWF before reaching a conclusion regarding each of the three tests.

(a) Why look behind the IWF acceptance that it is a "public body"?

> The IWF accepts the principles of the European Convention on Human Rights and undertakes to be governed subject to the Human Rights Act on the basis that it should be treated as a public body.
>
> – IWF Board Minutes, 2001[69]

> The IWF, in accepting that it is subject to the Human Rights Act, is essentially telling a future court that they would be susceptible to judicial review.
>
> – Ian Walden, 2011[70]

As a preliminary matter it might be objected that it is unnecessary to examine the public status of the IWF given the 2001 board resolution that it should be regarded as a "public body [*sic*]" for the purposes of the Human Rights Act.[71] Thus, the argument might run, any person wishing to challenge an action of the IWF could simply rely on that concession, obviating the need to consider the issue in any detail. At first glance this argument has some appeal. Certainly, the existence of this concession would make it substantially easier for anyone wishing to bring an action under the Human Rights Act. But there remain a number of reasons why it is still important to consider the issue.

First, the concession is a narrow one. It applies only to the Human Rights Act. Despite Walden's comments (which carry particular weight from a former board member of the IWF) it does not concede amenability to judicial review *per se*, nor does it accept IWF status as an emanation of the state for the purposes of direct effect.

---

[68] Para. 66.
[69] Internet Watch Foundation, 'Board Minutes 25 April 2001'.
[70] Ian Walden, 'The Future of Freedom of Speech' (presented at the SCL 6th Annual Policy Forum: 'The New Shape of European Internet Regulation', London, 15 September 2011), http://www.scl.org/files/scl_policy_forum_2011/The_Future_of_Freedom_of_Speech_-_Professor_Ian_Waldren.mp3.
[71] The term "public body" does not appear anywhere in the 1998 Act – presumably the reference is to a "public authority" as defined in section 6(3).

Also, the IWF is not bound by this resolution and might later seek to resile from it or cut back its scope. There is a recent example of such an official change of mind in the case of the Office of the Independent Adjudicator. That body in the space of two years went from assuring the public that its decision making was constrained by the possibility of judicial review[72] to arguing before the Court of Appeal[73] that it was not amenable to judicial review in relation to the substance of its work.[74] While it would be undesirable for a body to withdraw a commitment of this sort – particularly if it had been relied upon as part of an argument that further regulation is unnecessary – there would be nothing to prevent it barring some unusual facts which might give rise to an estoppel.

Finally, it was not inevitable that the IWF would adopt this posture and it would be undesirable to allow our analysis to rely heavily on a matter which could easily have gone the other way. The same reasoning applies more generally when we remember that the IWF is just one aspect of an internet system within the UK which depends heavily on self-regulation – if the results of this research are to help shed any light on other aspects of that system (such as the role of Nominet in domain name registration) then we should avoid overreliance on narrow factual circumstances to the exclusion of wider issues of general principle. Not all "self-regulatory" bodies will be so obliging as to admit their public status and it is significant that Nominet, for example, has not made a comparable concession.

[72] '[O]ur decisions are constrained by the possibility of judicial review and other forms of relationship to the court system.' Office of the Independent Adjudicator for Higher Education, 'Annual Report 2004', 2005, 18, http://www.oiahe.org.uk/media/1180/oia-annual-report-2004.pdf.
[73] *R. (Siborurema) v. Office of the Independent Adjudicator* [2007] EWCA Civ 1365.
[74] Mac Sithigh, 'Datafin to Virgin Killer', 18–19.

(b) The "but for" test

> [Speaking of the IWF] If it didn't exist the state would be forced to create it.
> – Andrew Cormack, 2009[75]

One of the most important criteria applied by the courts in determining whether a function is subject to judicial review is counterfactual – if the body in question didn't exist, would the state take on that function? An affirmative answer is not conclusive (witness the decision of the Court of Appeal in *Aga Khan*) but is strong evidence in favour of amenability to review.[76] In *R. v. Advertising Standards Authority, ex p. The Insurance Service*[77] for example the ASA was held to be reviewable notwithstanding that "it has no powers granted to it by statute or at common law, nor... any contractual relationship with the advertisers whom it controls" largely because it was "clearly exercising a public law function which, if the Authority did not exist, would no doubt be exercised by the Director General of Fair Trading".[78]

Applying this to the IWF, it is clear that its role in assessing and adjudicating on complaints of illegal material would, if not performed by it, be taken on by the state. Indeed, while the "but for" test is often criticised as being fictional in nature, the case of the IWF is unusually well suited to it.[79] The IWF was established in direct response to state pressure and the closing words of Chief Inspector French's 1996 letter to all ISPs – "We trust that with your co-operation and self regulation it will not be necessary for us to move to an enforcement policy" – set out the settled intention of the police to step in should the industry not take its own action.[80] This has remained the position since. For

---

[75] Cormack, Telephone interview.
[76] In *R. v. Chief Rabbi of the United Hebrew Congregations of Great Britain and the Commonwealth, ex p. Wachmann* [1992] 1 WLR 1036 Simon Brown J. reviewed the case law following *Datafin* and observed that in every case where non-governmental bodies had been held reviewable "were there no self-regulatory body in existence, Parliament would almost inevitably intervene to control the activity in question".
[77] (1990) 2 Admin LR 77.
[78] At 86.
[79] For criticism of the fictional nature of the test see e.g. Hunt, 'Constitutionalism and the Contractualisation of Government in the United Kingdom'.
[80] Metropolitan Police, 'Pornographic Material on the Internet'.

example, in 2011 the IWF transferred its responsibility for handling complaints of incitement to racial hatred (which had never sat easily within its remit and for which there was little enthusiasm[81]) to the "True Vision" service established by ACPO to centralise reports of hate crime – showing interchangeability between public and private regulators in carrying out the same work.[82]

(c) Public funding and non profit status

In both the Human Rights Act and direct effect case law some weight has been put on whether bodies are intended to be profit making and the nature of any state funding they receive. *YL* in particular has made it clear that payment for services delivered as part a contract on commercial terms with a public body is not in itself a subsidy, while more recently in *Weaver* the receipt of a state subsidy and charitable status were factors which weighed heavily in the finding that a Registered Social Landlord should be treated as a hybrid public authority. Similarly, cases such as *Rolls-Royce* have held that a body is less likely to be treated as an emanation of the state for the purposes of direct effect if it is engaged in an arm's length commercial relationship with the state.

In the case of the IWF these factors would weigh heavily in favour of public status under both categories. From its inception it has been a not for profit organisation and since 2005 it has enjoyed charitable status.[83] While it does "commercialise" the child abuse image database in the sense of charging licensing fees to filtering companies which wish to use it in their products, this has been done primarily on a cost recovery basis.[84] It has

[81] See in particular: Internet Watch Foundation, 'Board Minutes 12 October 2004', 12 October 2004, http://web.archive.org/web/20050308060749/http://www.iwf.org.uk/corporate/page.121.htm; Internet Watch Foundation, 'Board Minutes 27 November 2007', 27 November 2007, http://www.iwf.org.uk/accountability/governance/board-minutes/2007-board-minutes/27-november-2007; Internet Watch Foundation, 'Board Minutes 8 February 2011', 8 February 2011, http://www.iwf.org.uk/accountability/governance/board-minutes/2011-board-meetings/board-minutes-8-february-2011.

[82] Internet Watch Foundation, 'Incitement to Racial Hatred Removed from IWF's Remit'.

[83] Registered charity number 1112398.

[84] See Tony Fagelman, 'Commercialising the CAI Database - Recommendations from the Board and FC Working Group', 10 February 2005, http://web.archive.org/web/20050310190021/http://www.iwf.org.uk/corporate/page.128.277.htm.

since 2000 also consistently received a substantial subsidy from public funds, albeit from the European Safer Internet programmes rather than directly from national government, and in recent financial statements EU grants comprised 34% of its total income.[85]

(d) Statutory powers

Also central to judicial review, the Human Rights Act and direct effect is a consideration of the extent to which a body enjoys direct statutory powers. This takes different forms throughout the case law – from the *Foster* requirement of "special powers beyond those which result from the normal rules applicable in relations between individuals"[86] to the acceptance in *YL* that if a body possesses coercive, disciplinary or regulatory powers then this is a strong indication that it should be treated as a hybrid public authority.[87]

This factor would not be met in the case of the IWF which does not enjoy any *de jure* power of this sort. At most one might point to its recognition by the CPS and ACPO Memorandum of Understanding as a suitable body for reporting illegal images for the purposes of the defence under section 46 of the Sexual Offences Act 2003.[88] However, that MoU does not provide it with any statutory power. Instead, it merely serves as evidence in favour of a defence which might be available to individuals who promptly report CAI to the IWF. Consequently it would most likely not be sufficient to meet the *Foster* requirement of special powers, making it very unlikely that direct effect could be established against it. The decision in *National Union of Teachers* would not be an authority to the contrary – while in that case the school did not enjoy any special powers,

[85] £506,681 of a total £1,487,548: Internet Watch Foundation, 'Financial Statements for the Year Ended 31 March 2011', 2011, https://www.iwf.org.uk/assets/media/accounts/2011%20IWF%20Final%20typesigned.pdf.
[86] Para. 20.
[87] See in particular the comments of Lord Scott at para. 28, Lord Mance at para. 101, and Lord Neuberger at paras. 166-167.
[88] Crown Prosecution Service and Association of Chief Police Officers, 'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003', 6.

it nevertheless was very closely regulated in its activities by the state as part of a statutory framework and also had a formal legal basis in recognition by statutory instrument – both factors which would be lacking in the case of the IWF.

Direct effect aside, however, the *de facto* power exercised by the IWF would still be consistent with amenability to judicial review. An analogy might be drawn with the case of the Press Complaints Commission which has in effect conceded that it is a public authority for the purpose of the Human Rights Act and is amenable to judicial review, notwithstanding its lack of statutory powers.[89] Similarly, the Advertising Standards Authority was found to be reviewable in *R. v. Advertising Standards Authority, ex parte Insurance Services plc*[90] at a time before it enjoyed any statutory recognition.

(e) Integration into regulatory schemes and official oversight

> The IWF... is supported by the Police and CPS and works in partnership with the Government to provide a 'hotline' for individuals or organisations to report potentially illegal content and then to assess and judge that material on behalf of UK law enforcement agencies.
>
> – Crown Prosecution Service & Association of Chief Police Officers, 2004[91]

Given the lack of direct statutory powers of the IWF, it is important to consider whether it should nevertheless be treated as having a public status due to the way it fits into a wider public framework. In *Datafin* one of the key factors cited by Donaldson MR was the way in which the Takeover Panel had been incorporated by central government "into its own regulatory network"; similarly in the context of the Human Rights Act Woolf CJ held in *Poplar Housing* that "[t]he more closely the acts that could be of a private nature

[89] *R. (Ford) v. The Press Complaints Commission* [2001] EWHC Admin 683: "The Commission correctly in my view accepts for the purposes of the present permission application, that it is arguable whether it is a Public Authority for the purposes of Section 6 of the Human Rights Act 1998 ("the HRA") and is amenable to judicial review."

[90] (1989) 133 Solicitors Journal 1545, QBD.

[91] Crown Prosecution Service and Association of Chief Police Officers, 'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003'.

are enmeshed in the activities of a public body, the more likely they are to be public".[92] In *Poplar Housing*, therefore, the Court of Appeal was willing to accept that the housing association was to be regarded as carrying out a public function in managing social housing, particularly as it was so closely associated with Tower Hamlets which had both established it and continued to exercise significant control over its activities.

In this context, the close links between state authorities and the IWF would point to a finding of public status. The description by the CPS and ACPO of the IWF "assessing and judging material on behalf of UK law enforcement agencies" is itself telling and is borne out when we consider the totality of its functions.[93]

At an operational level we see this in the close working relationship between the IWF and the police. UK police forces direct complaints of online illegality in the first instance to the IWF, and in assessing those complaints IWF analysts apply standards of legality which reflect the general law and work on the basis of training from police.[94] Appeals against IWF decisions regarding legality ultimately lie to the police.[95] In 2010 the IWF entered into a "Service Level Agreement" with ACPO which is said to "provide a protocol for the management of investigations into criminal content" hosted in the UK and to guide the interactions between the IWF and its partners in the Metropolitan Police and Ceop.[96]

---

[92] Para. 65. In the same way Bingham MR in *Aga Khan* refers to the Jockey Club as not being "woven into any system of governmental control of horseracing" (at 953).

[93] It is also clear that these links would engage the responsibility of the state before the European Court of Human Rights. See e.g. *MM v. The Netherlands* (2004) 39 EHRR 19 where the Court held that the actions of a private citizen in recording telephone conversations was to be imputed to a public authority where the recording was carried out at the suggestion of the police, using apparatus supplied by police officers and according to their instructions. The fact that the individual would have been free to record such conversations herself was irrelevant – where police "made a crucial contribution to the execution of the scheme" the responsibility of the state was engaged (paras. 36-42). A similar argument can be made that this constitutes a "delegation" of state powers in the same way as was the case in *Woś v. Poland* no. 22860/02, 8 June 2006.

[94] Internet Watch Foundation, 'FAQs Regarding the IWF's Facilitation of the Blocking Initiative'.

[95] Internet Watch Foundation, 'Content Assessment Appeal Process'.

[96] Internet Watch Foundation and Association of Chief Police Officers, 'Service Level Agreement between the Association of Chief Police Officers (ACPO) and the Internet Watch Foundation (IWF)', 5 October 2010, http://www.acpo.police.uk/documents/crime/2010/201010CRIIWF01.pdf.

We also see this at a strategic level, when we consider the structure and accountability mechanisms under which the IWF operates. The current shape of the IWF heavily reflects the 1999 governance review commissioned by the Department of Trade and Industry and the Home Office[97] and periodic audits of the IWF's work indicate a significant element of accountability to the state. For example, the IWF itself described a 2004 audit of its work in the following terms:

> Police Commander David Armond (Met Police) and Professor David Wall (Leeds University) were *commissioned by the Home Office* to inspect and review of our operational procedures, appeals and reinstatement policies *on behalf of the Home Office* [emphasis added].[98]

In the same way a 2011 audit was described by the IWF as being "to [provide] independent reassurance to… Members, Government and parties with a particular interest in IWF affairs" and was carried out by a five person group three of whom were serving members of the Metropolitan Police.[99]

(f) Public or governmental function

In light of the above discussion it is also clear that the single most important *indicium* of public status for the purposes of both judicial review and the Human Rights Act – variously described as the presence of a "public element" or "public duty" (*Datafin*), a "governmental" function (*Aga Khan*) or a "function of government" (*Aston Cantlow*) – is present in this case insofar as the IWF is engaged in closely assisting the law enforcement process. Such a finding would not mean that every action carried out by the IWF should be regarded as public. Under section 6(5) of the Human Rights Act it would not be a public authority in relation to a particular act "if the nature of the act is private". In this case however the actions of the IWF in relation to Cleanfeed – receiving and

[97] KPMG Peat Marwick and Denton Hall, *Review of the Internet Watch Foundation*.
[98] Internet Watch Foundation, 'Chief Executive's Report 26 April 2005', 26 April 2005, http://web.archive.org/web/20051227133042/http://www.iwf.org.uk/corporate/page.141.299.htm.
[99] Gibson et al., 'Inspection of the Internet Watch Foundation'.

adjudicating on complaints of illegality, adding URLs to a block list and distributing that list to ISPs – should all be regarded as public rather than private in their nature.

(g) Policy factors against public status

The majority of factors point in favour of a finding that the IWF should be regarded both as a hybrid public body and as amenable to judicial review. But before reaching a conclusion we should consider whether there are any policy factors which point in the opposite direction.

Autonomy

In *R. v. Chief Rabbi, ex parte Wachmann*[100] Simon Brown J. accepted that as a matter of public policy it would be inappropriate for the court to engage in judicial review of a religious function – in that case, determination of whether a person was morally and religiously fit to hold rabbinical office. The court therefore held that this factor could be taken into account in finding that the function in question should not be regarded as one that had a "truly public character".[101] This reflects a wider policy, one which seeks as far as possible to respect the rightful autonomy of voluntary groups, in particular regarding adjudication on their own internal rules.[102] In the case of the IWF block list, however, this issue would not arise – insofar as the IWF is merely applying the general law, rather than criteria of its own, review by the court would if anything serve to promote its activities and would not undermine any independent discretion.

[100] [1992] 1 WLR 1036.
[101] At 1043.
[102] See also the discussion of 'constitutionalised autonomy' in Black, 'Constitutionalising Self Regulation'.

Alternative remedies

Particularly in the judicial review case law there is often a focus on whether other causes of action would be available to a claimant should a body not be regarded as public and cases such as *Aga Khan* have held that the existence of a private law remedy will weigh against amenability to review. The present case is however more akin to *Datafin* in that the most affected parties – site owners who are wrongfully blocked – are unlikely to have any contractual or other private law remedy against the IWF, making this a factor in favour of a finding of public status.[103]

(h) Conclusion on public status

Laidlaw has suggested that "there is a strong case that the IWF is a public authority under the HRA".[104] With the benefit of a fuller analysis and additional material not available to her – particularly the minutes of the board meeting which undertook to be governed in accordance with the HRA[105] – we can go further again and say that it would be very surprising if the IWF were not found to be a public authority for that purpose and it is also very likely that the IWF would be amenable to judicial review, though probably not subject to direct effect.

(vi) Limits of a finding of public status

This conclusion is, however, still not a complete answer to those critics who charge that the Cleanfeed system is insulated from legal scrutiny or avoids constitutional norms. Instead, it requires us to reframe our question from "does public law regulate the Cleanfeed system?" to "does public law *effectively* regulate the Cleanfeed system?"

---

[103] See chapter 2 for a discussion of the difficulties with a possible remedy in defamation.
[104] Laidlaw, 'The Responsibilities of Free Speech Regulators', 15.
[105] Although the minutes are no longer available on the IWF website cached copies are still available on the Internet Archive Wayback Machine: 'Wayback Machine', *Internet Archive*, accessed 19 October 2013, http://archive.org/web/.

Two particular limitations must be noted. First, we have thus far assessed the position of the IWF only. However, the Cleanfeed system is a diffuse one which also includes ISPs who enjoy considerable autonomy in how they implement the block list. For example, an ISP may choose to use a technology which overblocks, to block additional sites of their own choosing or to provide a deceptive error message to users instead of a stop page.[106] These actions by ISPs will have significant effects in their own right, but being outside the hands of the IWF would escape any judicial scrutiny. A public law remedy would not be available against ISPs which (unlike the IWF) have not conceded that they are bound by the Human Rights Act and do not have the same extensive interaction with the police and other state authorities.

Secondly, MacSithigh has highlighted a more general limitation of an approach based on an *ad hoc* finding of public status for the purpose of judicial review or the Human Rights Act – while such a finding might allow challenges to particular acts of the IWF, it would still leave the IWF outside the scope of other public law control mechanisms such as the Freedom of Information Act 2000.[107] In this he echoes the concerns of many public law writers who caution against a legalistic overreliance on the courts. As Cane has pointed out: "judge made administrative law is only the tiny tip of a huge iceberg of norms by which the performance of public functions is framed, influenced, guided, and regulated."[108]

For these reasons, the availability of judicial review is at best only a partial response to those critics who charge that the Cleanfeed system privatises government censorship.[109] For these critics the complaint is not just that the system might escape judicial oversight (though that is a key element) – in addition they fear that it allows the executive to act

[106] Lahtinen, 'Be Unlimited Causes Stir in Effort of Blocking Child Abuse Images'.
[107] Mac Sithigh, 'Datafin to Virgin Killer'.
[108] Peter Cane, *Administrative Law*, 4th ed. (Oxford: Oxford University Press, 2004), 8.
[109] See e.g. Akdeniz, 'Who Watches the Watchmen?'; Edwards, 'From Child Porn to China, in One Cleanfeed'; Petley, 'Web Control'.

outside parliamentary control while at the same time minimising political accountability as well as public law oversight in a more general sense. The exceptional, expensive and episodic remedy of litigation does little to address these wider points and can act only *ex post*, not *ex ante*. In addition – as we will discuss further in chapter 7 – the individual nature of judicial review and the relatively narrow scope of the rights which might be asserted mean that any litigation is unlikely to be able to tackle the wider structural issues presented by the Cleanfeed system.

4. Positive obligations of the state?

(i) Introduction

> [T]he Convention is mainly concerned not with what a State must do, but with what it must not do; that is, with its obligation to refrain from interfering with the individual's rights. Nevertheless, utilising the principle of effectiveness, the Court has held that even in respect of provisions which do not expressly create a positive obligation, there may sometimes be a duty to act in a particular way.
>
> – JG Merrills, 1988[110]

We have so far considered whether the actions of the IWF and ISPs should be attributed to the state. We now consider a related but distinct issue – even without such a finding, might the state have a duty to intervene to secure Convention rights as against private entities such as the IWF and ISPs? In the context of the ECHR such a duty is termed a "positive obligation" and has historically been a relatively infrequent occurrence: for the most part, the Convention aims to provide a safeguard against interferences by public authorities. Nevertheless, a growing body of Strasbourg case law has been willing to develop positive duties in particular contexts, making it possible that such a duty could be applied in the context of online speech also.[111]

---

[110] John Graham Merrills, *The Development of International Law by the European Court of Human Rights* (Manchester University Press, 1988), 103.

[111] As to positive duties generally see Alistair *R.* Mowbray, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights*, Human Rights in Perspective 2 (Oxford: Hart Publishing, 2004); Brice Dickson, 'Positive Obligations and the European Court of Human Rights', *Northern Ireland Legal Quarterly* 61 (2010): 203.

The wording of Article 10 does not at first seem favourable. By providing that "[t]his right shall include freedom to hold opinions and to receive and impart information and ideas *without interference by public authority*"[112] it is most naturally read as applying to restrictions imposed by the state rather than by private actors. Indeed, one of the leading books on positive obligations from 2004 devotes just two pages to Article 10, reflecting the relatively limited jurisprudence on this point at the time.[113] Despite this, a line of case law has seen the European Court of Human Rights gradually expand a number of positive obligations in relation to freedom of expression, applying the general doctrine of the court that there may be positive obligations inherent even in otherwise negative rights.[114]

(ii) Case law

Our starting point is 2000 when two cases found for the first time that positive obligations could arise on the part of the state under Article 10. In the first of these, *Fuentes Bobo v. Spain*[115], the applicant was a producer with the Spanish public broadcasting company who was dismissed for criticism of the company's management in a critical newspaper article and in remarks on radio programmes. This dismissal was upheld in later litigation. He claimed that his right to freedom of expression under Article 10 had been infringed, while the Spanish government replied that the television company was in form a private company and therefore its actions could not be attributed to the state. Despite this, however, the Court found that the state had a positive obligation in certain cases to protect the right to freedom of expression which extended to safeguarding the right from threats stemming from private persons. Accordingly in this case the court found that the applicant's dismissal was so disproportionate in nature

[112] Emphasis added.
[113] Mowbray, *The Development of Positive Obligations*, 194–195.
[114] *Marckx v. Belgium* (1979) Series A no. 31.
[115] App. no. 39293/98, judgment of 29 February 2000.

that to find it lawful did not meet "a pressing social need" and therefore constituted an interference with his right to freedom of expression.

Shortly afterwards in *Ozgur Gundem v. Turkey*[116] the court expanded on this in the context of a Kurdish newspaper which had been the victim of a series of attacks including the killing of journalists and distributors. The applicants alleged that these attacks were part of an orchestrated campaign by the state. Against this background the Court held that there was a positive obligation on the part of the state to ensure respect for freedom of expression. The failure either to provide adequate protection or to properly investigate the allegations of state collusion meant that Turkey had failed in its obligation to protect the newspaper in its exercise of freedom of expression. In an important paragraph the Court sets out factors to be applied in determining whether a positive obligation arises under Article 10:

> The Court recalls the key importance of freedom of expression as one of the preconditions for a functioning democracy. Genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals... In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States, the difficulties involved in policing modern societies and the choices which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities…[117]

In 2001 *Tierfabriken v. Switzerland*[118] extended the doctrine further again. In this case a private television company which enjoyed a monopoly within Switzerland refused to air an animal rights commercial, regarding it as a form of political advertising banned under national law. Switzerland argued that the company was acting in a private capacity and enjoyed the contractual freedom to refuse advertising as it wished. Nevertheless, the Court accepted that this constituted an infringement by the state. While stating that it did

[116] App. no. 23144/93, judgment of 16 March 2000.
[117] Para. 43.
[118] App. no. 24699/94, judgment of 28 June 2001.

not "consider it desirable, let alone necessary, to elaborate a general theory concerning the extent to which the Convention guarantees should be extended to relations between private individuals *inter se*"[119] the court held that where domestic law made lawful this treatment of the applicant then it had to be regarded as, in effect, a state sanctioned prohibition on political speech.[120] Significantly, the Court rejected the argument of the state that there were "various other possibilities to broadcast the information at issue", finding that the applicant had no ability to reach the entire public other than through the monopoly broadcaster.[121] It also rejected the argument that the finding of a positive obligation amounted to a "right to broadcast" which risked interfering with the rights of the television company, holding that a number of options were open to the state to remedy the breach.[122]

2003 saw an ultimately unsuccessful attempt to expand the doctrine which is of particular relevance for our discussion. In *Appleby v. UK*[123] the applicants were campaigners against a planned development on a public playing pitch. They sought to collect signatures in a shopping centre which served as the local town centre. This had been built by a public entity on public land but was then sold to a private company. The owner of the shopping centre refused permission to the applicants, leaving them with little effective access to locals (though on one occasion a sympathetic shop owner allowed them to set up a stand). The resulting claim in *Appleby* was both direct and indirect. The direct claim was that the state was responsible for the denial of freedom of expression in that it had transferred a public space into private ownership without securing the rights of the public to use the space for communication – by entering into an agreement with the new owner, for example. The indirect claim was that the state had failed in a positive obligation to secure the exercise of freedom of expression within the shopping centre. According to the applicants, therefore: "[a]ccess to the town centre was

[119] Para. 46.
[120] Para. 47.
[121] Para. 77.
[122] Para. 78.
[123] App. no. 44306/98, judgment of 6 May 2003.

essential for the exercise of those rights as it was the most effective way of communicating their ideas to the population".[124]

In rejecting this claim, the Court refused to accept the invitation of the applicants to follow case law from the United States and to designate the shopping centre as a "quasi-public" space in which freedom of expression rights could be asserted. While accepting the general principle that a positive obligation could be asserted against the state in relation to freedom of expression, it held that the property rights of the owner were also in play and declined to create a right of entry to private property for this purpose unless it could be said that a bar on access to property "had the effect of preventing any effective exercise of freedom of expression" or "the essence of the right has been destroyed" – giving the US example of *Marsh v. Alabama* as involving a "corporate town where the entire municipality is controlled by a private body".[125] Here, however, the Court found that the other channels still available to the applicants meant that they had not been "effectively prevented from communicating their views to their fellow citizens" so that their application must fail.[126]

While *Appleby* is the most important decision for our assessment of the IWF, a number of more recent decisions must also be mentioned which show an increasing willingness on the part of the Court to impose positive obligations on member states in relation to freedom of expression.

In the 2008 decision *Khurshid Mustafa and Tarzibachi v. Sweden*, the Court considered the right of an apartment dweller to use an indoor satellite dish as an aspect of the right to receive information. While this case concerned a private law dispute between tenant and landlord regarding the terms of a tenancy agreement prohibiting satellite dishes, the Court held that Article 10 was implicated where, as here, a judicial decision had the effect of preventing a person from receiving transmissions. The Court relied also on the

[124] Para. 34.
[125] Para. 47.
[126] Para. 48.

fact that the applicants had no other means open to them to receive the transmissions in question (news from their native Iraq), holding that the availability of newspapers and radio was not sufficient.[127]

Shortly afterwards in the 2009 decision of *Manole v. Moldova*[128] the Court considered complaints of censorship in a state-owned monopoly broadcaster and held that the failure to put in place laws preventing censorship of journalists in that broadcaster constituted an infringement of their rights under Article 10. According to the Court:

> a positive obligation arises under Article 10. The State, as the ultimate guarantor of pluralism, must ensure, through its law and practice, that the public has access through television and radio to impartial and accurate information and a range of opinion and comment, reflecting *inter alia* the diversity of political outlook within the country and that journalists and other professionals working in the audiovisual media are not prevented from imparting this information and comment. Where the State decides to create a public broadcasting system, the domestic law and practice must guarantee that the system provides a pluralistic audiovisual service.[129]

This decision, as with *Tierfabriken* before it, reflects particular concern on the part of the Court in relation to dominance over the media. While *Manole* relates specifically to a state-owned broadcaster the Court noted that its reasoning applied equally whether censorship is public or private, stating that if "a powerful economic or political group in a society is permitted to obtain a position of dominance over the audiovisual media and thereby exercise pressure on broadcasters and eventually curtail their editorial freedom" this would similarly undermine Article 10.[130] The reference to the State as the ultimate guarantor of pluralism is of particular importance in this context as it signals that legislation may be required to ensure that a plurality of views are represented in the media even though this might restrict the rights of media owners.

[127] Para. 45.
[128] App. no. 13936/02, judgment of 17 December 2009. See also *Centro Europa 7 Srl and Di Stefano v. Italy*, app. no. 38433/09, judgment of 7 June 2012.
[129] Para. 107.
[130] Para. 98.

Most recently, the 2010 decision in *Saliyev v. Russia*[131] has further examined the interaction between property rights and freedom of expression. In this case the applicant had written a newspaper article for a Russian municipal newspaper which alleged corruption in the takeover of an energy company. Shortly after publication the newspaper then withdrew and destroyed all remaining copies. According to the editor (who resigned over the incident) this was due to the fact that certain "untouchable" politicians were named in the article and exerted pressure to have the edition withdrawn.

In finding that an infringement under Article 10 had taken place, the Court considered the extent to which a "right of access" to the press could be said to exist as a positive obligation, balancing ownership rights and editorial considerations. The Court reiterated its earlier rulings that there is no general right of access to the media[132] so that "privately owned newspapers must be free to exercise editorial discretion in deciding whether to publish articles, comments and letters submitted by private individuals or even by their own staff reporters and journalists" and the "State's obligation to ensure the individual's freedom of expression does not give private citizens or organisations an unfettered right of access to the media in order to put forward opinions".[133] The approach may be different "where the press is, *de jure* or *de facto*, in the hands of a monopoly, especially a Government monopoly" where an obligation to provide a pluralistic service may arise.[134] However, in the absence of monopoly power the newspaper could properly take into account wider editorial considerations:

> Even if a newspaper is created to provide a public service it may have its own editorial policy and must not necessarily be neutral in its views. The choice of the material that goes into a newspaper, the decisions made as to limitations on the size and content of the paper and the treatment of public issues and public officials – whether fair or unfair – constitute the exercise of editorial control and judgment. Therefore, if the editor-in-chief had refused to accept the applicant's article when it was submitted for publication, the Court would analyse this situation through the prism of "right of access to the press", which enjoys only minimal, if any, protection under the Convention.[135]

[131] App. no. 35016/03, judgment of 21 October 2010.
[132] See e.g. *Melnychuk v. Ukraine*, app. no. 28743/03, judgment of 5 July 2005.
[133] Para. 52.
[134] Para. 53.
[135] Paras. 52-54.

The Court therefore held that an infringement would not have taken place if the editor had refused the article when it was submitted for publication as the newspaper in question did not have a monopoly over the printed press in the region and was subject to effective competition. However, once the article had been published this was no longer a case of "right of access" and instead became a direct interference with the applicant's right to freedom of expression under Article 10.[136]

(iii) Applying positive obligations to ISPs

Despite the growing case law in this area, no decision of the Court of Human Rights deals specifically with the issue of positive obligations to safeguard freedom of expression online. Nor has any clear position been taken by the other Council of Europe institutions. The risks of filtering by private entities have been highlighted by the Committee of Ministers – notably in the 2008 Recommendation on Respect for Freedom of Expression and Internet Filters[137] and the 2010 Declaration on Network Neutrality.[138] In those documents the Committee of Ministers has urged states to implement safeguards in relation to private filtering, but in each case it has stopped short of asserting that there is a positive obligation under Article 10 which requires that this be done.[139]

Turning to the surprisingly sparse literature, there is no agreement as to whether or how the Court might develop a positive obligation to protect speech against ISP interferences.

---

[136] Paras. 55-61.
[137] Committee of Ministers of the Council of Europe, 'Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters', 26 March 2008, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6.
[138] Committee of Ministers of the Council of Europe, 'Declaration of the Committee of Ministers on Network Neutrality', 29 September 2010, https://wcd.coe.int/ViewDoc.jsp?id=1678287.
[139] The Parliamentary Assembly has also stopped just short of this point: Parliamentary Assembly of the Council of Europe, 'Resolution 1877 on the Protection of Freedom of Expression and Information on the Internet and Online Media', 2012, http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=18323.

At most, there is a consensus that the decision in *Appleby* will be central to such an assessment – but considerable disagreement as to how it should be applied.

The most detailed case against positive obligations is made by Sluijs who examines the issue in the wider context of net neutrality. His claim is that *Appleby* shows a judicial concern for property rights which makes it very unlikely that states would be obliged to regulate private ISP filtering. He asserts that the *Appelby* reasoning – by referring to "destroying the essence" of the right under Article 10 – would justify intervention only if "an ISP blocks all expression on its network" so that it "shut[s] down its operations in a way that no Internet use would be possible".[140] As a result he predicts that "a majority of network management practices by European ISPs will escape the scope of Article 10 altogether".[141] Sluijs also suggests that ISP network management should itself be regarded as protected expression (relying on the decision in *Autronic v. Switzerland*[142] confirming that Article 10 applies to the means of transmission as well as the content) though conceding that in most cases this will be a relatively "low level"[143] form of expressive content.[144]

In the case of the Cleanfeed system, however, there are a number of features which mean that *Appleby* is not an entirely apt authority and Sluijs' comments would often be inapplicable. In the first place, it should be noted that Sluijs is writing in the context of network neutrality generally and focuses on the case of unilateral action by an individual provider. A system such as Cleanfeed – which involves state-prompted concerted action

[140] Sluijs, 'From Competition to Freedom of Expression', 530.
[141] Ibid.
[142] Series A no 178, (1990) 12 EHRR 485.
[143] Sluijs, 'From Competition to Freedom of Expression', 36.
[144] The fact that ISPs have Article 10 rights which may be invoked as against filtering orders has been accepted in the English context by *20th Century Fox v. British Telecom* [2011] EWHC 1981 (Ch) , para. 200 and *EMI v. British Sky Broadcasting* [2013] EWHC 379 (Ch), paras. 94 and 107, though in neither case was the extent of those rights considered in any detail, it simply being asserted that the property rights of the claimants outweighed such rights to the extent that they were engaged. It is interesting to compare C-70/10 *Scarlet Extended v. SABAM* where the Advocate General and the ECJ appear to proceed on the basis that the only freedom of expression rights implicated are those of the users and content providers, with the position of the ISP not being given special treatment. In both contexts this supports the argument that any ISP rights under Article 10 will be relatively weak.

which results in a near universal effect on the population – would raise more significant issues for Article 10 and would be more likely to trigger the plurality concerns which the ECtHR has identified in cases such as *Tierfabriken*. The individual may be able to vote with their feet to avoid traffic management by individual ISPs – however, this market response is unavailable in the Cleanfeed system. The situation here is closer to that in *Manole v. Moldova* where the Court has held that in the case of monopoly or dominant media power the state must intervene so as to guarantee a pluralistic service.[145] Laidlaw therefore argues that once a site is blacklisted by the IWF "the censorship is absolute, destroying entirely the essence of the right [with] no alternative options available".[146] This point is strengthened when we recall that the IWF URL list is also used by search engines such as Google so that a decision to block may prevent a user from learning that a page even exists.

Secondly, the relevance of *Appleby* is weaker than it might at first glance appear. It is notable that the Court in *Appleby* relied on the proprietary rather than expressive rights of the centre owner in justifying the exclusion of the applicants. This reflects the fact, highlighted by van Hoboken, that the Court has not recognised a general Article 10 right *not* to transmit or facilitate speech.[147] In *Saliyev v. Russia,* for example, the Court stressed that the limited nature of the right of access to the press is based largely on the right of newspapers to exercise their own editorial policy and judgment.[148] In the case of ISPs – who are overwhelmingly passive carriers of content created by others which they do not select – there is no equivalent countervailing right. Indeed van Hoboken makes a strong argument that such a right on the part of ISPs would be incompatible with the principle of end-user autonomy which has been developed by the Council of Europe in the Recommendation on Respect for Freedom of Expression and Internet Filters and the

[145] Para. 98.
[146] Laidlaw, 'The Responsibilities of Free Speech Regulators', 26; Joris van Hoboken, 'Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines' (University of Amsterdam, 2012), chap. 6 takes a similar view.
[147] van Hoboken, 'Search Engine Freedom', 145.
[148] Paras. 52-54.

Declaration on Network Neutrality.[149] Consequently, he argues that the nature of the balancing exercise involved must focus on any harm to property rights[150] – something which will be more difficult to show in the context of an ISP than a land owner. It is easy to see that a land owner will suffer a significant limitation of their rights by being forced to facilitate certain uses of their property – it is less easy to see how a network operator could be prejudiced in their proprietary rights by being required to allow users to access certain websites.[151]

In any event, even if ISPs do enjoy expressive rights under Article 10 as regards the blocking of content it will be very difficult for them to argue that this is a strong factor against the existence of a positive obligation when they have long portrayed themselves as mere conduits who simply deliver the content requested by their subscribers.[152]

Third, the balancing test applied in *Appleby* relied heavily on the alternatives available to the applicants and noted that their argument was in essence that they were entitled to use "the easiest and most effective method" even though "[i]t also remained open to them to campaign in the old town centre and to employ alternative means, such as calling door-to-door or seeking exposure in the local press, radio and television".[153] This aspect of *Appleby* is in tension with the Court's rulings in the field of audiovisual media and in both *Tierfabriken* and *Khurshid Mustafa and Tarzibachi v. Sweden* the Court has not accepted arguments that there is no violation of Article 10 where other channels of communication remained open. Instead, the Court has relied on the particular effectiveness and reach of certain types of media to hold that they lack adequate substitutes – which would suggest that internet communications should also be regarded as not having effective substitutes.

[149] van Hoboken, 'Search Engine Freedom', 141.
[150] Ibid., 145.
[151] Any concerns over excessive bandwidth use or network congestion could be accommodated under the balancing test set out in *Ozgur Gundem.*
[152] Daithi Mac Sithigh, 'Regulating the Medium: Reactions to Network Neutrality in the European Union and Canada', *Journal of Internet Law* 14, no. 8 (2011): 6.
[153] Para. 48.

Taking these factors together, it is likely that the Court would find a positive obligation to protect freedom of expression online against private action in the particular context of the Cleanfeed system where quasi-private action has resulted in one body having the ability to make blocking decisions with near-universal coverage of the UK population. Again, however, this would be only a partial response to criticisms of the system. Significant hurdles would face a litigant who sought to assert a positive obligation in this context. Most fundamentally, there would be no cause of action under the Human Rights Act. The essence of any claim would have to be that the state had failed to provide a legislative framework which protected Article 10 rights against private actions by ISPs. Such a claim would, however, be barred by section 6(6) of the Human Rights Act which ensures that the failure to make primary legislation shall not be the basis for an action under the Act.[154] Consequently, while the existence of a positive obligation might inform any other causes of action open to a victim of blocking it would not itself give rise to any basis for a domestic claim.[155] A claim based on a failure to legislate would instead have to be mounted in Strasbourg.

5. Conclusion

We began this chapter by noting the literature which suggested that the Cleanfeed system was questionable in that, *inter alia*, it avoided judicial review and the application of fundamental rights. Our survey of the law has considered these claims in detail and demonstrated that they are only partially true: the mechanisms of judicial review and an action under section 6 of the Human Rights Act are open to those who suffer harm as a result of the operation of Cleanfeed, and it is likely that there is a positive obligation on the part of the state to ensure that Cleanfeed is compatible with the requirements of Article 10 ECHR.

---

[154] Richard Gordon and Tim Ward, *Judicial Review & the Human Rights Act* (Routledge, 2000), 77–78.
[155] As to whether a positive obligation might have indirect horizontal effect by influencing the development of existing causes of action see Gavin Phillipson and Alexander Williams, 'Horizontal Effect and the Constitutional Constraint', *Modern Law Review* 74, no. 6 (2011): 878.

However, to say that the law can examine Cleanfeed is not the same as saying that it can do so *effectively*. We have identified the structural limitations of judicial review and Human Rights Act claims as well as the narrow effect of the positive obligation under Article 10 and we see that in each case the remedies which might be available are restricted in their scope. This point will be developed further in chapter 7 where it will be argued that the specific rights which might be asserted against blocking systems will do little to ensure good governance in their operation.

There is therefore considerable merit to the argument that the IWF and the Cleanfeed system should be brought within public governance norms by legislation.[156] An analogy might be drawn with ACPO which has been the subject of similar controversy – having extensive policing functions while being a private company limited by guarantee, and enjoying a powerful yet largely non-statutory position within policing in the UK as a whole.[157] Despite this anomalous position ACPO has been brought within a number of public law norms – being the subject of judicial review in its operation of the "National Domestic Extremism Database"[158] and made amenable to the Freedom of Information Act in 2011[159] – and it might be argued that the IWF could be treated similarly.

Against that, it should be stressed that neither the positive obligation of the state under Article 10 nor wider concerns about blocking demand that the entire operation of the IWF should be put on a statutory basis or that the IWF should become a conventional public body. Indeed, were this to be done it might very well be counter-productive. We have seen in chapters 4 and 5 that the self-regulatory nature of the IWF has both helped to stave off function creep and has delivered a level of transparency which significantly exceeds that of the Home Office on the same issue, despite the latter being subject to the

[156] Mac Sithigh, 'Datafin to Virgin Killer'; Edwards, 'From Child Porn to China, in One Cleanfeed'.
[157] On the governance of ACPO see e.g. Shami Chakrabarti, 'A Thinning Blue Line? Police Independence and the Rule of Law', *Policing* 2, no. 3 (2008): 367.
[158] *R. (Catt) v. Association of Chief Police Officers* [2012] EWCA Civ 192.
[159] Freedom of Information (Designation as Public Authorities) Order 2011, SI 2598/2011.

Freedom of Information Act. We have argued that these outcomes are largely due to a need to secure industry support – a factor which would be lost if the IWF were to be established on a statutory basis. Instead, alternative means of ensuring good governance should be considered. Korff and Brown, for example, suggest that exemptions from intermediary liability might be made conditional on ISP adherence to principles such as transparency and fair procedures.[160] An approach of this sort, coupled with the existing possibility of judicial review, could deliver significant improvements without the risks associated with establishing a statutory filtering system.

[160] Douwe Korff and Ian Brown, 'Social Media and Human Rights', in *Human Rights and a Changing Media Landscape* (Council of Europe, 2011), 200–201.

Chapter 7 – Regulating Blocking: Governance Standards and Fundamental Rights

1. Introduction

In the last chapter we considered whether the operation of the Cleanfeed system could be regarded as subject to public law for the purposes of applying fundamental rights standards. In this chapter we move on from that threshold question to address the substantive points which it raises regarding the ability of public law to regulate blocking. What standards should apply to internet blocking? To what extent are these already recognised in fundamental rights norms? Would the Cleanfeed system as currently administered meet those standards?

We do so first by surveying the literature which attempts to set standards for the use of internet blocking, considering both academic commentary and recommendations from international bodies. We then turn to English law to consider the ways in which domestic law regulates the use of internet blocking in other contexts. Finally we apply the European Convention on Human Rights to the Cleanfeed system to see to what extent it already embodies standards capable of governing internet blocking and whether the Cleanfeed system would comply with those standards.

It should be noted at the outset that this chapter is necessarily selective. In particular, only the European Convention on Human Rights will be considered. While other fundamental rights instruments such as the International Covenant on Civil and Political Rights are also relevant, the ECHR is the only one which has been transposed into English law and is therefore the most appropriate instrument to consider.[1] Similarly, the focus is on the most significant ECHR rights: freedom of expression under Article 10

[1] The EU Charter of Fundamental Rights also has direct effect insofar as national law implements Union law; however as regards the key provisions for internet filtering – Article 7 on respect for private and family life, Article 11 on freedom of expression and Article 47 on effective remedy and fair trial – it largely parallels the ECHR and therefore will not be considered separately. It should be noted that under Article 52(3) Charter rights take their corresponding ECHR rights as a minimum standard but may also go further to provide more extensive protection.

and to a lesser extent the right to a fair trial under Article 6. While the right to a private life under Article 8 is also implicated by some forms of blocking (as discussed in chapter 2 in relation to data protection) this issue does not appear to arise under the Cleanfeed system as currently implemented and therefore will not be considered. Similarly, issues under Article 13 ECHR regarding the right to an effective remedy will be mentioned only in passing.

2. Identifying standards by which to assess internet blocking

(i) The case for new standards

> In view of the fact that legislation concerning the Internet, which has to be seen against a background of rapidly changing new technologies, is particularly dynamic and fragmented, it is difficult to identify common standards based on a comparison of the legal situation in Council of Europe member States.
>
> – *Yildirim v. Turkey* (2012)[2]

The quotation above from the judgment of the European Court of Human Rights in *Yildirim* notes that internet blocking presents new problems and that there is no consensus as to how it should be evaluated. That decision turned on one particular aspect of filtering – the extent to which it may result in false positives or overblocking of legitimate material – but it exemplifies the wider structural issues which were considered in chapters 4 and 5. Many of these factors, such as inherent opacity and the technological choices embedded in filtering, are individually problematic and would merit special attention in any event – but when taken together the challenges they present multiply.

Reflecting this, there is a growing literature which recognises the difficulties presented by filtering and sets out to develop standards to assess it – standards which, if not

[2] App. no. 3111/10, judgment of 18 December 2012, para. 31.

entirely new, must at least flesh out more general human rights norms.[3] In this section we review that literature with a view to identifying the questions we should ask when assessing the fundamental rights compliance of filtering systems.

(ii) Procedural approaches

There is a wide consensus that procedural guarantees are central to legitimising blocking. This reflects the experience that filtering tends to be a particularly arbitrary and opaque process, so that even in democratic countries "censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or non-existent".[4] Consequently it is not surprising that most commentators see procedural safeguards as the greatest area of concern.

Typical of the procedural proponents is Nunziato, who argues for the international export of the due process values associated with the First Amendment.[5] She suggests that a focus on procedure avoids the contentious substantive question as to *what* should be blocked by each country and leaves open the possibility of reaching international consensus as to *how* blocking should take place. She identifies three criteria to be met for a filtering system to be acceptable: transparency and appealability of the initial decision to block certain material (including notice to the affected parties); limits on the discretion as to what should be blocked; and prompt judicial review in an adversary proceeding before any final decision to block is implemented.[6] Subject to these criteria,

[3] See e.g. Derek Bambauer, 'Cybersieves', *Duke Law Journal* 59, no. 3 (2009): 477; Derek E. Bambauer, 'Orwell's Armchair', *University of Chicago Law Review* 79 (2012): 863; Montero and Van Enis, 'Enabling Freedom of Expression in Light of Filtering Measures'; Callanan et al., *Internet Blocking*; 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): 260; Demeyer, Lievens, and Dumortier, 'Blocking and Removing Illegal Child Sexual Content'; Nunziato, 'How (not) to Censor'.
[4] Sanja Kelly and Sarah Cook, eds., *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media* (Freedom House, 2011), 5.
[5] Nunziato, 'How (not) to Censor'.
[6] Ibid., 1160.

she claims that filtering should be regarded as a desirable tool to ensure that state restrictions on content do not have an illegitimate extraterritorial effect.

A limiting aspect of the Nunziato approach is that it is court-centric – it presupposes that procedural safeguards should primarily be enforced through litigation, notwithstanding the cost and practical difficulties this is likely to create. By comparison, similar work by Bambauer looks to wider mechanisms of control.[7] In general terms, Bambauer agrees that filtering is a desirable governmental tool. His approach is again process focused and looks to four criteria:

> The first criterion is openness: does the country admit to filtering the Internet and describe clearly its rationale for blocking?...
>
> The Framework's second prong is transparency: is a country clear about what material is filtered, and is it specific about the criteria that determine blocking?...
>
> The third criterion is narrowness: how closely does empirical data about what a country actually blocks match the government's description of its censorship?...
>
> The Framework's fourth criterion is accountability: to what degree can citizens influence policymaking on what is censored? What measures or structures push officials to respond to constituents? What recourse is available to content owners who contend they have been blocked erroneously?[8]

As compared with Nunziato, his criteria are significantly more helpful in that they consider a broader set of factors which might constrain filtering – rather than simply looking to the courts, for example, Bambauer also asks to what extent filtering bodies might be subject to other democratic constraints and also considers the way in which civil society might use these metrics to oversee national filtering systems.[9]

[7] Bambauer, 'Cybersieves'; Bambauer, 'Orwell's Armchair'.
[8] Bambauer, 'Cybersieves', passim.
[9] Ibid., pt. IV.

In addition, Bambauer also engages with the question of how these general criteria might be turned into concrete legal requirements. In a detailed piece he has set out five specific requirements on which a US federal filtering statute could be based.[10]

First, Bambauer argues that standing to seek filtering orders should be limited to the US Attorney General, as a means of ensuring that filtering is limited to the most serious cases – ruling out its use in civil matters.[11]

Second, he seeks procedural protections to include notice before the fact in all cases, for both the points of contact for the relevant web pages and also the domain owner, with at least 90 days' notice being given before blocking takes effect. He also includes periodic review within these procedural protections, so that a filtering order should automatically expire after at most one year unless it is shown still to be necessary. To minimise the administrative burden on the state, he suggests that the focus of filtering orders should be on the content itself rather than on location – so that "if a site hosts child pornography images at one location, and faces a filtering order, the government should be able to readily obtain a modified order, without the procedural requirements listed above, if the site's owner moves those images to a new domain name or Web host".[12]

The third requirement is one of heightened proof, requiring "clear and convincing evidence" that the targeted content is illegal – a standard which should apply to each individual page or URL that the government seeks to censor, and a higher standard than the "preponderance of evidence" approach otherwise used in domain forfeiture cases.

Fourth, Bambauer points to the risks of overblocking and would require that any filtering order be limited to the blocking of full URLs only – ruling out the use of DNS or IP address based filtering systems. He would also require that ISPs display block

[10] Bambauer, 'Orwell's Armchair'.
[11] Ibid., 930–931.
[12] Ibid., 932.

pages – ideally including a link to the blocking order itself, but at a minimum explaining why the blocking took place.[13]

Finally, Bambauer would require public funding to reimburse the costs incurred by ISPs in establishing and running blocking systems – with a view to forcing the state to internalise the costs associated with filtering and thereby to minimise its use.[14]

Taken together, Bambauer argues that embedding these requirements in law would legitimate filtering and argues that this type of "hard censorship" (legally mandated censorship) is normatively preferable to existing types of "soft censorship" (by which he means "voluntary" censorship implemented in response to state pressure). In essence, his argument is that this type of filtering is already happening and therefore should be regularised by being put on a proper and more restrictive legal footing. There is some force to this point, but it is also remarkably optimistic in its implicit assumption that a new system would substitute for, rather than simply add to existing filtering.

While there is considerable value in the procedural safeguards which Nunziato and Bambauer propose, a wider problem with their work is that by focusing narrowly on procedure they address only the initial implementation of filtering systems to the exclusion of second-order effects. Both, for example, neglect the knock on effect which normalising filtering might have and the likelihood of function creep once systems have been established. They might reply that their proposals – by placing existing "voluntary" filtering on a formal legal basis – are nevertheless preferable to the status quo. This may well be true at the outset but (as Cleanfeed illustrates) the need to persuade ISPs to participate can help to keep filtering practices in check. Where a legal basis is established and the need for persuasion removed that restraining factor disappears.[15]

---

[13] Ibid., 934.

[14] Ibid., 934–935. Against that, however, once the fixed costs of initially establishing a filtering infrastructure are absorbed the small marginal costs of blocking additional sites through that infrastructure are unlikely to serve as a real deterrent.

[15] In the same way, formalising filtering might lead to technologies which allow circumvention – such as alternative DNS providers or virtual private networks – coming under attack to the detriment of wider

(iii) Assessing proportionality

A key criticism of procedural approaches is that they may obscure the threshold question as to whether blocking is a proportionate response to a particular problem. By comparison, Reidenberg offers a wider framework for considering "technological enforcement instruments" of all kinds.[16] He suggests that those instruments (such as filtering, but also including other tactics such as "electronic sanctions" in the form of denial of service attacks targeting overseas hosts) should be assessed according to the legal authority justifying their use, their intrusiveness, and four further criteria. The relevant passage is worth quoting in full:

> Like other police powers of the state, legal authority is a pre-requisite for the exercise of coercive powers. Each mechanism implicates important civil, political and sovereign rights. As a threshold matter, states must have a legal process in place to authorize the use and choice of technological enforcement tools. For the choice to use a technological instrument or to deploy a specific type of instrument, the basic principle guiding these decisions should be that a state only use the least intrusive means to accomplish the rule enforcement.
>
> Four factors must be considered to determine whether and how to use technologies for rule enforcement. First, a state must weigh the magnitude of any threat to public order. If a threat is significant, a state may be justified in taking more drastic measures, such as an electronic blockade. Second, the urgency of any threat is significant. If continuing rule violations pose imminent danger to a state's public order, a state will have a stronger justification to use more serious measures, such as electronic sanctions. Third, a state must evaluate the effectiveness of the tool. If a tool will not be effective against the rule violation, then the collateral implications may outweigh any justificatory use. Last, a state must consider the ultimate enforcement goal. If the state seeks the cessation of offending activity, the technological enforcement tool may be different than the choice to compel a violator to pay monetary damages.[17]

Here Reidenberg – although generally an advocate of filtering – makes the important point that the initial decision to use filtering must first be justified as a proportionate and effective response to a particular problem. A system which is either disproportionate or

---

internet freedoms. There is an analogy to be drawn with the way in which Digital Rights Management has come to restrict even actions which are explicitly permitted by copyright law – and the way in which circumvention of that technology has been criminalised.

[16] Reidenberg, 'States and Internet Enforcement'.

[17] Reidenberg, 'Yahoo and Democracy on the Internet', 229.

ineffective cannot be legitimised by being adopted democratically and administered in a procedurally fair manner.

(iv) International norms

Turning away from the academic literature we now consider the standards which international organisations have proposed to guide national implementations of filtering systems.

(a) International Telecommunications Union

The first set of standards comes from a perhaps surprising source – the International Telecommunications Union (ITU). While the ITU is not known for advocacy of freedom of expression, it has for some time been involved in promoting filtering as an online child protection measure and in 2009 issued guidelines on the implementation of child abuse material filtering.[18] In these it expresses concern that filtering systems will be ineffective if they lose public support and recommends that the basis on which blacklists are adopted must be clearly set out so that there should be no room for suspicion of government manipulation. It goes on to say that:

> It is important that the list of known sites and Usenet News groups is tested frequently, updated and verified to ensure accuracy. The list should not be cumulative; rather, a multi-layered retesting procedure will help to ensure public confidence in the operation of the list. It is also important to ensure that guidelines on list criteria be transparent. Some countries utilize an independent means of auditing the performance and operation of the list. Lastly, a mechanism should exist to allow for an appeal against inclusion on the list. The only sites on the list should be those which allow the publishing or display of content which is illegal according to the national laws of the country concerned. When a site is blocked, a STOP page should be displayed to the user. This STOP page has the dual function of giving information as to the reason the site was blocked (illegality of content) plus acting as a prevention vehicle that reminds the user/consumer of the illegal nature of the material, as well as the presence of law enforcement agencies online.[19]

[18] International Telecommunication Union, 'Guidelines for Policy Makers on Child Online Protection'.
[19] Ibid., 28–29.

These guidelines might be taken as a starting point for filtering systems, though they remain quite basic in some ways – for example, by assuming that blocking should take place at the level of the site rather than on a per-page basis, and by failing to specify that there should be a legal basis for the filtering system, audits and appeals. That caveat aside, the majority of these standards are already met by the Cleanfeed system as a whole with the notable exception of the stop page which is merely recommended – not required – by the IWF.[20]

(b) Global Network Initiative

The Global Network Initiative (GNI) is a multi-stakeholder group of internet companies, civil society organisations, academics and investors which has, since its launch in 2008, worked on safeguarding freedom of expression and personal privacy against state actions.[21] The participation of Google, Microsoft, Yahoo! and Facebook on the industry side along with groups such as Human Rights Watch, the Center for Democracy and Technology and the Berkman Center for Internet and Society gives it credibility, though it remains hampered by the fact that other internet firms such as Twitter remain outside. Recommendations from the GNI nevertheless have the potential to be significant – where implemented by participating companies they can have a substantial effect on the practice of censorship without any need for domestic legislative action.

The GNI represents a self-regulatory response by industry which seeks to promote accountability and legitimacy. It sets out to do this by adopting a general set of principles[22] supplemented by detailed implementation guidelines.[23] Although the general

[20] Internet Watch Foundation, 'Blocking Good Practice', 2011, http://www.iwf.org.uk/services/blocking/blocking-good-practice.
[21] For an overview see Colin Maclay, 'Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net?', in *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*, ed. Ronald Deibert et al. (Cambridge, MA: MIT Press, 2010).
[22] Global Network Initiative, 'Principles', 2008, http://globalnetworkinitiative.org/principles/index.php.
[23] Global Network Initiative, 'Implementation Guidelines', 2008, http://www.globalnetworkinitiative.org/implementationguidelines/index.php.

principles are somewhat vague, they are fleshed out considerably by the implementation guidelines which amongst other things provide that:

> When required to restrict communications or remove content, participating companies will:
>
> - Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression.
> - Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.
> - Interpret the governmental authority's jurisdiction so as to minimize the negative effect on to freedom of expression…
> - Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression, including the name of the requesting government entity and the name, title and signature of the authorized official…
> - Challenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression…
>
> Participating companies will seek to operate in a transparent manner when required by government to remove content or otherwise limit access to information and ideas. To achieve this, participating companies will, unless prohibited by law:
>
> - Clearly disclose to users the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications.
> - Disclose to users in a clear manner the company's policies and procedures for responding to government demands to remove or limit access to content or restrict communications.
> - Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.

These detailed provisions, to the extent that they are followed by participating companies and others influenced by the GNI, can substantially enhance oversight of filtering systems. By requiring clear legal authority before filtering will be implemented they have the potential to reduce the informal demands and pressures which governments may otherwise use. The commitment to notifying users of how filtering demands are treated and to indicate where content has been blocked is particularly important, both for its own sake and as an instrumental measure which will permit users to identify and challenge wrongful blocking.

One notable limitation of the GNI for our purposes is the way in which it focuses on direct state action and sees "voluntary" measures as outside its remit. Nevertheless, there is some indication that the transparency engendered by the GNI will carry over to these restrictions also. For example, although Google does not regard its participation in the IWF as falling within the scope of the GNI (treating it as a voluntary act on its part rather than a governmental requirement) it applies similar standards of transparency to its use of the URL list and will indicate when search results have been removed as containing child pornography.[24]

(c) Council of Europe

The Council of Europe has been active in developing standards regarding fundamental rights online and, as we have already seen, has moved from an uncritical promotion of self-regulation[25] towards an approach which is more sceptical of the risks which it poses to freedom of expression.[26] It has also specifically addressed the case of filtering and has consistently taken the view that general filtering (as distinct from filtering what children can see) threatens rights under Article 10 ECHR and should be used only in limited circumstances and subject to careful controls. The 2003 Declaration on Freedom of Communication on the Internet first set out this position, providing that:

> Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers. This does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries.
>
> Provided that the safeguards of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the

[24] See e.g. 'Child Pornography Complaint in Google Search', *Chilling Effects Clearinghouse*, 2009, http://www.chillingeffects.org/notice.cgi?sID=1161.
[25] See in particular Committee of Ministers of the Council of Europe, 'Recommendation on Self-Regulation Concerning Cyber Content'.
[26] See e.g. Committee of Ministers of the Council of Europe, 'Recommendation on the Protection of Human Rights with Regard to Search Engines'; Committee of Ministers of the Council of Europe, 'Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services', 2012, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)4.

> removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.[27]

Since then, this principle has been substantially expanded on in the 2008 Recommendation on Measures to Promote Respect for Freedom of Expression and Information with regard to Internet Filters which provides one of the most comprehensive set of guidelines to date.[28]

The starting point is awareness of internet filters, which is described as a key factor to enable users to exercise their fundamental rights. In particular, therefore, the Recommendation requires that users must be "informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering… Moreover, they should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies". The Recommendation then sets out eleven general principles for all types of filters:

> In co-operation with the private sector and civil society, member states should ensure that users are made aware of activated filters and, where appropriate, are able to activate and deactivate them and be assisted in varying the level of filtering in operation, in particular by:
>
> (i) developing and promoting a minimum level of information for users to enable them to identify when filtering has been activated and to understand how, and according to which criteria, the filtering operates (for example, black lists, white lists, keyword blocking, content rating, etc., or combinations thereof);
>
> (ii) developing minimum levels of and standards for the information provided to the user to explain why a specific type of content has been filtered;
>
> (iii) regularly reviewing and updating filters in order to improve their effectiveness, proportionality and legitimacy in relation to their intended purpose;
>
> (iv) providing clear and concise information and guidance regarding the manual overriding of an activated filter, namely whom to contact when it appears that content has been unreasonably blocked and the reasons which may allow a filter to be overridden for a specific type of content or Uniform Resource Locator (URL);

[27] Committee of Ministers of the Council of Europe, 'Declaration on Freedom of Communication on the Internet', 28 May 2003, https://wcd.coe.int/ViewDoc.jsp?id=37031.
[28] Committee of Ministers of the Council of Europe, 'Recommendation on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters'.

(v) ensuring that content filtered by mistake or error can be accessed without undue difficulty and within a reasonable time;

(vi) promoting initiatives to raise awareness of the social and ethical responsibilities of those actors who design, use and monitor filters with particular regard to the right to freedom of expression and information and to the right to private life, as well as to the active participation in public life and democratic processes;

(vii) raising awareness of the potential limitations to freedom of expression and information and the right to private life resulting from the use of filters and of the need to ensure proportionality of such limitations;

(viii) facilitating an exchange of experiences and best practices with regard to the design, use and monitoring of filters;

(ix) encouraging the provision of training courses for network administrators, parents, educators and other people using and monitoring filters;

(x) promoting and co-operating with existing initiatives to foster responsible use of filters in compliance with human rights, democracy and the rule of law;

(xi) fostering filtering standards and benchmarks to help users choose and best control filters.

Of these, points (vi) to (xi) might be regarded as aspirational but points (i) to (v) are quite concrete recommendations of particular importance – as the Wikipedia experience shows, problems with blocking can lie as much in the detailed implementation of a system as the fact of its existence.

The Recommendation goes on to specifically address the use of internet filters by the state and establishes seven additional requirements:

In this context, member states should:

(i) refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;

(ii) guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;

(iii) introduce, where appropriate and necessary, provisions under national law for the prevention of intentional abuse of filters to restrict citizens' access to lawful content;

(iv) ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content;

(v) 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;

(vi) avoid the universal and general blocking of offensive or harmful content for users who are not part of the group which a filter has been activated to protect, and of illegal content for users who justifiably demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes;

(vii) ensure that the right to private life and secrecy of correspondence is respected when using and applying filters and that personal data logged, recorded and processed via filters are only used for legitimate and non-commercial purposes.

In this regard the Recommendation sets particularly high standards for the use of filters by member states. In particular, it makes it clear that the use of general filtering will be a restriction on the right of freedom of expression under Article 10 ECHR and will therefore require both justification under Article 10(2) and compliance with Article 6 in relation to the decision to block (by a "competent national authority" – not a private entity) and availability of review by an independent body. At points (iii) and (v) the Recommendation raises issues often overlooked in the context of filtering, by asking member states to introduce measures to prevent deliberate abuse of filters and to provide for "recourse and remedy" in relation to wrongful blocking.

Significantly, in relation to remedies the Recommendation specifies that this should "include" suspension of filters – suggesting that there should be not merely an appeal mechanism but also provision for compensation in the event of harm suffered by those who are wrongfully blocked. This reflects the right to an effective remedy under Article 13 ECHR which requires that pecuniary damages should in principle be available for an infringement of rights guaranteed under the Convention.[29]

[29] *Peck v. United Kingdom*, application 44647/98, judgment of 28 January 2003, para. 109.

(d) United Nations Human Rights Council

The UN Special Rapporteur on Freedom of Expression, Frank La Rue, in 2011 reported to the UN Human Rights Council on the application to the internet of Article 19 of the International Covenant on Civil and Political Rights.[30] This report found that the "unique and transformative nature" of the internet provided an unparalleled opportunity to promote the right to freedom of opinion and expression, but expressed concern as to the way in which states are restricting information online without any legal basis and delegating censorship to private entities.[31] In relation to filtering, La Rue was "deeply concerned that mechanisms used to regulate and censor information on the Internet are increasingly sophisticated, with multi-layered controls that are often hidden from the public".[32] He went on to note that state use of filtering is often in violation of Article 19 where it is not established in law, is carried out without transparency and without "the intervention of or possibility for review by a judicial or independent body". Consequently he recommended that, at a minimum, states should:

- Provide lists of blocked websites and full details regarding the necessity for blocking each individual site;
- Provide for stop pages notifying users of each affected site; and
- Ensure that "[a]ny determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences".[33]

La Rue also went on to consider blocking of child pornography specifically, noting that it is "one clear exception where blocking measures are justified" subject to the requirements that "national law is sufficiently precise and there are sufficient safeguards

[30] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,*, A/HRC/23/40, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[31] Ibid., para. 75.
[32] Ibid., para. 29.
[33] Ibid., para. 70.

against abuse or misuse to prevent any 'mission creep', including oversight and review by an independent and impartial tribunal or regulatory body".[34] He also endorsed the work of the Global Network Initiative, and similarly stressed that although states are the "primary duty-bearers of human rights", corporations "also have a responsibility to respect human rights" which requires that they should "only implement restrictions… after judicial intervention; be transparent to the user involved about measures taken… and minimise the impact of restrictions strictly to the content involved".[35]

(v) Domestic legislation

Other sources of standards which might be applied to the Cleanfeed system are the few domestic laws which specifically address prior restraint of speech and filtering of internet content. The relevant provisions – section 12 of the Human Rights Act 1998, section 17 of the Digital Economy Act 2010, and section 97A of the Copyright, Designs and Patents Act 1988 – provide us with comparators and evidence as to the safeguards Parliament has considered appropriate.[36]

(a) Human Rights Act 1998, section 12

The first comparator is section 12 of the Human Rights Act 1998. This was introduced in response to media fears during the passage of the Human Rights Bill that it might make the courts too willing to grant injunctions restraining publication of stories alleged

[34] Ibid., para. 71.
[35] Ibid., para. 76.
[36] Excluded from this comparison is section 3 of the Terrorism Act 2006. This does confer a specific legislative authority on police to request removal of online material deemed to contravene that Act. However, unlike the other provisions mentioned it applies only to material hosted in the UK, does not create a filtering power, does not create a binding obligation on ISPs to remove material, and to date has never been used with police policy being to rely on informal requests instead. See Chris Williams, 'Terrorism Chiefs Don't Know What They've Censored Online', *The Register*, 12 November 2009, http://www.theregister.co.uk/2009/11/12/west_terror/; Home Office, 'Response to Freedom of Information Act Request Re Implementation of Terrorism Act 2006 to Internet Activity', *WhatDoTheyKnow*, 23 July 2010, http://www.whatdotheyknow.com/request/implementation_of_terrorism_act#incoming-102379.

to infringe the right to privacy and reflects a historic presumption[37] in English law against prior restraints and for subsequent litigation or prosecution as the preferred means of regulating speech.[38]

It therefore sets a high threshold which must be met before either interlocutory or final relief can be granted and provides:

> (1) This section applies if a court is considering whether to grant any relief which, if granted, might affect the exercise of the Convention right to freedom of expression.
> (2) If the person against whom the application for relief is made ("the respondent") is neither present nor represented, no such relief is to be granted unless the court is satisfied—
> (a) that the applicant has taken all practicable steps to notify the respondent; or
> (b) that there are compelling reasons why the respondent should not be notified.
> (3) No such relief is to be granted so as to restrain publication before trial unless the court is satisfied that the applicant is likely to establish that publication should not be allowed.
> (4) The court must have particular regard to the importance of the Convention right to freedom of expression and, where the proceedings relate to material which the respondent claims, or which appears to the court, to be journalistic, literary or artistic material (or to conduct connected with such material), to—
> (a) the extent to which—
> (i) the material has, or is about to, become available to the public; or
> (ii) it is, or would be, in the public interest for the material to be published;
> (b) any relevant privacy code.
> (5) In this section—
> "court" includes a tribunal; and
> "relief" includes any remedy or order (other than in criminal proceedings).

Although adopted in response to media concerns, the section is of general application and applies to all situations before a court or tribunal where "a relief, if granted, might affect the exercise of the Convention right to freedom of expression". It is clear from the decision of the ECtHR in *Yildirim* that a filtering order is to be regarded as affecting the exercise of the right to freedom of expression under Article 10, and consequently section 12 will be implicated in any proceedings which seek filtering as a remedy. In such cases

[37] Summarised by Thomas Paine in the following terms: 'A man does not ask liberty before hand to say something he has a mind to say, but he becomes answerable afterwards for the atrocities he may utter. In like manner, if a man makes the press utter atrocious things, he be comes as answerable for them as if he had uttered them by word of mouth'. 'Liberty of the Press', in *The Writings of Thomas Paine*, vol. IV (New York: GP Putnam's Sons, 1894).

[38] As reflected in cases such as *Bonnard v. Perryman* [1891] 2 Ch 269 which generally precludes interim injunctions against alleged defamation where the defendant is prepared to stand over their speech by pleading justification.

subsection (2) sets out what is in effect a right to be notified, providing that no relief shall be granted without all practicable steps being taken to notify the respondent unless there are "compelling reasons" why this should not happen. Subsection (3) disapplies the ordinary *American Cyanamid* rules regarding interlocutory relief and provides that no such relief shall be granted unless the applicant meets the more stringent test that it is likely to succeed at trial.[39] Subsection (4) then establishes a further protection by requiring the court to have regard to the Convention right to freedom of expression and (in relation to journalistic, literary or artistic material) also to the extent to which the material has been available to the public and whether it would be in the public interest for the material to be published.

We see therefore that the IWF can in effect exercise a power of prior restraint in a way which would be denied to the courts as a result of section 12. While we argue in chapter 6 that the IWF should be considered as being subject to the Human Rights Act, even treated as a public authority it would nevertheless not fall within the definition of "court" or "tribunal" within section 12 and would not be bound by it.[40] This gives the striking result that the IWF in making decisions on filtering will escape the norms – such as notification and a presumption against prior restraint – which were considered so important by Parliament that they were given special protection as against the courts. This highlights an important limitation of section 12, which arguably should apply whenever a "public authority" and not merely a "court or tribunal" is empowered to grant relief. More generally, however, it also flags a point which recurs throughout this thesis – the blocking powers of the IWF have developed in an *ad hoc* way which does not reflect the standards which Parliament has considered appropriate in other contexts.

The Wikipedia block in 2008 illustrates the practical consequences of this exclusion. In that case, the album cover which was blocked by the IWF was a type of "artistic material". Consequently, had the blocking of the album cover been before a court then

[39] As to which see *Cream Holdings v. Banerjee* [2004] UKHL 44.
[40] "Tribunal" is restrictively defined in section 21 to mean "any tribunal in which legal proceedings may be brought" which would require an adversarial process of some sort.

under subsection (4)(a)(i) one of the factors which the court would be required to consider would be "the extent to which the material has, or is about to, become available to the public". Given that the album in question had been and continued to be widely available, it is difficult to imagine that a court in applying this factor would be inclined to make an order blocking distribution of the image. In much the same way, section 12 prevents restraint of publication before trial unless the court is satisfied that the applicant is "likely to establish" that publication should not be allowed – a standard which is on the face of it higher than the IWF's test of "potentially illegal".[41]

Section 12 is an important provision which, if followed, would demand changes to the practices of the IWF. That said, section 12 was not adopted with filtering in mind and its effects should not be overstated. In particular, the only person entitled to notification under section 12(2) is "the person against whom the application for relief is made". In the case of filtering, this would be the ISP rather than the domain owners or owner of the site to be blocked – leaving them without any notice or opportunity to be heard. Consequently, even full compliance with section 12 would not ensure fair procedures for those most affected by blocking.

(b) Digital Economy Act 2010, section 17

The only English legislation which specifically addresses the question of internet filtering is the Digital Economy Act 2010, making it an especially apt comparator – and one which also tends to cast doubt on the operation of the Cleanfeed system. The 2010 Act owes its genesis to lobbying from the movie and music industries demanding measures to tackle filesharing. The Labour government responded by including this issue within a review by Lord Stephen Carter of the wider "digital economy". The resulting 2009 Digital Britain Report put forward a number of proposals largely reflecting these industry demands.[42] These formed the nucleus of the Digital Economy Bill 2009 which the Labour government then controversially rushed through the wash-

[41] Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative'.
[42] Stephen Carter, *Digital Britain: Final Report* (London, 2009).

up procedure in the dying days of its term. The 2010 Act therefore provides for a number of measures which may be implemented by the Secretary of State for Culture, Media and Sport up to and including disconnection of subscribers and blocking of websites alleged to be infringing copyright.[43]

Blocking is regulated by section 17 of the Act which allows the Secretary of State to make regulations providing for "the granting by a court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright".[44] A blocking injunction is defined to mean "an injunction that requires a service provider to prevent its service being used to gain access to the location".[45]

Before the Secretary of State can bring this power into effect he or she must first be satisfied that (a) online copyright infringement is having a serious adverse effect on businesses or consumers, (b) making the regulations is a proportionate way to address that effect, and (c) making the regulations would not prejudice national security or the prevention or detection of crime. The draft regulations must also be approved by each House of Parliament.[46] In addition, the section is prescriptive about the content of any regulations which might be made. Amongst other things, the regulations must:

- Require that notice be given to the operator of the location (the person having editorial control over material at the location).[47]
- Limit blocking injunctions to situations where a "substantial amount of material" infringing copyright is involved.[48].
- Provide that the court must take account of:

[43] See generally Anne Barron, '"Graduated Response" À l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010', *Journal of Media Law* 3, no. 2 (2011): 305.
[44] Subsection (1).
[45] Subsection (2).
[46] Subsection (11). Further consultation requirements are set out in section 18.
[47] Subsections (6) and (12).
[48] Subsection (4).

- Any steps taken by the service provider or operator to prevent infringement;
- Any steps taken by the copyright owner to facilitate lawful access to the material;
- Any representations made by a Minister;
- Whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests (which would include considerations of overblocking and other collateral damage); and
- The importance of freedom of expression.[49]

This power to implement site blocking was, along with the rest of the Digital Economy Act, the subject of intense criticism when it was adopted. Opposition to the Act brought together civil liberties groups, ISPs and consumer rights advocates alike.[50] While the main focus of the opposition was the possibility of "technical measures" being taken against subscribers alleged to have infringed copyright, the site blocking provisions were also identified as both impractical and a threat to fundamental rights.[51] This continued opposition proved influential with the incoming coalition government and in February 2011 the new Culture Secretary Jeremy Hunt asked Ofcom to assess whether the blocking power under section 17 "could work in practice".[52] In an important report in May 2011, Ofcom concluded that it would not – with a key finding being that "[f]or all blocking methods circumvention by site operators and internet users is technically possible and would be relatively straightforward by determined users".[53] Since that

[49] Subsection (5).
[50] Two ISPs – BT and TalkTalk – went so far as to bring an (unsuccessful) judicial review of the Act: *R. (British Telecommunications plc and TalkTalk Telecom Group plc) v. Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232.
[51] See e.g. James Griffin, 'The Effect of the Digital Economy Act 2010 upon "Semiotic Democracy"', *International Review of Law, Computers & Technology* 24, no. 3 (November 2010): 251; Barron, '"Graduated Response" À l'Anglaise'; Felipe Romero Moreno, 'Unblocking the Digital Economy Act 2010; Human Rights Issues in the UK', *International Review of Law, Computers & Technology* 27, no. 1–2 (2013): 18.
[52] Department for Culture, Media and Sport, 'Ofcom to Review Aspects of Digital Economy Act', *Inside Government*, 1 February 2011, https://www.gov.uk/government/news/ofcom-to-review-aspects-of-digital-economy-act.
[53] Ofcom, *Site Blocking*, 5.

report the coalition has stated that it will not implement section 17 and that it intends to repeal the site blocking provisions of the Digital Economy Act – though, as we shall see, a separate jurisdiction to block websites on copyright grounds has been developed by the courts under section 97A of the Copyright, Designs and Patents Act 1988.[54]

While section 17 of the 2010 Act is now a dead letter, the safeguards which it included are still important as indicators of legislative intention regarding the control of filtering in the only legislation to date to explicitly deal with the issue. It is therefore significant that the Cleanfeed system would not meet any of those safeguards. In particular, Cleanfeed was adopted following informal pressure from the Home Office without any formal Parliamentary input while section 17 requires a prior finding of proportionality and Parliamentary approval of the draft regulations. Similarly, the blocking power which the 2010 Act would vest in a court is in the case of the IWF vested in a private body. The criteria which must be included in any regulations under section 17 are also absent in the case of Cleanfeed – notably the requirements that a website owner must be notified and that risks of overblocking and other collateral damage must be taken into account by the court before a blocking order is made.

(c) Copyright, Designs and Patents Act 1988, section 97A

One of the reasons for the demise of the blocking provisions in the Digital Economy Act was that, by the time it had passed, copyright plaintiffs had already found a new vehicle for their ambitions in section 97A of the Copyright, Designs and Patents Act 1988. This section (inserted in 2003 to implement the Copyright in the Information Society Directive[55]) provides that:

> The High Court… shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright.

[54] Barron, '"Graduated Response" À l'Anglaise'; Romero Moreno, 'Unblocking the Digital Economy Act'.
[55] Directive 2001/29/EC.

Although this section does not explicitly refer to filtering, it has been interpreted in a series of cases to apply to internet access providers and to confer on the High Court the power to make blocking orders cutting off access to particular websites.[56] Crucially, it contains no safeguards or guidance as to how this power should be exercised so that (unlike section 17 of the Digital Economy Act) the development of any controls has been left entirely to judicial discretion.[57]

Newzbin2

The first case to apply this jurisdiction was *Twentieth Century Fox v. British Telecommunications*[58] – better known as *Newzbin2*. In this case the plaintiffs chose BT as a defendant precisely because of its use of the Cleanfeed system, arguing that BT could add the Newzbin2 site (previously found to be infringing) to its blocking list without any great technical difficulty or cost. Arnold J. accepted their arguments that a blocking injunction could be imposed on BT under s.97A, relying in large part on a finding that the cost of implementing blocking using the existing system would be "modest and proportionate". The court rejected arguments that a blocking injunction would amount to a general monitoring obligation contrary to article 15 of the E-Commerce Directive and held that it would be "prescribed by law" notwithstanding the general terms of section 97A and complete lack of guidance in that section. The court also held that an injunction blocking access to the entire site rather than specific URLs was appropriate, holding that any non-infringing uses were *de minimis* and that the

[56] See generally Meale, 'NewzBin2'; Toby Headdon, 'Beyond Liability: Injunctions after L'Oreal v eBay', *Computers and Law* 22, no. 3 (2011): 26; Darren Meale, 'Avast, Ye File Sharers! The Pirate Bay Is Sunk', *Journal of Intellectual Property Law & Practice* 7, no. 9 (2012): 646; Sophie Stalla-Bourdillon, 'Liability Exemptions Wanted! Internet Intermediaries' Liability under UK Law', *Journal of International Commercial Law and Technology* 7, no. 4 (2012): 289.

[57] The only restriction is in subsection (2) which specifies factors to be taken into account in deciding if a provider has "actual knowledge". This has largely been made redundant in any case by the broad interpretation of "actual knowledge" in *Twentieth Century Fox v. British Telecommunications* [2011] EWHC 1981 (Ch).

[58] [2011] EWHC 1981 (Ch).

burden on the plaintiffs of notifying specific URLs would be excessive.[59] Finally, the court applied a remarkably low standard regarding the effectiveness of the order and held that it would be proportionate even if it was circumvented by a majority of users.[60]

In a follow on hearing the court considered the precise form of the order to be granted.[61] Significantly, it rejected the argument that the plaintiffs should indemnify BT against any claims which might arise from third parties who were the victims of overblocking – for example, due to the plaintiffs notifying an innocent IP address or URL to BT in the future. Instead, the court held compliance with the order would provide a complete defence for BT and in any event BT would not incur liability for overblocking:

> It appears unlikely that any subscriber would have a claim against BT for breach of contract anyway, for two reasons. First, BT's broadband service terms incorporate its Acceptable Use Policy. This states that "You must not infringe the rights of others, including… copyright". Thus a subscriber could not claim against BT for being prevented from accessing Newzbin2 for the purpose of obtaining infringing content. Secondly, BT's terms contain a series of limitations and exclusions: paragraphs 7 and 8 in clause 1.1.1.24 provide that "we do not guarantee either the quality of the service or that the service will be available at all times" and "The quality of the… service is dependant on… other conditions or circumstances beyond our control", and paragraph 21 in clause 1.1.1.27 provides that "Unless we are negligent, our only responsibility is to pay you the rental credit as described in paragraph 19", which appears to apply only where there is a continuous total loss of service that persists for more than three days.
>
> As for third parties who are not subscribers, my conclusion is the same. In any event, I find it very difficult to see the basis on which such a third party could have a claim in tort against BT. Counsel for BT suggested that a third party might have a claim for interference with contractual relations, but he did not explain how an order against BT could result in BT interfering with the contractual relations of a third party with a fourth party.[62]

This is a notably weak treatment of possible liability – it does not, for example, address the point that a block page might be defamatory – but is nevertheless important in illustrating the difficulties which would be faced by any person claiming to have been the victim of overblocking. If ISPs can avoid liability for wrongful blocking due to their terms of use or the lack of a contractual relationship with a third party then judicial

[59] Para. 186.
[60] Para. 198.
[61] *Twentieth Century Fox v. British Telecommunications (No.2)* [2011] EWHC 2714 (Ch.).
[62] Paras. 51-52.

review of the IWF would appear to be the only remedy available – and overblocking which is not directly attributable to the IWF would go entirely uncontrolled.

Developing the Newzbin2 jurisdiction

In some ways the *Newzbin2* decision was still very narrow – it granted a blocking order against a single site, which had previously been determined to be infringing on a wholesale basis following *inter partes* proceedings and where the non-infringing content was found to be *de minimis*. Two later cases have, however, pushed the blocking jurisdiction considerably further – aided by the fact that ISPs have chosen not to resist these applications.

The first was *Dramatico Entertainment v. British Sky Broadcasting.*[63] This saw the music industry seek blocking of The Pirate Bay ("TPB") torrent site. Unlike *Newzbin2*, however, there had been no prior proceedings against TPB, the operators of TPB were neither joined nor served in the blocking proceedings, and the ISPs did not appear and were not represented at the initial hearing to determine whether TPB should be blocked. Consequently it is disappointing but perhaps not surprising that the High Court (Arnold J.) entirely failed to consider the possible rights of TPB and its operators under Article 6 ECHR in holding that there was no obligation to notify TPB of the proceedings.[64] A later judgment in those proceedings did accept that the court was obliged to consider whether a blocking order was proportionate as regards parties not before the court:

> where (as here) the terms of the orders have been negotiated between the parties, and those parties are professionally represented, then it may be assumed that the orders are proportionate as between the parties; but it does not necessarily follow that they are proportionate as between the Claimants and users of the Defendants' services. Accordingly, it is the duty of the Court not simply to rubber stamp the terms agreed by the parties, but independently to consider the proportionality of the proposed orders from the perspective of individuals affected by them who are not before the Court. [65]

[63] [2012] EWHC 268 (Ch).
[64] Paras. 9-15.
[65] *Dramatico Entertainment v. British Sky Broadcasting (No. 2)* [2012] EWHC 1152 (Ch), para. 11.

That obligation to consider proportionality, however, illustrates a fundamental inconsistency in the court's reasoning – how can the court assess the impact on those not before the court without affording them an opportunity to be heard? If taken seriously this would require – contrary to the earlier ruling – that the affected parties should be notified and given the opportunity to make submissions.[66]

In 2013 the blocking jurisdiction was extended further again in *EMI v. British Sky Broadcasting.*[67] In this case the music industry sought blocking orders against three different torrent sites – KAT (Kickass Torrents), H33T and Fenopy. As in *Dramatico Entertainment v. British Sky Broadcasting* the court (Arnold J.) held that there was no obligation to serve the proceedings on the sites to be blocked.[68] There was, however, a significant difference between the cases. In *Dramatico* the site to be blocked was The Pirate Bay which, as the name suggests, was an avowed proponent of filesharing. There was, therefore, no real issue as to whether it was infringing. The three sites at issue in *EMI v. British Sky Broadcasting*, however, purported to respect copyright and to comply with take down notices. Consequently it is striking that the court in *EMI v. British Sky Broadcasting* was prepared to make adverse findings of fact on what would have been contested issues had the sites been joined as parties – and was prepared to make a blocking order in what was in effect an *ex parte* proceeding.[69] As before, no consideration was given to the possible Article 6 ECHR rights of the sites.

Assessing the section 97A case law

It is not surprising that copyright plaintiffs have not felt the need to push for implementation of the blocking provisions in the Digital Economy Act when the section

[66] This was a case where the approach taken in *Golden Eye v. Telefonica* [2012] EWHC 723 (Ch) would have been appropriate. In that *Norwich Pharmacal* application against an ISP by a copyright plaintiff Arnold J. himself recognised the limitations of what are in substance *ex parte* applications by allowing Consumer Focus to intervene in the proceedings for the purpose of representing the interests of the intended defendants. It is unfortunate that he did not take the same approach in this case.
[67] [2013] EWHC 379 (Ch).
[68] Para. 10.
[69] The ISPs again did not appear and were not represented.

97A case law has already given them everything that they could have hoped for by way of blocking, minus the safeguards which the Digital Economy Act regulations would have imposed. In effect, therefore, a parallel jurisdiction has been developed by the High Court which is now the only filtering power exercised by the English courts.

Despite this, however, it is of relatively little value in assessing the Cleanfeed system. It does show a judicial willingness to adopt blocking as a remedy, even if it is capable of being circumvented by a majority of users. However, it is focused on the rights of ISPs and mandatory rather than voluntary blocking. Consequently there is relatively little attention given to issues such as overblocking which affect parties who were not represented before the court, with no consideration at all of the fundamental issue of fair procedures under Article 6 ECHR. In addition, the finding that the section 97A power is "prescribed by law" was made prior to the decision of the ECtHR in *Yildirim* and will have to be revisited in light of that decision.

It should also be noted that these blocking orders present fundamental transparency issues. While there are public judgments in the initial cases discussed above, subsequent cases have seen blocking orders issued without any written judgment being available.[70] The process by which plaintiffs have additional sites blocked under existing orders is also opaque. Under the order granted in *Newzbin2* (and presumably, though we have no way of knowing, in later orders also) the ISP is required to block the site itself and also "any other IP address or URL whose sole or predominant purpose is to enable or facilitate access to the Newzbin2 website".[71] The effect of this is to confer a power on the plaintiffs to notify additional IP addresses and URLs to the ISPs to be blocked. This is intended to deal with mirrors or alternative URLs adopted solely to circumvent the blocking order, but creates a substantial risk that innocent sites will be wrongfully

[70] 'UK ISPs Block Huge Movie Site Movie2K, Proxy Immediately Unblocks', *TorrentFreak*, 20 May 2013, http://torrentfreak.com/uk-isps-block-huge-movie-site-movie2k-proxy-immediately-unblocks-130520/.
[71] [2011] EWHC 1981 (Ch), para. 56.

blocked in an invisible process without any prior judicial scrutiny. The Article 6 ECHR point is all the more acute in this context.

3. Blocking and the European Convention on Human Rights

Having identified standards which might be used to assess filtering systems we now turn to ask whether in light of those standards the IWF and the Cleanfeed system as a whole can be said to comply with fundamental rights guarantees under the ECHR as implemented by the Human Rights Act.

(i) Standard of review: margin of appreciation and judicial deference

Before we look to the substance of the system we should first mention the applicable standard of review. It is true that the ECtHR will afford a margin of appreciation to national laws in general, with a wider margin regarding questions of freedom of expression in the area of morals.[72] However this is rooted in the notion that the requirements of morals vary from place to place so that state authorities are "in principle in a better position than the international judge to give an opinion on the exact content of those requirements as well as on the 'necessity' of a 'restriction' or 'penalty' intended to meet them".[73] This principle is therefore one which applies only in Strasbourg – it does not apply to review by a domestic judge.[74]

[72] *Handyside v. United Kingdom*¸ app. no. 5493/72, judgment of 7 December 1976; *Müller v. Switzerland*, app. no. 10737/84, judgment of 24 May 1988.
[73] *Handyside*, para. 48.
[74] This point is discussed in some detail by Fenwick and Phillipson, who argue that English judges must also 'strip away' the margin of appreciation in Strasbourg judgments which are relied upon as domestic precedents if they are not to smuggle the margin of appreciation into domestic decision making. '[T]he courts have paid lip service to the notion that the margin of appreciation has no role to play in domestic decision-making. In nearly every case… the courts have then gone on to apply Strasbourg case law heavily influenced by that doctrine, thus precisely applying the margin of appreciation. On occasions, courts have then gone on to pile on top of it a further layer of deference – the discretionary area of judgment.' Fenwick and Phillipson, *Media Freedom under the Human Rights Act*, 146.

A different question would therefore arise if an English judge were faced with a claim against the IWF regarding Cleanfeed: to what extent should judicial deference be given to its actions? Following the adoption of the Human Rights Act there has been considerable discussion of the appropriate judicial deference to be given either directly to Parliament or indirectly to public authorities exercising powers conferred by Parliament, reflecting the democratic accountability of these bodies.[75] In relation to the IWF, however, no such deference would be appropriate – although a public authority for the purposes of the Human Rights Act it is neither created by nor answerable to Parliament and lacks any such democratic accountability. At most one might say that a court might attach particular evidential weight to the views of the IWF in areas where it has special expertise – but this would fall short of any deference as a matter of principle. Consequently the courts in reviewing the acts of the IWF will have to make an independent and hard-edged judgment as to whether those acts are compliant with the ECHR and the Human Rights Act.

(ii) Article 10

The first obligation to be considered is the right to freedom of expression and information under Article 10 which provides that:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for

[75] See e.g. Francesca Klug, 'Judicial Deference under the Human Rights Act 1998', *European Human Rights Law Review*, 2003, 125; Ian Leigh, 'The Standard of Judicial Review after the Human Rights Act', in *Judicial Reasoning under the UK Human Rights Act.*, ed. Helen Fenwick, Gavin Phillipson, and Roger Masterman (Cambridge: Cambridge University Press, 2007); David Keene, 'Principles of Deference under the Human Rights Act', in *Judicial Reasoning under the UK Human Rights Act*, ed. Helen Fenwick, Gavin Phillipson, and Roger Masterman (Cambridge: Cambridge University Press, 2007).

the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

(a) Existence of an interference

Child pornography as expression within Article 10

A preliminary question is whether child pornography constitutes a type of expression within Article 10 ECHR or whether – as the US Supreme Court held in *New York v. Ferber*[76] – child pornography involving actual minors should be viewed as unprotected speech. In the first case to consider the issue the ECtHR has recently accepted that the possession and distribution of child pornography can amount to an exercise of freedom of expression, so that the requirements of Article 10(2) must be met in relation to its criminalisation.

In *Karttunen v. Finland*[77] the applicant was a Finnish artist who exhibited in a gallery a work which included hundreds of sexually explicit photographs of children, downloaded from the internet. She argued that she included these images to raise awareness of the easy accessibility of child pornography. She was convicted of possessing and distributing sexually obscene pictures depicting children (although no sanction was imposed on her) with the Finnish courts taking the view that her right to freedom of expression was outweighed by the need to protect children against sexual abuse and the violation of their privacy. When she brought the matter to the Court in Strasbourg the Court accepted that her conviction, even where no penalty was imposed, "constituted an interference with her right to freedom of expression, as guaranteed by Article 10(1) of the Convention".[78] Nevertheless, the Court went on to rule that her application was manifestly ill-founded, holding that the national courts had correctly ruled that the

[76] 458 US 747 (1982).
[77] App. no. 1685/10, judgment of 10 May 2011.
[78] Para. 17.

offence was justified by "the need to protect children against sexual abuse as well as against violation of their privacy".[79]

This holding is significant for our evaluation of the Cleanfeed system in that it precludes any argument that child pornography is categorically outside the protections of Article 10 – instead measures attempting to restrict child pornography must still be assessed under Article 10 in the ordinary way.

Filtering as a prior restraint

In *Yildirim* the ECtHR accepted that the blocking orders imposed by the Turkish judicial system, insofar as they were given prior to a full ruling on the merits, constituted a prior restraint both in relation to the targeted site and also the others affected by the overblocking in that case.[80] While Article 10 does not of itself preclude prior restraints the Court has long accepted that "the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court" particularly given the perishable nature of news stories and other topical material which might be blocked.[81] By analogy, the Cleanfeed system would similarly constitute a prior restraint. Indeed this reflects the IWF's own view that they merely decide on *potential* illegality on the basis that "a definitive legal judgement is a matter for the courts".[82]

Filtering as an artificial border

It should also be noted that any national filtering system calls for special scrutiny as being in "direct conflict" with the wording of Article 10, which guarantees the right to

[79] Paras. 6 and 25.
[80] Para. 52.
[81] *Ylidirim*, para. 47 citing *Sunday Times v. United Kingdom* Series A No 30, (1979-80) 2 EHRR 245.
[82] Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative'.

freedom of expression "regardless of frontiers".[83] As the Court put in *Cox v. Turkey*, the starting point is that:

> Article 10 rights are enshrined "regardless of frontiers" and… no distinction can be drawn between the protected freedom of expression of nationals and that of foreigners. This principle implies that the Contracting States may only restrict information received from abroad within the confines of the justifications set out in Article 10(2).[84]

A tripartite right: speaker, intermediary and user

Another important aspect of Article 10 is that it conceptualises freedom of expression as a right involving three parties – encompassing the freedom to speak, the freedom to receive information and also the freedom of those who facilitate speech. In an internet context this means that intermediaries are also protected by the right, as can be seen from the recent decision in *Neij and Kolmisoppi v. Sweden.*[85] In that case the applicants had been involved in the running of The Pirate Bay file sharing site and were convicted of complicity to commit crimes in violation of the Copyright Act. They claimed that their convictions amounted to an interference with their Article 10 rights. While their claim was ultimately declared ill-founded and inadmissible, the Court did accept their preliminary point that Article 10 was implicated by legislation which criminalised their actions as intermediaries.

The Court noted first the well established rule that "Article 10 applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information". Consequently, the Court held that Article 10 applied to the applicants insofar as they "put in place the means for others to impart and receive information" so that any interference with the running of the site would breach Article 10 unless it met the conditions set out in Article 10(2).

---

[83] *Ylidirim* para. 67.
[84] *Cox v. Turkey*, app. no. 2933/03, judgment of 20 May 2010.
[85] *Neij and Sunde Kolmisoppi v. Sweden,* app. no. 40397/12, decision of 19 February 2013.

This finding means, in the context of Cleanfeed, that we must consider the impact of filtering on at least three groups: the users who are prevented from viewing a page, those with editorial responsibility for a page, and the intermediaries who host or otherwise facilitate access to a page. We could also add a fourth group to this list, consisting of other content providers who may suffer collateral damage from a blocking system. Given the judgments in *Karttunen* and *Yildirim* it is clear that the operation of the Cleanfeed system will constitute an interference with the rights of members of all these groups, which requires that we consider whether that interference can be justified in accordance with the requirements of Article 10(2).

(b) Legitimate aim

Having determined that there is an interference, we next ask whether it serves one of the purposes identified in Article 10(2). For the most part this is a straightforward question. Certainly the Cleanfeed system can be said to aim at "the prevention of disorder or crime" by preventing the further creation and possession of illegal images, "the protection of the reputation or rights of others" by preventing children from being further victimised by the dissemination of their images and also "the protection of morals"[86] by preventing accidental exposure of internet users to these images.[87]

This is supported by the decision in *Karttunen* where the Court accepted the criminalisation of CAI as unproblematic without any independent analysis, merely deferring to the national court's findings that the law "was intended to protect morals as well as the reputation or rights of others" and was therefore "mainly based on the need

[86] See in general Christopher Nowlin, 'The Protection of Morals under the European Convention for the Protection of Human Rights and Fundamental Freedoms', *Human Rights Quarterly* 24, no. 1 (2002): 278 et seq.

[87] As to accidental exposure see *Perrin v. United Kingdom*, app. no. 5446/03, decision of 18 October 2005, where the Court held that a conviction for obscenity was appropriate notwithstanding the applicant's argument that "websites are rarely accessed by accident and normally have to be sought out by the user", holding that "the web page in respect of which the applicant was convicted was freely available to anyone surfing the internet".

to protect children against sexual abuse as well as violation of their privacy but also on moral considerations".[88]

Indeed the recent judgment of the Court in *KU v. Finland*[89] strongly suggests that prevention of the distribution of CAI is not merely a legitimate aim but would itself be a positive obligation on the state. In *KU* the applicant was a 12 year old child whose contact details were posted on a dating site along with a statement suggesting that he was seeking older men. As a result he received an email soliciting him. A police investigation was launched but was hampered by a lack of any legal basis on which to compel the internet service provider to disclose information identifying the person who placed the advertisement. Consequently no prosecution was brought, prompting the applicant to complain that his rights under Article 8 had been infringed. The Court accepted this argument, holding that:

> States have a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution. Where the physical and moral welfare of a child is threatened such injunction assumes even greater importance… Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives.[90]

This reasoning would apply *a fortiori* to protection from further distribution of images of abuse.[91]

It should be noted, however, that these approaches presuppose that the material in question involves images of actual children. If, for example, the Cleanfeed system were

[88] Para. 22.
[89] App. no. 2872/02, judgment of 2 December 2008.
[90] Para. 46.
[91] Sunde suggests that this reasoning would extend further to a positive obligation to use filters for the purpose of blocking child abuse images: Inger Marie Sunde, 'Enforcing Legal Protection against Online Violation of Privacy', in *Nordic Yearbook of Law and Informatics 2010–2012: Internationalisation of Law in the Digital Information Society*, ed. Dan Jerker B Svantesson and Stanley Greenstein (Copenhagen: Ex Tuto Publishing, 2013), http://brage.bibsys.no/politihs/bitstream/URN:NBN:no-bibsys_brage_40052/1/enforcing_legal_protection.pdf.

to be extended to cover virtual child pornography such as cartoon images then it would not necessarily follow that such a restriction would serve a legitimate aim for the purposes of Article 10. We may compare the US Supreme Court decision in *Ashcroft v. Free Speech Coalition*[92] which struck down a provision of the Child Pornography Prevention Act of 1996 dealing with "virtual" child pornography on the basis that it criminalised speech which "records no crime and creates no victims by its production".[93]

(c) Prescribed by law

> All restrictions on Convention rights have to be justified by reference to some law. They cannot be invented out of thin air or imposed by the authority as a matter of brute executive force.
>
> – Conor Gearty, 2004[94]

The next and more difficult question is whether the interference created by the Cleanfeed system can be said to be "prescribed by law". The most well known treatment of this concept was given in *Sunday Times v. United Kingdom*[95] where the Court held that in addition to requiring a legal basis it also imposes requirements regarding the quality of the law. First, "the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case". Secondly, "a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[96]

This has been supplemented in *Ekin Association v. France*[97] which held that in relation to prior restraints "a legal framework is required, ensuring both tight control over the

[92] 535 US 234 (2002).
[93] See generally Simpson, 'Controlling Fantasy in Cyberspace'.
[94] Conor Gearty, *Principles of Human Rights Adjudication* (Oxford University Press, 2004), 74.
[95] Series A No 30, (1979-80) 2 EHRR 245.
[96] Paras. 47 and 49.
[97] App. no. 39288/98, judgment of 17 July 2001.

scope of bans and effective judicial review to prevent any abuse of power".[98] In that case a law which gave the Minister of the Interior a wide-ranging power to ban foreign publications by administrative action was held to be contrary to Article 10. Central to this finding were the facts that bans took place prior to any hearing while the only judicial review available was limited in its scope (rather than considering the merits) and was not automatic but required the publisher to apply to the courts.[99] Consequently, the Court took the view that the judicial review procedures in place provided "insufficient guarantees against abuse".

The decision in *Ekin Association* was applied in *Yildirim v. Turkey*[100] in which the ECtHR considered for the first time the question of internet filtering. *Yildirim* challenged a decision of a Turkish court which issued an order blocking access to the entirety of the Google Sites service in an attempt to prevent access to a single site critical of Atatürk. The court had initially issued an order which was limited to the offending website. That order was sent to the state Telecommunications and Information Technology Directorate (the TİB) for execution. The TİB however lacked the technical capability to block this particular site and therefore advised the court that it would be necessary to block all material hosted on the subdomain sites.google.com. The court varied the order accordingly.[101]

The blocking order therefore blocked a vast number of entirely unrelated sites, including one belonging to a Turkish PhD student who found himself unable to access his own site. He claimed that this measure breached his right to freedom to hold opinions and to receive and impart information and ideas under Article 10. The ECtHR found at the outset that this overblocking constituted an interference with his rights notwithstanding that the order intended to target a third party site and that it was relatively limited in its

[98] Para. 58.
[99] Paras. 58-65.
[100] App. no. 3111/10, judgment of 18 December 2012.
[101] Paras. 8 to 12.

effects.[102] Consequently the Court considered whether the measure could be said to be "prescribed by law".

Under Turkish law, statute provided that the court could order the blocking of access to "Internet publications where there are sufficient grounds to suspect that their content is such as to amount to... offences".[103] The law in turn specified the eight class of offences for which such orders could be issued.[104] However, the ECtHR nevertheless found that the blocking in this case was not prescribed by law in that neither the applicant's site nor Google Sites *per se* fell within the scope of this section, while the law had "no provision for a wholesale blocking of access such as that ordered in the present case" and did not authorise "the blocking of an entire Internet domain like Google Sites which allows the exchange of ideas and information".[105] The Court was also critical of the role of the TİB as an administrative body in widening the blocking order, noting that "the TİB could request the extension of the scope of a blocking order even though no proceedings had been brought against the website or domain in question and no real need for wholesale blocking had been established".[106]

The ECtHR then referred to *Ekin Association* in reiterating the need for "tight control" and "effective judicial review" in the case of prior restraints, and found that these elements were missing. In relation to judicial review of prior restraints the Court held that this required "a weighing-up of the competing interests at stake... designed to strike a balance between them" and also "a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression". Both were absent here, where national law did not provide for any balancing test and where the domestic courts had simply acted on the recommendation of the TİB without considering the proportionality of the blocking measure and its collateral impact on

[102] Paras. 53 to 55.
[103] Para. 61.
[104] Para. 15.
[105] Paras. 62.
[106] Para. 63.

internet users. Consequently the Court held that the measure "did not satisfy the foreseeability requirement under the Convention and did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society".[107]

This is a judgment of fundamental importance for internet blocking laws generally in its treatment of overblocking. The approach of the Turkish authorities was, in effect, to assume that a degree of overblocking was implicitly permitted to achieve the blocking explicitly authorised by statute. The ECtHR has now entirely rejected that approach. While the judgment is not a model of clarity, the key holding appears to be that any overblocking must itself be explicitly authorised by a law including safeguards to ensure that the extent of the overblocking is both necessary and proportionate. Otherwise, the collateral damage caused by a blocking order will not be "prescribed by law".

Self-regulatory systems as "prescribed by law"

> Independent courts of law are the guarantors of justice which have a fundamental role to play in a state governed by the rule of law. In the absence of a valid legal basis, the issuing of blocking orders and decisions by public or private institutions other than independent courts of law is therefore inherently problematic from a human rights perspective.
>
> – Yaman Akdeniz, 2011[108]

Can Cleanfeed – as a self-regulatory system with no statutory underpinning – be said to be prescribed by "law"? The leading decision on this issue is *Barthold v. Germany*[109] in which the applicant was a veterinary surgeon who had been disciplined under rules of conduct adopted by a non-state professional body. His claim that these rules did not constitute "law" was rejected by the ECtHR, which held that it was sufficient that there had been a "parliamentary delegation" to the professional body and that the rules needed approval by the state before they took effect. This approach will require formal state

[107] Para. 67.
[108] Yaman Akdeniz, *Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States* (Organisation for Security and Cooperation in Europe, 2011), 24, http://www.osce.org/fom/80723.
[109] (1985) Series A no. 90, (1985) 7 EHRR 383.

involvement in the rule making process before a restriction can be said to be prescribed by law. In particular, *Barthold* appears to set a minimum standard of state delegation of rulemaking and involvement in the oversight of rules before these can be said to be "law" for the purposes of Article 10(2).[110] The Cleanfeed system clearly could not meet this standard and therefore would not be "prescribed by law" in this sense.

There has been one domestic case applying *Barthold – R. v. Advertising Standards Authority, ex p. Matthias Rath BV*[111] – which gave it a far less demanding interpretation. In that case Turner J. held that a ruling under the Advertising Standards Authority (ASA) Code of Practice should be regarded as "prescribed by law", notwithstanding that the ASA was a self-regulatory body established by the industry itself and lacking a statutory basis. It was held sufficient that there was indirect recognition for the ASA in legislation given the "statutory underpinning" provided by the Control of Misleading Advertisements Regulations which recognised the desirability of self-regulatory controls.[112] However, the decision in *Matthias Rath* would still not permit the Cleanfeed system to be regarded as "prescribed by law". The permissive approach in that case – even if a correct application of *Barthold* – would not be appropriate following the decision in *Yildirim* which specifically requires, in the case of blocking, that there must be "a legal framework… ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power".[113] The absence of these factors would mean that Cleanfeed would still not be prescribed by law even if we could make the case that it was somehow indirectly recognised.

[110] See e.g. Hans-Bredow-Institut, *Study on Co-Regulation Measures in the Media Sector: Final Report* (Hamburg: University of Hamburg, 2006), 151, http://ec.europa.eu/avpolicy/docs/library/studies/coregul/final_rep_en.pdf.
[111] [2000] EWHC Admin 428.
[112] SI 1988/915.
[113] Para. 64.

Contractual terms as a legal basis

Callanan *et al.* have suggested that ISP terms of use might provide a legal basis for filtering systems – subject to the requirements that the user would have to "openly consent" to such terms, that the user would have the ability to make a free choice whether to accept, and that the legality of the terms would remain subject to review under e.g. the Unfair Contract Terms Directive.[114] This in some ways echoes our discussion in chapter 5 regarding the ability of user consent to legitimise a self-regulatory system, but it is problematic when applied to state involvement. There is no support in the caselaw for this proposition, which would treat private law as a substitute for the public law basis which the ECtHR requires. It is also inapt in the stage at which it applies – if a person freely consents to filtering then it would be more logical to say that there is no interference with that person's right than to say that there is an interference which is justified as having a legal basis. In any event, however, it is clear that this argument could not apply in the Cleanfeed system where the UK government has deliberately acted to deny users such a choice.

Accessibility and predictability

Would the Cleanfeed system meet the requirements established in *Sunday Times*, *Ekin Association* and *Yildirim* in relation to the accessibility and precision of the norms restricting speech? Some elements of the system might. The criteria used by the IWF in determining whether URLs should be added to the CAIC list are public and simply mirror the underlying law criminalising CAI.[115] There is, following the Wikipedia incident, an element of discretion where blocking images might create specific risks – this is, however, significantly circumscribed and much less open-ended than other discretions which have been upheld by the ECtHR.[116]

[114] Callanan et al., *Internet Blocking*, 183.
[115] Internet Watch Foundation, 'IWF URL List Policy and Procedures'.
[116] Compare e.g. *Tolstoy Miloslavsky v. United Kingdom* (1995) Series A no. 316, (1995) 20 EHRR 442 where wide jury discretion in relation to defamation damages was upheld as compatible with Article 10.

Despite this, however, the Cleanfeed system as a whole would fail when considered against the requirements in *Ekin Association* and *Yildirim* that prior restraints are permissible only if there is "a legal framework… ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power". The absence of any judicial involvement, in either the decision to block or the assessment of the proportionality of a particular type of block, fails to meet the standards set out in those cases. In addition, while the IWF does recommend that blocking take place at the full URL level, to the extent that ISPs remain free to block at an IP or DNS level then arbitrary overblocking is still likely to take place in the precise manner condemned by the ECtHR in *Yildirim.*

(d) Necessary in a democratic society

The final question to be asked of the Cleanfeed system for the purposes of Article 10(2) is whether it can be said to be "necessary in a democratic society". This involves a proportionality test which considers whether there is a "pressing social need"[117] for the interference and whether the interference goes further than is "proportionate to the legitimate aim pursued".[118] In particular we must ask whether an outcome could be achieved by less restrictive means than those actually used.[119] In the context of filtering this test requires us to consider both underblocking and overblocking.[120]

---

[117] *Handyside*, para. 48.
[118] *Handyside*, para. 49.
[119] See e.g. *Campbell v. United Kingdom*, app. no. 13590/88, judgment of 25 March 1992, where the Court held that the routine reading of correspondence from lawyers to prisoners could not be justified where the legitimate needs of the prison authorities could be achieved by the less invasive method of opening (but not reading) letters suspected of containing contraband.
[120] The cost of implementing a filtering system would also feed into the proportionality test if the system were mandatory. It will not be considered here however as the Cleanfeed system remains voluntary at the ISP level. On cost as a factor in proportionality generally see *Twentieth Century Fox v. British Telecommunications* [2011] EWHC 1981 (Ch); *Twentieth Century Fox v. British Telecommunications (No.2)* [2011] EWHC 2714 (Ch) and *EMI Records Ltd & Ors v. British Sky Broadcasting Ltd & Ors* [2013] EWHC 379 (Ch). In those cases BT has estimated its costs in complying with filtering injunctions at £5,000 for the initial implementation and £100 for each injunction notified to it thereafter.

Takedown at source

An important element in favour of the proportionality of the Cleanfeed system is that it is confined to material hosted outside the United Kingdom.[121] This reflects the principle that filtering should be limited to those cases where the less restrictive means of takedown at source is impossible. Where material is hosted within the UK the justification for filtering – that a site is beyond the reach of national authorities – does not apply and the ordinary criminal process should take its course. Similarly, moves by the IWF towards international takedown are to be welcomed for similar reasons – if foreign hosting providers are willing to remove material notified to them then blocking again is a disproportionate response.[122]

Underblocking

We have seen that the Cleanfeed system is prone to underblocking in the sense that it will prevent only a small subset of attempts to view CAI, is relatively easily evaded and leaves untouched other sources such as peer to peer.[123] How will this affect our assessment of its proportionality under Article 10?

A comparable issue arose in *Perrin v. United Kingdom*[124] ("*Perrin*") where the applicant had been convicted of the offence of publishing an obscene article in the form of a web page which depicted "people covered in faeces, coprophilia, coprophagia and men involved in fellatio". Before the Strasbourg court he claimed that this was a disproportionate interference with his freedom of expression arguing, amongst other things, that similar material was readily available elsewhere on the internet. The Court did not accept that the sanction was disproportionate even if the law was largely

[121] Internet Watch Foundation, 'FAQs Regarding the IWF's Facilitation of the Blocking Initiative'.
[122] The decision in *Yildirim* indicates that this should be taken into account, noting that "there is nothing in the case file to indicate that Google Sites was notified under section 5(2) of Law no. 5651 that it was hosting illegal content, or that it refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings." (Para. 62.)
[123] Williams, 'New Web Filter Laws Questioned by Top Child Abuse Cop'.
[124] App. no. 5446/03, decision of 18 October 2005.

ineffective to prevent other comparable websites from being accessible. Instead it held that "the fact that the [Obscene Publications] Act may provide only limited protection to vulnerable people is no reason why a responsible Government should abandon the attempt to protect them". The Court went on to distinguish the decision in *Observer and Guardian v. United Kingdom.*[125] In that case (part of the notorious *Spycatcher* litigation) the Court had held that it was disproportionate to continue an injunction against newspapers restraining publication of "confidential" material which was readily available elsewhere. Here, however, the Court took the view that:

> there is a clear difference between what is necessary to preserve the confidentiality of secret information, which is compromised after the very first publication of the information and what is necessary to protect morals, where harm can be caused at any time at which a person is confronted with the material.

While *Perrin* was an admissibility decision rather than a fully argued and reasoned judgment, it is likely that the same approach would be taken in the context of CAI where the harm lies in continued distribution as well as the initial publication. Consequently the limited effectiveness of the Cleanfeed system would not in and of itself mean that the system is disproportionate for the purposes of Article 10.[126]

Overblocking

There is as yet no judicial consensus on what degree of overblocking will make a restriction disproportionate under Article 10(2) though some standards are slowly emerging. In an offline context we can look to comparators such as *Ürper and others v. Turkey*[127] where the ECtHR held that orders banning the future publication of entire periodicals went beyond any restraint which might be necessary in a democratic society and therefore amounted to impermissible censorship. By analogy it seems unlikely that

[125] App. no. 13585/88, judgment of 26 November 1991.
[126] Compare *Twentieth Century Fox v. British Telecommunications* [2011] EWHC 1981 (Ch) where Arnold J. held that a blocking order against a filesharing site would be justified "even if it only prevented access… by a minority of users".
[127] Apps. nos. 55036/07, 55564/07, 1228/08, 1478/08, 4086/08, 6302/08 and 7200/08, *Ürper and Others v. Turkey*, judgment of 20 October 2009, para. 44.

filtering systems which block at the level of an entire website or domain would be acceptable where there is other, legitimate, content on that site or domain.[128] This is supported by the decision in *Yildirim* where the Court – without explicitly ruling on the point – appeared to take the view that the blocking measure was in any event disproportionate on the basis that it "produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all the sites hosted by Google Sites".[129]

The European Court of Justice in *Scarlet Extended v. SABAM*[130] has taken into account the potential that a filtering system "might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications" as one factor in deciding that an injunction did not strike a fair balance between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.[131] Unhelpfully, however, it did not elaborate on this point or consider what degree of overblocking (if any) might be compatible with the fair balance it describes.

At a domestic level, the only authority directly on point is the judgment of Arnold J. in *Newzbin2* which held that an order requiring blocking of an entire site was proportionate, notwithstanding that not all of the content on that site would infringe copyright. This decision did not, however, discuss the standards which might apply to that assessment other than to say that: "the order would potentially prevent BT

[128] Compare the analysis in General Comment 34: 'Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3.' United Nations Human Rights Committee, *General Comment No. 34 - Article 19: Freedoms of Opinion and Expression*, CCPR/C/GC/34, 12 September 2011, para. 43, http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.
[129] Para. 68.
[130] Case C-70/10, [2011] ECR I-11959.
[131] Paras. 52-53.

subscribers from making use of Newzbin2 for non-infringing uses. On the evidence, however, the incidence of such uses is *de minimis*".[132]

While these decisions do not establish any definitive standards in relation to overblocking they do provide us with some guidance under which the IWF will generally perform well. The IWF has led the way in its use of full URLs as the basis for the CAIC list – unlike, for example, the EU funded CIRCAMP model which deliberately overblocks at the domain name level.[133] Consequently the system can be granular down to the level of the individual image, without needing to block entire pages or sites.[134] This will not eliminate overblocking – for example, the content of pages might change following their classification – but it does minimise it in a way which many other systems do not.[135]

The difficulty lies not with the IWF CAIC list itself but rather with ISPs' technical implementations which may lead to collateral damage. For example, some ISPs have chosen to filter by using DNS or even IP based blocking – which has resulted in the type of massive overblocking condemned by the ECtHR in *Yildirim*.[136] Will this mean that the Cleanfeed system should be regarded as disproportionate? Our analysis in this area is complicated by the fact that only the IWF itself will be regarded as a public authority so that the private choices ISPs make in implementation are most likely beyond the scope of Article 10. As a result it is possible that this overblocking cannot be attributed to the

[132] *Twentieth Century Fox v. British Telecommunications* [2011] EWHC 1981 (Ch) para. 186.
[133] McIntyre, 'Child Abuse Images and Cleanfeeds'.
[134] Though technical mistakes on the part of IWF analysts can still lead to overblocking. See Clayton, 'Technical Aspects of the Censoring of Wikipedia'.
[135] There is a trade-off here. Location based filtering necessarily suffers from the fact that what is at a particular location can and does change. It is however computationally less demanding and potentially less invasive of privacy than hash value based filtering, which would gain precision at the cost of more invasive inspection of user traffic. See the discussion in McIntyre, 'Child Abuse Images and Cleanfeeds'.
[136] Lahtinen, 'Be Unlimited Causes Stir in Effort of Blocking Child Abuse Images'; Joe McNamee, 'Blocking of Innocent Websites by O2 Ireland', *EDRi: European Digital Rights*, 14 July 2010, http://www.edri.org/edrigram/number8.14/o2-blocking-websites-ireland.

state, especially as the IWF recommends against these types of systems.[137] (Though the IWF could – and should – make it a contractual condition of taking the CAIC list that licensees would block only at the full URL level.) This highlights a point we encountered in chapter 6 – while judicial review of the IWF may address some concerns it is at best only a partial means of oversight and in particular cannot deal with issues which arise at the ISP level.

(iii) Article 6

While the main issues presented by the Cleanfeed system relate to Article 10 ECHR, there is also a significant issue regarding the procedural rights guaranteed by Article 6. Is the decision to block a particular website a "determination of… civil rights and obligations" of the site operator so as to trigger the entitlement to a "fair and public hearing" before "an independent and impartial tribunal established by law"? If so, would the system meet the requirements of Article 6?[138]

(a) "Civil rights and obligations"

One of the less satisfactory aspects of the Strasbourg case law is the application of Article 6 to non-criminal cases.[139] The concept of "civil rights and obligations" was early on given a restrictive interpretation so as to apply to private law obligations only, leaving most public law matters outside its scope.[140] More recently, however, the trend in the jurisprudence of the Court has been to widen the scope of the concept to ensure

[137] Internet Watch Foundation, 'Combating Online Child Sexual Abuse Content at National and International Levels: IWF Experience, Tactical Suggestions and Wider Considerations', 2010, 6, http://www.iwf.org.uk/resources/tactical-briefing.
[138] This section assumes that blocking would not constitute the "determination… of any criminal charge" insofar as it would not meet the criteria set out in *Engel and others v. The Netherlands*, apps. nos. 5100/71, 5101/71, 5102/71, 5354/72, and 5370/72, judgment of 8 June 1976. In this context there is no finding of guilt on the part of an individual, nor any punishment as that term is understood by the Strasbourg court.
[139] Korff and Brown, 'Social Media and Human Rights', n. 236.
[140] See generally David Harris et al., *Law of the European Convention on Human Rights*, 2nd ed. (Oxford: Oxford University Press, 2009), chap. 6.

greater protection for individuals.[141] Consequently, while there is no authority expressly on this point, it is most likely that blocking decisions made by national authorities would fall within Article 6 – either on the basis that freedom of expression must be regarded as a "civil right"[142] or else on the basis that the result of a blocking decision is decisive for private rights and obligations[143] by interfering with the commercial operation of a site.[144]

The Council of Europe Recommendation on Internet Filtering supports this view by stating that blocking of content should only take place if "the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6".[145]

(b) Requirements imposed by Article 6

Given that Article 6 applies to decisions to block content, a significant overhaul of the structures and practices of the IWF would be necessary to put in place the legal framework which Article 6 requires.[146] As the IWF stands it cannot be described as "established by law" for the purposes of blocking decisions insofar as it has no basis in legislation.[147] It therefore would also lack the other requirements of a tribunal identified in *Belilos v. Switzerland* in relation to "determining matters within its competence on the basis of rules of law and after proceedings conducted in a prescribed manner" and

[141] See e.g. *Ferrazzini v. Italy*, app. no. 44759/98, judgment of 12 July 2001.
[142] Compare *Reisz v. Germany*, app. no. 3201, decision of 20 October 1997.
[143] *Ringeisen v. Austria*, app. no. 2614/65, judgment of 16 July 1971.
[144] Martin Husovec, 'In Rem Injunctions: Case of Website Blocking', 28 April 2013, http://papers.ssrn.com/abstract=2257232.
[145] Committee of Ministers of the Council of Europe, 'Recommendation on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters'.
[146] This section will look only at the most problematic aspects which would require reform under Article 6. Others might well pass muster as is. For example, the IWF would, because of its subject matter, likely be exempt from the requirement of publicity on the basis that it might prejudice the administration of justice to reveal all URLs of sites blocked by it. Compare *B and P v. UK* 34 EHRR 529 upholding blanket confidentiality rules regarding family law matters.
[147] See e.g. Harris et al., *Law of the European Convention on Human Rights*, 297–298.

"independence, in particular of the executive; impartiality; duration of its members' terms of office; [and] guarantees afforded by its procedure".[148]

The absence of any notification – either before or after a decision to block is made – would also be incompatible with Article 6 which establishes a right to an adversarial trial to include "the opportunity for the parties to a civil or criminal trial to have knowledge of and comment on all evidence adduced or observations filed with a view to influencing the Court's decision".[149] *Ruiz-Mateos v. Spain*[150] illustrates this point, finding that there was a breach when the applicants were not allowed to reply to written submissions made by counsel for an opposing party on the basis that there was a right for one party to have knowledge of and to comment on observations or evidence filed by the other party. This will apply *a fortiori* where one party has not been notified and is therefore entirely unaware of the existence of proceedings. Indeed, quite apart from Article 6 the failure to provide any notice would almost certainly provide the basis for judicial review on traditional procedural grounds.[151] There is a striking parallel with the decision in *R. v. Norfolk County Council, ex parte M*[152] in which the High Court held that a local authority decision to enter a person's name on a child abuse register as a suspected abuser had been made in breach of natural justice where this was done after a one sided investigation and without affording him the opportunity to object or make representations.

(c) Judicial review as satisfying Article 6

Might these deficiencies be cured by the possibility of judicial review of the IWF before the High Court? It is true that Article 6 does not require that all first instance decision

[148] App. no. 10328/83, judgment of 29 April 1988, para. 64.
[149] *Vermeulen v. Belgium* 32 EHRR 313, para. 33.
[150] A262, 15 EHRR 505 PC.
[151] Particularly following the decision in *Osborn v. The Parole Board* [2013] UKSC 61 which stressed that human rights protection is not a distinct area of law limited to ECHR obligations but permeates the legal system as a whole.
[152] [1989] 2 All ER 359.

makers must comply with the requirements of that article.[153] In the interests of "flexibility and efficiency"[154] the Court has narrowed the requirement of an independent tribunal and will allow decisions which affect fundamental rights to be made administratively at first instance, provided that there is "subsequent control by a judicial body that has full jurisdiction and does provide the guarantees of Article 6(1)".[155] The case law on this point, however, makes it clear that "full jurisdiction" requires the existence of an appeal on the merits: a mere review of legality is insufficient.[156] Consequently, judicial review in the restrictive sense in which it exists in English law would be unlikely to ensure that the IWF decision making process meets the requirements of Article 6.[157]

4. Conclusion

This chapter has demonstrated that from an English perspective the application of governance standards and fundamental rights to filtering is an area which is nascent at best. It is particularly striking to see how little influence Parliament has had on the development of the law in this area. While both section 12 of the Human Rights Act and section 17 of the Digital Economy Act reflect parliamentary concern about prior restraints of speech, these concerns are not addressed in the two nationwide filtering systems which have actually developed – blocking under section 97A and Cleanfeed. Indeed it is remarkable that the courts in developing the section 97A jurisprudence have chosen to reject safeguards (such as notification) which Parliament considered to be of fundamental importance when passing the Digital Economy Act.

---

[153] Harris et al., *Law of the European Convention on Human Rights*, 228–232.
[154] *Le Compte, Van Leuven and De Meyere v. Belgium* (1981) 4 EHRR 1, para. 51.
[155] *Albert and Le Compte v. Belgium* 5 EHRR 533, para. 29. A separate, more lenient jurisprudence applies in cases of administrative discretion and policy choices: see *Bryan v. United Kingdom* 21 EHRR 342.
[156] Harris et al., *Law of the European Convention on Human Rights*, 228–232.
[157] See e.g. *W v. United Kingdom* 10 EHRR 293 PC; *Kingsley v. United Kingdom* app. no. 35605/97, judgment of 7 November 2000.

At an international level there is a substantial degree of consensus as to the norms which filtering should meet. The most important of these – accepted by both the Council of Europe and the UN Human Rights Committee – is a rejection of private censorship so that mandatory filtering should take place only with a legislative basis and only where decisions on blocking are made by an independent public body or a judicial body. There is then near universal consensus regarding the need for procedural safeguards and in particular transparency in blocking (such as the use of block pages) and the need for blocking to take place at the level of the item to be blocked only.

Applying these standards to the IWF and Cleanfeed we see that the IWF generally does well while the Cleanfeed system as a whole does poorly. In overall terms the IWF meets the majority of the procedural and structural safeguards identified (though it lacks an adequate appeals process) and in relation to the ECHR falls down primarily due to the lack of notification for Article 6 and its lack of a legal basis as required by Article 10. The system as a whole, however, suffers due to the fact that ISPs remain free to disregard the safeguards recommended by the IWF. In particular, so long as ISPs remain free to overblock rather than use full URL blocking then the system as a whole is compromised. Consequently, while the blocking of CAI is certainly a legitimate aim, the manner in which it is implemented would not meet the requirements of the ECHR.

To what extent then might the rights discussed in this chapter be used to enforce these standards against the Cleanfeed system? Here we face the problem that in most cases the concerns are structural and not easily addressed by the use of individual rights. There are several dimensions to this problem.

First, a standard or recommendation for good governance simply might not have an equivalent individual right associated with it. For example, it is hard to see how there could be an enforceable individual right to the use of a block page. In fact, conceptualising the area in rights terms may be counterproductive – we have already seen in chapter 2 how defamation fears have deterred ISPs from using block pages.

Second, even if a particular standard does mirror an individual right (the right to be notified, for example) then there is no guarantee that litigation will be an appropriate vehicle to secure that right. There will be relatively few cases where the facts are favourable to challenge blocking practices. Of those, where a site owner discovers that they have been wrongfully blocked then their interest is, understandably, in having the site unblocked – not establishing a point of principle for the benefit of some unknown person in the future. In addition, the nature of blocking is such that the site owner will usually be abroad and thus have little interest in domestic law. Finally, the cost of taking an action is likely to be prohibitive. The Wikipedia incident illustrates these points – in that instance the blocked entity was well resourced, well versed in the law and ideologically committed to freedom of expression. Despite this, however, once the block was reversed it had no interest in pursuing the matter further.[158]

Assuming we can jump these first two hurdles we may still face a third one – given the diffuse nature of the Cleanfeed system, there may be no remedy available against the entity responsible. If, for example, an ISP is overblocking by using DNS blocking based on the IWF list then there is no obvious basis for action against either the IWF (which recommends against DNS blocking) or the ISP itself. Even treating the IWF as a public entity will not assist with downstream interferences which are the result of the manner of implementation by private ISPs. While it might be possible to attribute some of these interferences to the state – by arguing that there is a positive obligation to promote freedom of expression online – the challenges involved in doing so are greater again.

[158] Mike Godwin, General Counsel to the Wikimedia foundation, made it clear at the time that he saw this as a matter for 'citizens in the UK' to take forward: Mike Godwin, 'Why IWF's Wikipedia Reversal Is Not Enough', 12 December 2008, http://archive.is/GbiOi.

Given these points, the rights discussed in this chapter may well be valuable in individual cases but are unlikely to act as a vehicle for any systemic change in the Cleanfeed system. It is difficult to disagree with Brown and Korff who have argued in a similar context that:

> the ECHR as currently applied is insufficient to regulate the actions of private entities involved in the day-to-day operation of the Internet. It should not be left to the indirect, haphazard application of the doctrine of horizontal effect to secure the rights to communication, expression and association of everyone, including political activists, on the Internet vis-à-vis ISPs, search engines and blog hosts, for example. In our opinion, the emerging Internet governance principles (which specifically extend to private sector entities) should become legally enforceable. [159]

[159] Korff and Brown, 'Social Media and Human Rights', 205.

Chapter 8 – Conclusion

1. Introduction

In this thesis we have assessed the Cleanfeed system and developed the argument that it sits at the intersection of three distinct regulatory strategies – regulation by code, gatekeeper regulation and self-regulation – which individually and all the more so collectively present substantial risks for freedom of expression online. We have seen that many of these risks have manifested themselves in the Cleanfeed system as a whole – notably a lack of transparency, limited feedback, overblocking, function creep and reduced accountability – though at the same time the self-regulatory nature of the system has helped to promote transparency and accountability and reduce function creep in the IWF itself. We have considered the fundamental rights standards which should apply to blocking and have concluded that Cleanfeed would not meet the requirements of the ECHR. However, we have also seen that the available public law remedies would be insufficient to address these issues so that systemic change is necessary if Cleanfeed is to be made ECHR compliant. In this chapter we conclude by considering the implications of these findings for possible reform of the Cleanfeed system and for filtering in the UK more generally.

2. Proposals for reform

(i) Moving towards co-regulation?

The most common response to criticisms of self-regulation is to argue for more state involvement in the regulatory mechanism.[1] Greater involvement, so the argument runs, will legitimate and provide greater transparency to self-regulatory systems as well as guarding against abuses of power, while still maintaining the flexibility of self-

[1] See e.g. Ian Bartle and Peter Vass, 'Self-Regulation within the Regulatory State: Towards a New Regulatory Paradigm?', *Public Administration* 85 (December 2007): 885.

regulation. Lievens *et al.* have argued for this in the area of online child protection provided that five standards are met:

> 1. A more balanced constitution of co-regulatory bodies with the equal participation of different partners (government, industry, and users);
> 2. Systems that ensure that co-regulatory bodies are accountable to the government if they act outside the scope of their competences;
> 3. A clear, unambiguous legal basis;
> 4. Easily accessible arrangements regarding the operation of the co-regulatory bodies; and
> 5. A clear division of tasks and competences between those bodies and the government.[2]

In identifying these standards they drew on work by Ofcom, which is under a statutory obligation to promote the development of effective forms of self- and co-regulation and to that end has developed criteria which it will use in determining whether to transfer regulatory responsibilities to a co-regulatory body.[3] For example, in relation to appeals Ofcom advise:

> [I]t is desirable for there to be a genuinely independent appeals mechanism that complies with the Human Rights Act 1998. Examples of the features of an appeal process which promote independence include, appeal arbitrators or panel members drawn from outside the industry and appointed on fixed, preferably non-renewable terms, and open, even-handed and transparent procedures. Careful consideration will need to be given to who appoints the appellate body.[4]

The current IWF "appeals" process, consisting of a simple referral to a police force, does not meet this standard and would be considerably improved if it did.[5]

A "Digital Rights Commission"?

The possibility of building in safeguards in this way has an obvious appeal and this approach has been developed by Laidlaw who argues for the establishment of a statutory

[2] Lievens, Dumortier, and Ryan, 'The Co-Protection of Minors in New Media', 146.
[3] Ofcom, 'Criteria for Promoting Effective Co- and Self-Regulation', 2004, http://stakeholders.ofcom.org.uk/binaries/consultations/co-reg/statement/co_self_reg.pdf.
[4] Ibid., 12.
[5] Internet Watch Foundation, 'Content Assessment Appeal Process'.

body to regulate the IWF and other internet speech gatekeepers such as search engines.[6] Under her proposal a UK "Digital Rights Commission" would have three broad sets of functions:

- Education, policy and research;
- Corporate support – assisting internet companies with internal corporate social responsibility codes, policy assessment tools and human rights audits; and
- Remedial and rule making – dealing with complaints from owners of sites who claim to have been wrongfully blocked or de-listed from search engines.[7]

The remedial functions would be a last resort once internal appeals had been exhausted and would enable the Commission to make binding decisions regarding complaints of wrongful blocking, including the power to fine and to award damages.[8] The point regarding damages in addition to a fine is significant – we have already seen that *Peck*[9] requires that damages should be available for breach of a Convention right if national remedies are to meet the requirements of Article 13 ECHR and Laidlaw argues that any national scheme which fails to specifically provide for damages would not be compliant.

Laidlaw describes this approach as "meta-regulation" or "the legal regulation of self-regulation" rather than co-regulation.[10] This reflects the fact that under her proposal the IWF itself would continue to be self-regulatory without any statutory basis. In this, she appears to assume that oversight by a Digital Rights Commission would remedy the Article 10 issues she identifies in the IWF. However, this would leave open the objection that its blocking role would still not be "prescribed by law" as defined by cases such as *Barthold v. Germany*.[11] Given the fundamental nature of the power exercised by

[6] Emily Laidlaw, 'Internet Gatekeepers, Human Rights and Corporate Social Responsibilities' (London School of Economics and Political Science (LSE), 2012), chap. 6, http://etheses.lse.ac.uk/317/.
[7] Ibid., 227.
[8] Ibid., 230–231.
[9] *Peck v. United Kingdom*, app. no. 44647/98, judgment of 28 January 2003, para. 109.
[10] Laidlaw, 'Internet Gatekeepers', 220–221.
[11] App. no. 8734/79, judgment of 25 March 1985.

the IWF it would be necessary that the power have an express legal basis. The closest precedent might be the way in which Ofcom has delegated certain functions to the Authority for Video on Demand (ATVOD). ATVOD has evolved from a self-regulatory to a statutory co-regulatory structure as a result of the Audio Visual Media Services Directive which requires that video on demand services should be regulated on at least a co-regulatory basis and the way in which this was done might serve as an example for the IWF.[12]

This objection aside, there would be merit to Laidlaw's proposal. In particular, by leaving Cleanfeed as a voluntary system for ISPs it would leave open the possibility of ISPs reining in any function creep by declining to implement it.

(ii) Establishing the IWF as a public body?

Edwards would go further and has argued that the IWF should be reconstituted as a full public body. In her model the IWF would continue its blacklisting function but on a statutory basis with a board comprised of a "majority of legal professional members alongside industry and charity representatives and chaired by an independent member of the judiciary who could resist [government pressure to expand the blocking list]".[13] The main advantage would be that this approach would clearly satisfy the requirement that blocking should be "prescribed by law" as required by Article 10 ECHR. While it is unlikely that the IWF itself could be constituted as an "independent and impartial tribunal" under Article 6 ECHR, we have seen that it would be sufficient that there is "subsequent control by a judicial body that has full jurisdiction and does provide the guarantees of Article 6(1)".[14] Consequently a framework whereby the IWF makes initial

[12] See e.g. Prosser, 'Self-Regulation, Co-Regulation and the Audio-Visual Media Services Directive'; Daithi Mac Sithigh, 'Co-Regulation, Video-on-Demand and the Legal Status of Audio-Visual Media', *International Journal of Digital Television* 2, no. 1 (2011): 49–66.
[13] Edwards, 'Pornography, Censorship and the Internet', 657–658.
[14] *Albert and Le Compte v. Belgium* 5 EHRR 533, para. 29.

decisions which could then be appealed on the merits to the First Tier Tribunal could in principle be compatible with the ECHR.

Edwards' argument is based in large part on the fear that future governments might instruct the IWF to begin blocking additional content and she has identified the IWF as being ill-placed to resist such pressure, being lacking in independence and prone to function creep.[15] Ironically, however, the current research suggests that putting the IWF on a statutory basis might exacerbate rather than mitigate function creep without necessarily providing better governance in return.

We have seen that the self-regulatory structure of the IWF – by demanding industry and charity support for any extension – has helped to ensure that no expansion of the blocking system has taken place despite frequent political suggestions to this effect.[16] Consequently where the expansion of blocking has taken place it has done so outside the IWF – most significantly in the form of s.97A blocking orders which we have argued are themselves not ECHR compliant.[17] In the same way, the IWF has demonstrated a level of transparency in its activities which far outweighs that of (for example) the Home Office in its existing scheme for filtering of "terrorist" websites.[18] There are a number of ways in which self-regulation has provided an alternative accountability mechanism and acted as a check on the actions of the state, which might be jeopardised if the IWF were to be established as a public body with compulsory powers.

Perhaps the closest comparator is Australia where the Australian Communications and Media Authority (ACMA), police and certain regulatory agencies have been given statutory powers to order ISP level blocking and the removal of links to content, with proposals on the table to extend these powers much further.[19] Despite the statutory basis

[15] Edwards, 'Pornography, Censorship and the Internet', 657.
[16] Chapter 5.
[17] Chapter 7.
[18] See section 4 of this chapter.
[19] For background see David Vaile and Renée Watt, 'Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra', *Telecommunications Journal of*

for that filtering it has been marred by repeated controversies with complaints that it is entirely opaque, has resulted in significant collateral damage (wrongfully blocking 250,000 sites in one particular instance) and has been extended well beyond its original justification.[20] Most famously, in 2009 ACMA threatened fines of up to $11,000 per day for an online forum which posted a link to a blocked anti-abortion website – followed up by threats of similar fines for sites which linked to a leaked blacklist on Wikipedia.[21] This was followed soon after by a leak of ACMA's own blacklist which revealed that the authority had blocked:

> a slew of online poker sites, YouTube links, regular gay and straight porn sites, Wikipedia entries, euthanasia sites, websites of fringe religions such as satanic sites, fetish sites, Christian sites, the website of a tour operator and even a Queensland dentist.[22]

In short, therefore, it is clear that public bodies are not in any way immune from function creep and we must also consider what might be *lost* by a move away from self-regulation or co-regulation.

3. Generalising from Cleanfeed to other forms of filtering

> The government is to order broadband companies to block extremist websites and empower a specialist unit to identify and report content deemed too dangerous for online publication… Ministers are understood to want to follow the model used to crack down on online child abuse. The Internet Watch Foundation, which is partly industry-funded, investigates reports of illegal child abuse images online; it can then ask service providers to block or take down websites. The prime minister, David Cameron, is understood to favour a similar model for terrorist content. A

Australia 59, no. 2 (2009); Anna Cairo and Rowan Wilken, 'The Australian Government Internet Filter: Its Scope, and Its Potential Civil Liberties Implications', *Telecommunications Journal of Australia* 62, no. 2 (2012), http://tja.org.au/tja/index.php/tja/article/view/308.

[20] Renai LeMay, 'Interpol Filter Scope Creep: ASIC Ordering Unilateral Website Blocks', *Delimiter*, 15 May 2013, http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/; Ben Grubb, 'How ASIC's Attempt to Block One Website Took down 250,000', *The Sydney Morning Herald*, 5 June 2013, http://www.smh.com.au/technology/technology-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html.

[21] Asher Moses, 'Banned Hyperlinks Could Cost You $11,000 a Day', *Sydney Morning Herald*, 17 March 2009, http://www.smh.com.au/articles/2009/03/17/1237054787635.html; Fran Foo, 'ACMA Takes Aim at Whirlpool, Supplier', *The Australian*, 13 March 2009, http://www.australianit.news.com.au/story/0,24897,25181408-15306,00.html.

[22] Asher Moses, 'Leaked Australian Blacklist Reveals Banned Sites', *The Sydney Morning Herald*, 19 March 2009, http://www.smh.com.au/articles/2009/03/19/1237054961100.html.

> government-funded body, possibly within the counter-terrorism referral unit, will order companies including BT, TalkTalk, BSkyB and Virgin Media to block websites, according to industry sources.
>
> – Juliette Garside, *The Guardian*, 27 November 2013[23]

The perceived success of the IWF and Cleanfeed has reinforced the commitment of the UK to self-regulation online and has led to a fascination on the part of successive governments with internet blocking as a regulatory tactic. The system has been cited in support of the expansion of mandatory blocking to various other contexts ranging from filesharing sites[24], to sites which glorify terrorism[25], encourage suicide[26] or promote anorexia.[27] Very often this takes the facile form of simply pointing to Cleanfeed as a proof of concept[28] but even more sophisticated observers have uncritically accepted the claim that it is a "breakthrough" to be emulated.[29] At the time of writing, this has again manifested itself in proposals from the Prime Minister's Extremism Task Force to develop a parallel system, modelled on Cleanfeed, which would "work with internet companies to restrict access to terrorist material online which is hosted overseas".[30]

Against these claims, this thesis has demonstrated that when analysed in detail the Cleanfeed system is much more problematic and does not support the further extension of blocking. To begin with, we have seen that policy discussions often fail to

---

[23] Juliette Garside, 'Ministers Will Order ISPs to Block Terrorist and Extremist Websites', *The Guardian*, 27 November 2013, http://www.theguardian.com/uk-news/2013/nov/27/ministers-order-isps-block-terrorist-websites.

[24] As enacted in the Digital Economy Act 2010.

[25] Chris Williams, 'Jacqui's Jihad on Web Extremism Flops', *The Register*, 13 February 2009, http://www.theregister.co.uk/2009/02/13/jacqui_smith_web_extremism/.

[26] Ministry of Justice, 'Suicide and the Internet - Updating the Law', 17 September 2008, http://www.justice.gov.uk/news/newsrelease170908a.htm; John Ozimek, 'Net Suicide Bill Would Breathe Life into Government Censorship', *The Register*, 24 September 2008, http://www.theregister.co.uk/2008/09/24/suicide_bill_censorship/; Kelly Fiveash, 'Health Minister Warns ISPs: Block Suicide Websites or Face Regulation', *The Register*, 10 September 2012, http://www.theregister.co.uk/2012/09/10/norman_lamb_calls_for_isps_to_block_suicide_websites/.

[27] Papadopoulos, *Sexualisation of Young People Review*, 78.

[28] See e.g. James Brandon, *Virtual Caliphate: Islamic Extremists and Their Websites* (London: Centre for Social Cohesion, 2008), 79.

[29] 'Breakthrough' being the term used by Nellie Kroes, Vice-President of the European Commission: Internet Watch Foundation, '2010 Annual Report', 2.

[30] Prime Minister's Task Force on Tackling Radicalisation and Extremism, *Tackling Extremism in the UK* (London: Cabinet Office, 2013), para. 3.1, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/263181/ETF_FINAL.pdf.

differentiate between the (very successful) role of the IWF in dealing with illegal material hosted in the UK and its role in providing a blacklist of sites hosted abroad. By conflating the two, proponents of blocking are (often unwittingly) using the success of the notice and takedown remit to justify expansion of the very different filtering remit.[31] When we separate the two, it becomes clear that Cleanfeed is a wider system which brings together a variety of actors in addition to the IWF itself. The result is that many of the desirable features of the IWF are lost in the operation of the system as a whole. For example, while the IWF has shown a strong commitment to transparency the implementation of Cleanfeed has until recently been marked by precisely the opposite, with the majority of ISPs misleading users as to its use.[32]

Claims that Cleanfeed represents a gold standard in the technical implementation of blocking are also undermined by this research. While the particular URL blocking system pioneered by BT is an improvement on prior techniques we have seen that it is still prone to causing significant collateral damage and is still not universally used, with some ISPs still using much cruder IP and DNS based approaches.[33] This may have been tolerable so far as blocking was limited to a relatively small number of domains hosting child pornography – however, it is set to present much wider problems if expanded.[34]

This has become particularly evident following the decision in *Newzbin2* allowing copyright plaintiffs to co-opt ISP blocking systems so that many more domains will be blocked and for a longer duration in each case. The first examples of overblocking came in August 2013 with the blocking of approximately 200 sites (including the *Radio Times* and Blackburn Rovers FC) resulting from a section 97A blocking order granted to the

[31] See e.g. Carter, *Digital Britain: Final Report*, 202–203.
[32] See chapter 4.
[33] Clayton, 'Technical Aspects of the Censoring of Wikipedia'.
[34] A report commissioned by Ofcom in 2012 found that over 97% of websites were hosted on shared IP addresses, creating a substantial risk of overblocking: CSMG, *Study into Websites Sharing Internet Protocol Addresses*, 26 April 2012, http://stakeholders.ofcom.org.uk/binaries/internet/websites-sharing.pdf.

Premier League against sports streaming site FirstRow.[35] This was matched at the same time by the blocking of copyright news site *TorrentFreak* under an order intended to block access to the filesharing site EZTV.[36] In each case users and site owners were left unaware of the reason for the blocking which took several days to identify and eventually remedy. While these high profile mistakes may cause ISPs to take more care in the way in which they implement blocking, it is likely that similar overblocking will continue unless the courts revisit the scope of the orders being granted under section 97A. In the meantime, however, cases such as these should give pause to those who advocate extending blocking further.

Finally, we have also made the case that child abuse images represent the best case scenario for blocking and it is impossible to generalise from this into other areas.[37] This reflects both principle and pragmatism. In principle, blocking of CAI is by far the easiest to justify as a proportionate protection of individual rights and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has noted that in this regard it is an "exception" which cannot be used to justify wider blocking measures:

> child pornography is one clear exception where blocking measures can be justified, provided that the national law is sufficiently precise and there are effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[38]

From a practical perspective, there is near universal agreement on the illegality of such material and considerable public support for countermeasures. Such images are more

[35] Glyn Moody, 'Massive Overblocking Hits Hundreds Of UK Sites', *Techdirt.*, 15 August 2013, http://www.techdirt.com/articles/20130815/09563524186/massive-overblocking-hits-hundreds-uk-sites.shtml; 'Radio Times Casualty of Piracy Fight', *BBC*, 14 August 2013, http://www.bbc.co.uk/news/technology-23699681; Shona Ghosh, 'Rights-Holders Taking down Legitimate Sites in Piracy Crackdown', *PC Pro*, 14 August 2013, http://www.pcpro.co.uk/news/broadband/383614/rights-holders-taking-down-legitimate-sites-in-piracy-crackdown.

[36] Shona Ghosh, 'Sky Blocks News Site after DNS Exploit', *PC Pro*, 12 August 2013, http://www.pcpro.co.uk/news/broadband/383587/sky-blocks-news-site-after-dns-exploit.

[37] See chapter 1, section 3(ii).

[38] United Nations Human Rights Committee, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 10.

straightforward to identify and the comparatively small number of sites involved makes it technologically and administratively more convenient to introduce blocking systems. These points do not, however, apply to the other types of content which it has been proposed to block, making CAI blocking an entirely inappropriate comparator.

4. Further research

While this thesis has focused on the Cleanfeed system as a particularly useful case study, the governance and fundamental rights arguments it develops are of wider significance for UK internet governance. We have already seen how the IWF typifies long-standing government policy favouring self-regulatory controls for online content and as a result there are several comparable systems in the UK which merit further research using the approach outlined in this work.

Two current examples stand out in particular. The best known is that of Nominet which has suspended thousands of .uk domain names based on mere police accusation of involvement in crime, without any legislative basis, court order or indeed even an internal policy to govern how it does so.[39] Similar issues also arise with the Home Office which has since November 2008 operated a voluntary scheme to block "terrorist" websites.[40] Under this scheme the Home Office provides a secret list of URLs which it deems to be "unlawfully terrorism related" to firms which supply filtering software, who in turn incorporate these URLs into their blacklists. There is no notification or appeal process against this blacklisting, nor is the user notified that the URL has been blocked

[39] Chris Williams, 'Nominet Appoints Itself Web Policeman', *The Register*, 21 January 2010, http://www.theregister.co.uk/2010/01/21/nominet_lock/; Michael O'Floinn, 'Dealing with Domain Names Used in Connection with Criminal Activity: Background Report for Nominet', 2011, http://webmedia.company.ja.net/edlabblogs/regulatory-developments/2011/03/26/nominet-domain-suspension-paper/; Nominet, 'Current Policy Discussions and Consultations', 2013, http://www.nominet.org.uk/how-participate/policy-development/current-policy-discussions-and-consultations.

[40] For background see Public Service, 'Using the Internet to Reduce the Threat of Terrorism', *Public Service*, 9 November 2009, http://www.publicservice.co.uk/feature_story.asp?id=12949; Home Office, *Prevent Strategy*, 79; Home Office, *CONTEST - the United Kingdom's Strategy for Countering Terrorism: Annual Report* (London: The Stationery Office, 2013), 22.

at the request of the Home Office. While the reach of this blocking is less than that of Cleanfeed (it applies only where filtering software is in use at a local level) it is nevertheless significant as it operates to prevent users from reading certain material in institutions such as libraries and universities where freedom of expression is of particular importance. Both cases – Nominet and the Home Office – exemplify the concerns identified in this thesis regarding internet governance and require analysis from a fundamental rights perspective.

Appendix

Methodology

This research set out to investigate the doctrinal and policy issues which might arise from the operation of the Cleanfeed system. It began with a review of the academic literature in law and other relevant disciplines (in particular computer science, regulation and political science) to identify the work which has already been done on fundamental rights and governance in relation to filtering of internet content generally and the Cleanfeed system in particular.

Following this review it became apparent that there while there is an extensive literature on the technical, legal and governance aspects of internet filtering generally[1] there had been relatively little work done on the operation of the Cleanfeed system or its legal implications.[2] The IWF had been the subject of a number of case studies placing it in a wider context of self- and co-regulatory systems.[3] That work had, however, generally focused on the IWF itself. It paid less attention to the other actors in the Cleanfeed system – the ISPs which implemented filtering and the various state bodies which either encouraged or facilitated this. Consequently there was little material which considered either the origins or the operation of the Cleanfeed system in sufficient detail to allow it to be fully assessed.[4]

[1] For summaries see e.g. Deibert et al., *Access Denied*; Ronald Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010).
[2] Indeed, the main pieces which do address English law specifically all postdate the start of this research: Mac Sithigh, 'Datafin to Virgin Killer'; Marsden, 'Internet Co-Regulation and Constitutionalism'; Marsden, *Internet Co-Regulation*, chap. 2; Laidlaw, 'The Responsibilities of Free Speech Regulators'.
[3] See in particular Marsden, Simmons, and Cave, *Options for and Effectiveness of Internet Self- and Co-Regulation Inception Report*; Marsden et al., *Options for and Effectiveness of Internet Self- and Co-Regulation Phase 1 Report*; Cave, Marsden, and Simmons, *Options for and Effectiveness of Internet Self- and Co-Regulation*; Tambini, Leonardi, and Marsden, *Codifying Cyberspace*.
[4] A notable exception on the technical side is Clayton, 'Anonymity and Traceability in Cyberspace', chap. 7.

It was therefore necessary to widen the sources used to gain a full picture of the Cleanfeed system. The first port of call was the IWF website which made available all board minutes and the majority of internal policy documents from 2000 onwards. This was followed by a search of publicly indexed freedom of information requests which revealed a number of responses from the Home Office and other departments regarding the IWF.[5] The evolution of government policy was also assessed using a search of government publications, Hansard and mainstream media for references to the IWF and filtering during the relevant period. Given the background provided by these sources, the implementation of the Cleanfeed system was then traced using specialist industry publications, publicly archived mailing lists and other sources such as the LINX Public Affairs bulletin. These proved useful in providing contemporaneous evidence as to how the system was perceived by those in industry at the time. They also proved useful in providing greater clarity on a number of points which were either glossed over or simply misunderstood by the mainstream media.

These records were then supplemented by a series of interviews with individuals who were either key participants in the adoption and development of Cleanfeed or were otherwise experts in the area of online child protection and internet filtering. These were chosen with a view to filling in the information already identified as absent from the literature and offering a representative sample of the views of the various stakeholders. Interviews were carried out over the period from July 2009 to October 2010 on a semi-structured basis with the following:

- John Carr, IWF Board Member, 1997-2004, member of the Executive Board of the UK Council for Child Internet Safety, 2008 onwards;

[5] E.g. Home Office, 'Response to Freedom of Information Act Request Re Internet Watch Foundation Audits', 10 March 2009, http://www.whatdotheyknow.com/request/internet_watch_foundation_audits#incoming-20085; Home Office, 'Response to Freedom of Information Request Re the Relationship between the IWF and the Home Office and Network Level Blocking', 26 February 2009, https://www.whatdotheyknow.com/request/relationship_between_the_home_of.

- Cormac Callanan, CEO of INHOPE (International Association of Internet Hotlines), 2003-2007;
- Richard Clayton, Senior Research Assistant in the Computer Laboratory of the University of Cambridge, 2006 onwards, Technical Advisor, Demon Internet, 1995-2000;
- Don Colcolough, Director, Investigations & Law Enforcement Affairs AOL, 2002-2006, Director, Cyber Security AOL, 2006-2013;
- Andrew Cormack, Chief Regulatory Advisor to JANET(UK), 2002 onwards, Chair IWF Funding Council 2009 onwards;
- Roger Darlington, IWF Chairman 2000-2005;
- Malcolm Hutty, IWF Board Member 2000-2002, LINX Regulation Officer 2003-2005, LINX Head of Public Affairs 2006 onwards;
- Stuart Hyde, Deputy Chief Constable of Cumbria Constabulary, 2009-2012, Chief Constable of Cumbria Constabulary, 2012 onwards, former ACPO spokesman on e-Crime prevention and President of the Society for the Policing of Cyberspace;
- Nicholas Lansman, Secretary General of the Internet Service Providers' Association (ISPA), 1995 onwards;
- Michael Moran, detective sergeant on secondment to Interpol, specialising in online child sexual exploitation, 2006 onwards;
- Roland Perry, Public Affairs Officer at RIPE NCC, 2005-2010, IWF Board Member, 2001-2003 and Director of Public Policy at the London Internet Exchange (LINX), 1999-2003;
- Peter Robbins, Chief Executive IWF, 2002-2011;
- Peter Sommer, Visiting Fellow/Professor at the London School of Economics Information Systems Integrity Group, 1994 onwards;
- Nick Truman, Head of Internet Customer Security, British Telecom, 2001-2009.

In addition, one other individual closely familiar with the development of Cleanfeed was interviewed on a confidential basis and declined to be identified given what they described as the sensitive nature of the topic.

Ethics

This research involves the use of views attributed to interviewees by name unless they express a preference to speak in confidence, in which case their identities will not be revealed and their views will be used for background only. Research ethics approval was granted by the School of Law on 3 March 2009 subject to interviewees giving informed consent to be interviewed on this basis.

Terminology

(i) "Child pornography" or "child abuse images"?

> Please note that "child pornography", "child porn" and "kiddie porn" are not acceptable terms. The use of such language acts to legitimise images which are not pornography, rather, they are permanent records of children being sexually abused and as such should be referred to as child sexual abuse images.
>
> – Internet Watch Foundation, 2013[6]

In recent years children's groups have sought to eliminate the use of the term "child pornography", arguing that it trivialises the abuse suffered by children and tends to lead to confusion with legitimate adult pornography. The law, however, has not kept up and references to "child pornography" are still common in legislation, case law and other materials – particularly earlier material relevant to this work. This thesis generally uses the terms child abuse images (CAI) or child abuse material (CAM) with "child pornography" being used mostly for consistency with the older terminology in particular contexts.

[6] Internet Watch Foundation, 'About Us', 2013, http://www.iwf.org.uk/about-iwf.

(ii) "Cleanfeed" as a generic term

When BT implemented server level filtering in 2004 "Cleanfeed" was used as an internal project name, not as a public title.[7] Despite this, the term stuck as a description of the BT scheme[8] and, soon after, as a term for similar filtering by UK ISPs.[9] It has also been taken up internationally as a generic title for systems which it has influenced in Australia[10] and Canada.[11] In doing so, the term has also widened in meaning – from initially describing the filtering *technology* used by BT to now describing the wider *system* by which blocking takes place – including, for example, the designation of sites to be blocked and the possibility of appeal against such blocks.[12] Consistent with this usage, Cleanfeed will be used throughout this work as convenient shorthand for the overall system of blocking by UK ISPs of URLs designated by the IWF.

(iii) "ISPs"

For most consumers the term internet service provider or ISP denotes their broadband provider. It would be more accurate to describe these as internet *access* providers, reflecting the fact that the term ISP is wide enough to include a variety of internet services such as search engines, DNS provision, hosting, content aggregation, and so on. Nevertheless, in the context of filtering the term ISP is most commonly used to denote a consumer level connectivity provider and it will be used in that way in this work.[13]

---

[7] "Cleanfeed" is a registered trade mark of the THUS group of companies and is used by them to describe *voluntary* filtering at an end-user level.
[8] Hunter, 'BT's Bold Pioneering Child Porn Block Wins Plaudits amid Internet Censorship Concerns'.
[9] Edwards, 'From Child Porn to China, in One Cleanfeed'.
[10] Derek Bambauer, 'Filtering in Oz: Australia's Foray into Internet Censorship', December 2008, http://ssrn.com/abstract=1319466.
[11] Jane Bailey, 'Confronting Collective Harm: Technology's Transformative Impact on Child Pornography', *University of New Brunswick Law Journal* 56 (2007): 65.
[12] See e.g. the usage in Wikipedia: 'Cleanfeed (content Blocking System)', *Wikipedia*, 15 June 2013, http://en.wikipedia.org/w/index.php?title=Cleanfeed_(content_blocking_system)&oldid=555796381.
[13] See e.g. Eneman, 'Internet Service Provider (ISP) Filtering of Child-Abusive Material'; Sophie Stalla-Bourdillon, 'Chilling ISPs... When Private Regulators Act without Adequate Public Framework', *Computer Law & Security Review* 26 (2010): 290; Paul Ohm, 'The Rise and Fall of Invasive ISP Surveillance', *University of Illinois Law Review*, 2009; Kleinschmidt, 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content'.

(iv) "Filtering" or "blocking"?

In some contexts – particularly in the United States – the terms "filtering" and "blocking" have been given distinct meanings, with filtering being used to describe voluntary end-user systems while blocking describes systems which are imposed – usually at network level – without the consent of the user.[14] This is a useful distinction which highlights the fact that there is a crucial difference between technologies which help to empower users in exercising bottom-up control and those which enforce censorship on a top-down basis at the behest of the state.[15] The general practice in the European literature, however, is to use the terms interchangeably and that is reflected in this thesis where both are used in the context of mandatory network level systems.[16]

[14] 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).
[15] Eva Lievens and Peggy Valcke, 'Regulatory Trends in a Social Media Context', in *Routledge Handbook of Media Law*, ed. Monroe E Price and Stefaan Verhulst (Abingdon: Routledge, 2013), 572.
[16] See e.g. Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative'; 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, 2008); Callanan et al., *Internet Blocking*.

Bibliography

'Administrators' noticeboard/2008 IWF Action'. *Wikipedia*, 2008. http://en.wikipedia.org/wiki/Wikipedia:Administrators%27_noticeboard/2008_IWF_action.

Akdeniz, Yaman. 'Cyber-Rights & Cyber-Liberties (UK) Report - Who Watches the Watchmen: Part II'. *Cyber-Rights & Cyber-Liberties*, September 1998. http://www.cyber-rights.org/watchmen-ii.htm.

———. 'Cyber-Rights & Cyber-Liberties (UK) Report, Who Watches the Watchmen'. *Cyber-Rights & Cyber-Liberties*, November 1997. http://web.archive.org/web/200012031831/http://www.leeds.ac.uk/law/pgs/yaman/watchmen.htm.

———. *Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States*. Organisation for Security and Cooperation in Europe, 2011. http://www.osce.org/fom/80723.

———. 'Governing Racist Content on the Internet: National and International Responses'. *University of New Brunswick Law Journal* 56 (2007): 103.

———. *Internet Child Pornography and the Law: National and International Responses*. Aldershot: Ashgate, 2008.

———. 'Internet Content Regulation: UK Government and the Control of Internet Content'. *Computer Law & Security Report* 17, no. 5 (30 September 2001): 303.

———. *Sex on the Net: The Dilemma of Policing Cyberspace*. Behind the Headlines. London: South Street, 1999.

———. 'The Regulation of Pornography and Child Pornography on the Internet'. *The Journal of Information Law and Technology* 2, no. 1 (1997). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1.

———. '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): 260.

———. 'Who Watches the Watchmen? The Role of Filtering Software in Internet Content Regulation'. In *The Media Freedom Internet Cookbook*. Vienna: Organisation for Security and Cooperation in Europe, 2004. http://www.osce.org/publications/rfm/2004/12/12239_89_en.pdf.

All Party Parliamentary Communications Group. *Can We Keep Our Hands off the Net? Report of an Inquiry by the All Party Parliamentary Communications Group*. London, 2009. www.apcomms.org.uk/uploads/apComms_Final_Report.pdf.

'apComms Inquiry into Internet Traffic: Third Oral Evidence Session', 7 July 2009. http://www.apcomms.org.uk/uploads/090707_apComms_Oral_Evidence_-_3.doc.

Arthur, Charles. 'Internet Watch Foundation Reconsiders Wikipedia Censorship'. *The Guardian*, 9 December 2008. http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-censorship-iwf-reconsiders.

Article 29 Data Protection Working Party. 'Opinion 2/2006 on Privacy Issues Related to the Provision of Email Screening Services', 21 February 2006. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_en.pdf.

Bailey, Jane. 'Confronting Collective Harm: Technology's Transformative Impact on Child Pornography'. *University of New Brunswick Law Journal* 56 (2007): 65.

Baldwin, Robert, and Martin Cave. *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press, 1999.

Bambauer, Derek. 'Cybersieves'. *Duke Law Journal* 59, no. 3 (2009): 477.

———. 'Filtering in Oz: Australia's Foray into Internet Censorship', December 2008. http://ssrn.com/abstract=1319466.

———. 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering', 2008. http://ssrn.com/paper=1143582.

Bambauer, Derek E. 'Orwell's Armchair'. *University of Chicago Law Review* 79 (2012): 863.

Banisar, David. *Speaking of Terror*. Strasbourg: Council of Europe, 2008. http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

Barlow, John Perry. 'A Declaration of the Independence of Cyberspace', 8 February 1996. http://homes.eff.org/~barlow/Declaration-Final.html.

———. 'Thinking Locally, Acting Globally'. *Time*, 15 January 1996. http://www.time.com/time/magazine/article/0,9171,983964,00.html.

Barron, Anne. '"Graduated Response" À l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010'. *Journal of Media Law* 3, no. 2 (2011): 305.

Bartle, Ian, and Peter Vass. *Self-Regulation and the Regulatory State - a Survey of Policy and Practice*. Bath: Centre for the Study of Regulated Industries, 2005. http://www.bath.ac.uk/management/cri/pubpdf/Research_Reports/17_Bartle_Vass.pdf.

———. 'Self-Regulation within the Regulatory State: Towards a New Regulatory Paradigm?' *Public Administration* 85 (December 2007): 885–905.

Beattie, Scott. *Community, Space and Online Censorship: Regulating Pornotopia*. Farnham: Ashgate, 2009.

Bendrath, Ralf, and Milton Mueller. 'The End of the Net as We Know It? Deep Packet Inspection and Internet Governance'. *New Media & Society* 13 (27 April 2011).

Birnhack, Michael D., and Niva Elkin-Koren. 'The Invisible Handshake: The Reemergence of the State in the Digital Environment'. *Virginia Journal of Law and Technology* 8 (2003): 6.

Bits of Freedom. 'Dutch Providers Abandon "ineffective" Web Blocking', 7 March 2011. https://www.bof.nl/2011/03/07/dutch-providers-abandon-ineffective-web-blocking/.

Black, Julia. 'Constitutionalising Self Regulation'. *Modern Law Review* 59 (1996): 24.

———. 'Legitimacy and the Competition for Regulatory Share', 23 June 2009. http://ssrn.com/abstract=1424654.

Bourke, Michael, and Andres Hernandez. 'The "Butner Study" Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders'. *Journal of Family Violence* 24, no. 3 (1 April 2009): 183.

Bowcott, Owen. 'Police Move on Internet Porn'. *The Guardian*, 27 July 1995.

Boyle, James. 'Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors'. *University of Cincinnati Law Review* 177 (1997): 186.

Brandon, James. *Virtual Caliphate: Islamic Extremists and Their Websites*. London: Centre for Social Cohesion, 2008.

Breindl, Yana. *Internet Content Regulation in Liberal Democracies: A Literature Review*. DH Forschungsverbund – Working Papers Zu Digital Humanities 2. Göttingen: Göttingen Centre for Digital Humanities, 2013. http://www.gcdh.de/files/1113/6549/2342/YBreindl_Literature_Review_Mar2013_final.pdf.

Bright, Martin. 'BT Puts Block on Child Porn Sites'. *The Observer*, 6 June 2004. http://www.guardian.co.uk/technology/2004/jun/06/childrensservices.childprotection.

Broadband Stakeholder Group. 'Voluntary Industry Code of Practice on Traffic Management Transparency for Broadband Services', March 2011. http://www.broadbanduk.org/component/option,com_docman/task,doc_details/gid,1335/Itemid,63/.

Brown, Ian. 'Internet Filtering: Be Careful What You Ask for'. In *Freedom and Prejudice: Approaches to Media and Culture*, edited by Süheyla Kirca Schroeder and LuEtt Hanson. Istanbul: Bahcesehir University Press, 2008.

Brownsword, Roger. 'Code, Control, and Choice: Why East Is East and West Is West'. *Legal Studies* 25 (2005): 1.

———. *Rights, Regulation, and the Technological Revolution*. Oxford: Oxford University Press, 2008.

'BT Sounds Child Web Porn Warning'. *BBC News*, 7 February 2006. http://news.bbc.co.uk/1/hi/uk/4687904.stm.

Cairo, Anna, and Rowan Wilken. 'The Australian Government Internet Filter: Its Scope, and Its Potential Civil Liberties Implications'. *Telecommunications Journal of Australia* 62, no. 2 (2012). http://tja.org.au/tja/index.php/tja/article/view/308.

Callanan, Cormac, Marco Grecke, Estelle De Marco, and Hein Dreis-Ziekenheiner. *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies*. Dublin: Aconite Internet Solutions, 2009. http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf.

Cameron, David. 'The Internet and Pornography'. presented at the NSPCC, London, 22 July 2013. https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action.

Campbell, Colin D. 'The Nature of Power as Public in English Judicial Review'. *The Cambridge Law Journal* 68, no. 01 (2009): 90.

Cane, Peter. *Administrative Law*. 4th ed. Oxford: Oxford University Press, 2004.

Carlin, John. 'Flying Bimbo Leads Blitz on Cyberporn'. *The Independent*, 3 December 1995.

Carr, John. *Child Abuse, Child Pornography and the Internet*. London: NCH, 2004. http://www.make-it-safe.net/esp/pdf/Child_pornography_internet_Carr2004.pdf.

———. 'Submission Regarding Communications Bill', 10 June 2002. http://www.chis.org.uk/uploads/55.pdf.

———. Telephone interview, 16 November 2009.
Carr, John, and Zoe Hilton. ‘Combating Child Abuse Images on the Internet - International Perspectives’. In *Internet Child Abuse: Current Research and Policy*, edited by Julia Davidson and Peter Gottschalk. Abingdon: Routledge, 2011.
Carter, Stephen. *Digital Britain: Final Report*. London, 2009.
Cave, Jonathan, Christopher Marsden, and Steve Simmons. *Options for and Effectiveness of Internet Self- and Co-Regulation*. Santa Monica: RAND, 2008. http://www.rand.org/pubs/technical_reports/TR566/.
Chakrabarti, Shami. ‘A Thinning Blue Line? Police Independence and the Rule of Law’. *Policing* 2, no. 3 (2008): 367.
Cheung, Anne, and Rolf H. Weber. ‘Internet Governance and the Responsibility of Internet Service Providers’. *Wisconsin International Law Journal* 26, no. 2 (2008).
Child Exploitation and Online Protection Centre. ‘A Picture of Abuse: A Thematic Assessment of the Risk of Contact Child Sexual Abuse Posed by Those Who Possess Indecent Images of Children’, June 2012. http://ceop.police.uk/Documents/ceopdocs/CEOP%20IIOCTA%20Executive%20Summary.pdf.
‘Child Pornography Complaint in Google Search’. *Chilling Effects Clearinghouse*, 2009. http://www.chillingeffects.org/notice.cgi?sID=1161.
CIRCAMP. ‘CIRCAMP Fact Sheet English’. *CIRCAMP*. Accessed 20 July 2010. http://circamp.eu/index.php?option=com_content&view=article&id=15:circamp-fact-sheet-english&catid=1:project&Itemid=2.
———. ‘CIRCAMP Overview’. *CIRCAMP*. Accessed 27 March 2010. http://circamp.eu/index.php?option=com_content&view=article&id=11:circamp-overview&catid=1:project&Itemid=2.
Clayton, Richard. ‘Anonymity and Traceability in Cyberspace’. PhD, University of Cambridge, 2005. http://www.cl.cam.ac.uk/~rnc1/thesis.pdf.
———. ‘Clause 53 of the Sexual Offences Bill: The Problem of “Making”’. FIPR, 23 March 2003. http://www.cl.cam.ac.uk/~rnc1/SexualOffencesBill.pdf.
———. ‘Failures in a Hybrid Content Blocking System’. presented at the Workshop on Privacy Enhancing Technologies, Dubrovnik, 30 June 2005. http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.
———. ‘Technical Aspects of the Censoring of Wikipedia’. *Light Blue Touchpaper*, 11 December 2008. http://www.lightbluetouchpaper.org/2008/12/11/technical-aspects-of-the-censoring-of-wikipedia/.
‘Cleanfeed (content Blocking System)’. *Wikipedia*, 15 June 2013. http://en.wikipedia.org/w/index.php?title=Cleanfeed_(content_blocking_system)&oldid=555796381.
Colcolough, Don. ‘Investigating and Prosecuting Computer Facilitated Crimes Against Children: An AOL Perspective’. presented at the 2009 National Children’s Alliance NCA NET, 28 May 2009. http://www.childrensmn.org/web/mrcac/handouts/184933.pdf.

Collins, Barry. ‘Charity: Child Abuse Filters Save Men from Themselves’. *PC Pro*, 23 February 2009. http://www.pcpro.co.uk/news/248117/charity-child-abuse-filters-save-men-from-themselves/print.

Collins, Richard. ‘Networks, Markets and Hierarchies: Governance and Regulation of the UK Internet’. *Parliamentary Affairs* 59, no. 2 (1 April 2006): 314.

———. ‘Three Myths of Internet Governance Considered in the Context of the UK’. *Prometheus* 22, no. 3 (2004): 267.

Committee of Ministers of the Council of Europe. ‘Declaration of the Committee of Ministers on Network Neutrality’, 29 September 2010. https://wcd.coe.int/ViewDoc.jsp?id=1678287.

———. ‘Declaration on Freedom of Communication on the Internet’, 28 May 2003. https://wcd.coe.int/ViewDoc.jsp?id=37031.

———. ‘Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters’, 26 March 2008. https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6.

———. ‘Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines’, 4 April 2002. https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)3.

———. ‘Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services’, 2012. https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2012)4.

———. ‘Recommendation Rec(2001)8 on Self-Regulation Concerning Cyber Content (self-Regulation and User Protection against Illegal or Harmful Content on New Communications and Information Services)’, 5 September 2001. https://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2001)8.

Committee on Energy and Commerce. *Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites.* Washington, DC: US Government Printing Office, 2006. http://ftp.resource.org/gpo.gov/hearings/109h/30530.txt.

Connell, Francis J. ‘Censorship and the Prohibition of Books in Catholic Church Law’. *Columbia Law Review* 54 (1954): 699.

Connett, David, and Jon Henley. ‘These Men Are Not Paedophiles: They Are the Internet Abusers’. *The Observer*, 25 August 1996.

Cooke, Louise. ‘Controlling the Net: European Approaches to Content and Access Regulation’. *Journal of Information Science*, 33, no. 3 (2007): 360.

Cormack, Andrew. Telephone interview, 30 July 2009.

Cornford, Tom. ‘The New Rules of Procedure for Judicial Review’. *Web Journal of Current Legal Issues* 5 (2000). http://webjcli.ncl.ac.uk/2000/issue5/cornford5.html.

Craig, Paul. ‘The Legal Effect of Directives: Policy, Rules and Exceptions’. *European Law Review* 34, no. 3 (2009): 349.

Crawford, Adam. ‘Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security’. *Theoretical Criminology* 10, no. 4 (November 2006): 449–79.

Crown Prosecution Service. ‘Indecent Photographs of Children: Legal Guidance’, August 2010. http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/.

———. ‘Obscene Publications: Legal Guidance’, March 2010. http://www.cps.gov.uk/legal/l_to_o/obscene_publications/.

Crown Prosecution Service, and Association of Chief Police Officers. ‘Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) Concerning Section 46 Sexual Offences Act 2003’, 6 October 2004. http://www.iwf.org.uk/documents/20041015_mou_final_oct_2004.pdf.

CSMG. *Study into Websites Sharing Internet Protocol Addresses*, 26 April 2012. http://stakeholders.ofcom.org.uk/binaries/internet/websites-sharing.pdf.

Daintith, Terence. ‘Regulation by Contract: The New Prerogative’. *Current Legal Problems*, 1979, 41.

Daly, Angela. ‘Private Power and New Media: The Case of the Corporate Suppression of WikiLeaks and Its Implications for the Exercise of Fundamental Rights on the Internet’. In *Human Rights and Risks in the Digital Era*, edited by Christina M. Akrivopoulou and Nicolaos Garipidis. IGI Global, 2012.

Darlington, Roger. ‘Chairing The Internet Watch Foundation’. *Roger Darlington’s Homepage*. Accessed 21 July 2009. http://www.rogerdarlington.co.uk/iwf.html.

———. ‘How the Internet Could Be Regulated’, 7 January 2009. http://www.rogerdarlington.co.uk/Internetregulation.html.

———. ‘IWF Newsgroup Policy’, 18 July 2001. http://web.archive.org/web/20040308014713/http://www.iwf.org.uk/about/policies/ngpolrep.htm.

———. ‘Should the Internet Be Regulated?’, 25 February 2010. http://www.rogerdarlington.me.uk/regulation.html.

Davies, CJ. ‘The Hidden Censors of the Internet’. *Wired*, 20 May 2009. http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet.aspx?page=all.

Deibert, Ronald, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Denied*. Cambridge, MA: MIT Press, 2008.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010.

Demeyer, Karel, Eva Lievens, and Jos Dumortier. ‘Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective’. *Policy & Internet* 4, no. 3–4 (2012): 1.

Department for Culture, Media and Sport. ‘Ofcom to Review Aspects of Digital Economy Act’. *Inside Government*, 1 February 2011. https://www.gov.uk/government/news/ofcom-to-review-aspects-of-digital-economy-act.

———. ‘Tackling Illegal Images - New Proactive Approach to Seek out Child Sexual Abuse Content’. *GOV.UK*, 18 June 2013.

https://www.gov.uk/government/news/tackling-illegal-images-new-proactive-approach-to-seek-out-child-sexual-abuse-content.

Department for Trade and Industry and Department for Culture, Media and Sport. *A New Future for Communications*. London: HMSO, 2000.

Dickson, Brice. 'Positive Obligations and the European Court of Human Rights'. *Northern Ireland Legal Quarterly* 61 (2010): 203.

Digital Rights Ireland. 'Garda Plans for Web Blocking Referred to Data Protection Commissioner'. *Digital Rights Ireland*, 29 March 2011. http://www.digitalrights.ie/2011/03/29/garda-plans-for-web-blocking-referred-to-data-protection-commissioner/.

Donnelly, Catherine. 'Positive Obligations and Privatisation'. *Northern Ireland Legal Quarterly* 61 (2010): 209.

DTI. 'DTI Press Release P/96/636', 14 August 1996. http://www.mit.edu/activities/safe/cases/demon/minister-statement.txt.

Dyson, Esther, George Gilder, George Keyworth, and Alvin Toffler. 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2)'. *Future Insight*, August 1994. http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html.

Edwards, Lilian. 'From Child Porn to China, in One Cleanfeed'. *SCRIPT-Ed* 3, no. 3 (September 2006).

———. 'IWF v Wikipedia and the Rest of the World (except OUT-LAW)'. *panGloss*, 15 December 2008. http://blogscript.blogspot.com/2008/12/iwf-v-wikipedia-and-rest-of-world.html.

———. 'Pornography, Censorship and the Internet'. In *Law and the Internet*, edited by Lilian Edwards and Charlotte Waelde, 3rd ed. Oxford: Hart Publishing, 2009.

———. 'Section 127 of the Communications Act 2003: Threat or Menace?' *Society for Computers and Law*, 9 October 2012. http://www.scl.org/site.aspx?i=ed28102.

———. 'The Fall and Rise of Intermediary Liability Online'. In *Law and the Internet*, edited by Lilian Edwards and Charlotte Waelde, 3rd ed. Oxford: Hart Publishing, 2009.

Elmer-Dewitt, Philip. 'On a Screen near You: Cyberporn'. *Time*, 3 July 1995.

Eneman, Marie. 'Internet Service Provider (ISP) Filtering of Child-Abusive Material: A Critical Reflection of Its Effectiveness'. *Journal of Sexual Aggression: An International, Interdisciplinary Forum for Research, Theory and Practice* 16, no. 2 (2010): 223.

Espiner, Tom. 'IWF Chief: Why Wikipedia Block Went Wrong'. *ZDNet.co.uk*, 20 February 2009. http://news.zdnet.co.uk/internet/0,1000000097,39616171,00.htm.

Ezor, Jonathan I. 'Busting Blocks: Revising 47 U.S.C. §230 To Address The Effective Lack Of Legal Recourse For Wrongful Inclusion In Spam Filters Under U.S. Law'. *ExpressO*, 2010. http://works.bepress.com/jonathan_ezor/1.

Fagelman, Tony. 'Commercialising the CAI Database - Recommendations from the Board and FC Working Group', 10 February 2005. http://web.archive.org/web/20050310190021/http://www.iwf.org.uk/corporate/page.128.277.htm.

Feather, Clive. ‘Home Office Meeting of January 19th’. *Clive Feather’s Home Page*. Accessed 14 January 2009. http://www.davros.org/homeoffice/.

———. ‘Re: Cleanfeed and Wikipedia’, 8 December 2008. http://markmail.org/message/jmmztsegqpcjykns.

Federal Communications Commission. ‘In the Matter of Preserving the Open Internet: Broadband Industry Practices’, 21 December 2010. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.

Feintuck, Mike, and Mike Varney. *Media Regulation, Public Interest and the Law*. 2nd ed. Edinburgh: Edinburgh University Press, 2006.

Fenwick, Helen, and Gavin Phillipson. *Media Freedom under the Human Rights Act*. Oxford: Oxford University Press, 2006.

Fiveash, Kelly. ‘Health Minister Warns ISPs: Block Suicide Websites or Face Regulation’. *The Register*, 10 September 2012. http://www.theregister.co.uk/2012/09/10/norman_lamb_calls_for_isps_to_block_suicide_websites/.

Foo, Fran. ‘ACMA Takes Aim at Whirlpool, Supplier’. *The Australian*, 13 March 2009. http://www.australianit.news.com.au/story/0,24897,25181408-15306,00.html.

Freeman, Jody. ‘Private Parties, Public Functions and the New Administrative Law’. *Administrative Law Review* 52, no. 3 (2000): 813.

———. ‘The Contracting State’. *Florida State University Law Review* 28 (2000): 155.

Garside, Juliette. ‘Ministers Will Order ISPs to Block Terrorist and Extremist Websites’. *The Guardian*, 27 November 2013. http://www.theguardian.com/uk-news/2013/nov/27/ministers-order-isps-block-terrorist-websites.

Gearty, Conor. *Principles of Human Rights Adjudication*. Oxford University Press, 2004.

Gellman, Robert. ‘Disintermediation and the Internet’. *Government Information Quarterly* 13, no. 1 (1996): 1.

Ghosh, Shona. ‘Rights-Holders Taking down Legitimate Sites in Piracy Crackdown’. *PC Pro*, 14 August 2013. http://www.pcpro.co.uk/news/broadband/383614/rights-holders-taking-down-legitimate-sites-in-piracy-crackdown.

———. ‘Sky Blocks News Site after DNS Exploit’. *PC Pro*, 12 August 2013. http://www.pcpro.co.uk/news/broadband/383587/sky-blocks-news-site-after-dns-exploit.

Gibbs, Samuel. ‘UK’s Top Tech Executives Meet for Summit against Online Child Abuse’. *The Guardian*, 18 November 2013. http://www.theguardian.com/technology/2013/nov/18/uk-top-tech-executives-online-child-abuse.

Gibson, Allan, Gareth Patterson, Harriet Dempster, Mike Balcombe, and Chris Mayle. ‘Inspection of the Internet Watch Foundation’, 30 March 2011. http://www.iwf.org.uk/assets/media/news/Inspection%20of%20the%20IWF%202011.pdf.

Gillespie, Alisdair. *Child Exploitation and Communication Technologies*. Lyme Regis: Russell House Publishing, 2008.

———. ‘Child Pornography: Balancing Substantive and Evidential Law to Safeguard Children Effectively from Abuse’. *International Journal of Evidence & Proof* 9, no. 1 (March 2005): 29–49.
Global Network Initiative. ‘Implementation Guidelines’, 2008. http://www.globalnetworkinitiative.org/implementationguidelines/index.php.
———. ‘Principles’, 2008. http://globalnetworkinitiative.org/principles/index.php.
Godwin, Mike. ‘Why IWF’s Wikipedia Reversal Is Not Enough’, 12 December 2008. http://archive.is/GbiOi.
Goldman, Eric. ‘47 USC 230(c)(2) and Immunity for Online Filtering’. 2009. http://www.ericgoldman.org/Speeches/47usc230c2.pdf.
Goldsmith, Jack. ‘Against Cyberanarchy’. In *Who Rules the Net*, edited by Adam D. Thierer and Clyde Wayne Crews. Washington, D.C.: Cato Institute, 2003.
Goldsmith, Jack L, and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press, 2006.
Goodin, Dan. ‘Finland Censors Anti-Censorship Site’. *The Register*, 18 February 2008. http://www.theregister.co.uk/2008/02/18/finnish_policy_censor_activist/.
Goodwins, Rupert. ‘UK ISPs Switch on Mass Wikipedia Censorship’. *ZDNet.co.uk*, 6 December 2008. http://community.zdnet.co.uk/blog/0,1000000567,10009938o-2000331777b,00.htm.
Gordon, Richard, and Tim Ward. *Judicial Review & the Human Rights Act*. Routledge, 2000.
Gould, Mark. ‘An Island in the Net: Domain Naming and English Administrative Law’. *John Marshall Journal of Computer & Information Law* 15 (1997): 493.
Grabosky, Peter. ‘Using Non-Governmental Resources to Foster Regulatory Compliance’. *Governance* 8, no. 4 (1995): 527.
Gracey, Mark. ‘Censorship or Common Sense?’ presented at the Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities, Oxford Internet Institute, 8 September 2005. http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/mark_gracey.pdf.
Graham, Georgia. ‘Embarrassed Husbands Will Have to Discuss Plans to Watch Online Porn with Their Wives, Says David Cameron’. *The Telegraph*, 18 November 2013. http://www.telegraph.co.uk/technology/google/10457726/Embarrassed-husbands-will-have-to-discuss-plans-to-watch-online-porn-with-their-wives-says-David-Cameron.html.
Graham, Irene. ‘Will PICS Torch Free Speech on the Internet?’ *Communications Law Bulletin* 17, no. 1 (1998): 11.
Griffin, James. ‘The Effect of the Digital Economy Act 2010 upon “Semiotic Democracy”’. *International Review of Law, Computers & Technology* 24, no. 3 (November 2010): 251.
Grimmelmann, James. ‘Regulation by Software’. *Yale Law Journal* 114 (2005): 1719.
Grossman, Wendy. ‘IWF Reforms Could Pave Way for UK Net Censorship’. *The Register*, 29 December 2006. http://www.theregister.co.uk/2006/12/29/iwf_feature/.

———. ‘IWF: What Are You Looking At?’ *The Independent*, 25 March 2002. http://www.independent.co.uk/news/business/analysis-and-features/iwf-what-are-you-looking-at-655425.html.
———. ‘The Great Firewall of Britain’. *Net.wars*, 24 November 2006. http://www.pelicancrossing.net/netwars/2006/11/the_great_firewall_of_britain.html.
———. ‘Watching the Internet Watchers’. *The Inquirer*, 15 February 2002. http://www.theinquirer.net/inquirer/news/1017543/watching-the-internet-watchers.
Grubb, Ben. ‘How ASIC’s Attempt to Block One Website Took down 250,000’. *The Sydney Morning Herald*, 5 June 2013. http://www.smh.com.au/technology/technology-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html.
GSMA Mobile Alliance Against Child Sexual Abuse Content. ‘Implementation of Filtering of Child Sexual Abuse Images in Operator Networks’, November 2008. www.gsmworld.com/documents/GSMA_Child_Tech_Doc.pdf.
Hadfield, Greg. ‘Internet Firms Are Told to Switch off the Filth’. *Daily Mail*, 30 December 1995.
Hannan, Martin. ‘Caught in the Sordid Net of Cybersex’. *The Scotsman*, 27 July 1995.
Hans-Bredow-Institut. *Study on Co-Regulation Measures in the Media Sector: Final Report*. Hamburg: University of Hamburg, 2006. http://ec.europa.eu/avpolicy/docs/library/studies/coregul/final_rep_en.pdf.
Harden, Ian. *The Contracting State*. Buckingham: Open University Press, 1992.
Hardy, I. Trotter. ‘The Proper Legal Regime for Cyberspace’. *University of Pittsburgh Law Review* 55 (1993): 993.
Hargrave, Sean. ‘Surfing with a Safety Net’. *The Guardian*, 29 June 2006. http://www.guardian.co.uk/technology/2006/jun/29/guardianweeklytechnologysection.
Harris, David, Michael O’Boyle, Ed Bates, and Carla Buckley. *Law of the European Convention on Human Rights*. 2nd ed. Oxford: Oxford University Press, 2009.
Headdon, Toby. ‘Beyond Liability: Injunctions after L’Oreal v eBay’. *Computers and Law* 22, no. 3 (2011): 26.
Heins, Marjorie. *Not in Front of the Children: ‘Indecency’, Censorship, and the Innocence of Youth*. 2nd ed. Rutgers University Press, 2007.
Higgins, Charlotte, and Vikram Dodd. ‘Tate Modern Removes Naked Brooke Shields Picture after Police Visit’. *The Guardian*, 30 September 2009. http://www.guardian.co.uk/artanddesign/2009/sep/30/brooke-shields-naked-tate-modern.
Home Office. *CONTEST - the United Kingdom’s Strategy for Countering Terrorism: Annual Report*. London: The Stationery Office, 2013.
———. ‘Press Release: Improving Child Protection on the Internet - A Partnership for Action’, 29 March 2001. http://www.cyber-rights.org/documents/safe_uk.htm.
———. *Prevent Strategy*. London: HMSO, 2011.
———. ‘Response to Freedom of Information Act Request Re Implementation of Terrorism Act 2006 to Internet Activity’. *WhatDoTheyKnow*, 23 July 2010.

http://www.whatdotheyknow.com/request/implementation_of_terrorism_act#incoming-102379.

———. ‘Response to Freedom of Information Act Request Re Internet Watch Foundation Audits’, 10 March 2009. http://www.whatdotheyknow.com/request/internet_watch_foundation_audits#incoming-20085.

———. ‘Response to Freedom of Information Act Request Re the Relationship between the Home Office and the IWF’. *What Do They Know?*, 1 January 2009. https://www.whatdotheyknow.com/request/relationship_between_the_home_of.

———. ‘Response to Freedom of Information Request Re the Relationship between the IWF and the Home Office and Network Level Blocking’, 26 February 2009. https://www.whatdotheyknow.com/request/relationship_between_the_home_of.

Hood, Christopher, Henry Rothstein, and Robert Baldwin. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press, 2004.

House of Commons, Home Affairs Committee. *First Report on Computer Pornography*. London: HMSO, 1994.

House of Commons, Select Committee on Culture, Media and Sport. *The Multi-Media Revolution*. London: HMSO, 1998.

House of Lords, Select Committee on Science and Technology. *Information Society: Agenda for Action in the United Kingdom*. London: HMSO, 1996.

Hudson, Anthony. ‘Advice in Relation to Usenet Newsgroup Names and Website Addresses’, 16 July 2002.

Hunt, Murray. ‘Constitutionalism and the Contractualisation of Government in the United Kingdom’. In *The Province of Administrative Law*, edited by Michael Taggart. Oxford: Hart Publishing, 1997.

Hunter, Philip. ‘BT’s Bold Pioneering Child Porn Block Wins Plaudits amid Internet Censorship Concerns’. *Computer Fraud & Security* 2004, no. 9 (2004): 4.

Husovec, Martin. ‘In Rem Injunctions: Case of Website Blocking’, 28 April 2013. http://papers.ssrn.com/abstract=2257232.

Hutty, Malcolm. ‘89% Say ISPs Should Track Access to Paedophile Sites’. *LINX Public Affairs*, 16 March 2005. https://publicaffairs.linx.net/news/?p=281.

———. ‘Cleanfeed: The Facts’. *LINX Public Affairs*, 10 September 2004. https://publicaffairs.linx.net/news/?p=154.

———. ‘IWF Human Rights Review’. *LINX Public Affairs*, 26 November 2013. https://publicaffairs.linx.net/news/?cat=20.

Hynönen, Kalle. ‘No More Mere Conduit? Abandoning Net Neutrality and Its Possible Consequences on Internet Service Providers’ Content Liability’. *Journal of World Intellectual Property* 16, no. 1–2 (2013): 72.

International Telecommunication Union. ‘Guidelines for Policy Makers on Child Online Protection’, 2009. http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/policy_makers/policy_makers.pdf.

Internet Service Providers Association, LINX, and Safety-Net Foundation. ‘R3 - Rating, Reporting, Responsibility for Child Pornography and Illegal Material on the Internet’, 23 September 1996. http://www.mit.edu/activities/safe/labeling/r3.htm.

Internet Watch Foundation. ‘2000 Annual Report’, 2001.
———. ‘2006 Annual Report’, 2007. http://www.iwf.org.uk/documents/20070412_iwf_annual_report_2006_%28web%29.pdf.
———. ‘2010 Annual Report’, 2011. http://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf.
———. ‘2011 Annual Report’, 2012. https://www.iwf.org.uk/assets/media/annual-reports/annual%20med%20res.pdf.
———. ‘About Us’, 2013. http://www.iwf.org.uk/about-iwf.
———. ‘Blocking Good Practice’, 2011. http://www.iwf.org.uk/services/blocking/blocking-good-practice.
———. ‘Blocking of Child Sexual Abuse Websites’, 18 June 2009. http://www.iwf.org.uk/public/page.148.htm.
———. ‘Board Minutes 1 December 2009’, 1 December 2009. http://www.iwf.org.uk/accountability/governance/board-minutes/2009-board-minutes/1-december-2009.
———. ‘Board Minutes 11 July 2006’, 11 July 2006. http://web.archive.org/web/20061111152429/http://www.iwf.org.uk/corporate/page.163.htm.
———. ‘Board Minutes 12 February 2002’, 12 February 2002. http://web.archive.org/web/20020403125653/http://www.iwf.org.uk/about/bd12-02mins.htm.
———. ‘Board Minutes 12 July 2000’, 12 July 2000. http://web.archive.org/web/20020223200050/http://www.iwf.org.uk/about/board/board120700.htm.
———. ‘Board Minutes 12 October 2004’, 12 October 2004. http://web.archive.org/web/20050308060749/http://www.iwf.org.uk/corporate/page.121.htm.
———. ‘Board Minutes 16 October 2012’, 16 October 2012. https://www.iwf.org.uk/assets/media/accountability/board/Minutes%2016%20October%202012%20Web.pdf.
———. ‘Board Minutes 18 July 2001’, 18 July 2001. http://web.archive.org/web/20040810233237/http://www.iwf.org.uk/about/policies/minutes_180701.html.
———. ‘Board Minutes 20 November 2012’, 20 November 2012. https://www.iwf.org.uk/assets/media/accountability/board/IWF%20Board%20Meeting%20Minutes%2020%20November%202012.pdf.
———. ‘Board Minutes 22 July 2003’, 22 July 2003. http://web.archive.org/web/20040810234039/http://www.iwf.org.uk/about/policies/minutes_220703.htm.
———. ‘Board Minutes 25 April 2001’, 25 April 2001.
———. ‘Board Minutes 25 Nov 2008’. *Internet Watch Foundation*, 25 November 2008. http://iwf.org.uk/corporate/page.200.htm.

———. ‘Board Minutes 25 November 2008’, 25 November 2008. http://www.iwf.org.uk/accountability/governance/board-minutes/2008-board-minutes/25-november-2008.
———. ‘Board Minutes 27 January 2009’, 27 January 2009. http://www.iwf.org.uk/accountability/governance/board-minutes/2009-board-minutes/27-january-2009.
———. ‘Board Minutes 27 November 2007’, 27 November 2007. http://www.iwf.org.uk/accountability/governance/board-minutes/2007-board-minutes/27-november-2007.
———. ‘Board Minutes 28 May 2013’, 28 May 2013. https://www.iwf.org.uk/assets/media/accountability/board/Final%20IWF%20Board%20Meeting%20approved%20amended%20Minutes%2028May2013%20web%20version.pdf.
———. ‘Board Minutes 29 September 2009’. *Internet Watch Foundation*, 29 September 2009. http://www.iwf.org.uk/corporate/page.215.617.htm.
———. ‘Board Minutes 29 September 2009’, 29 September 2009. http://www.iwf.org.uk/accountability/governance/board-minutes/2009-board-minutes/29-september-2009.
———. ‘Board Minutes 30 March 2010’, 30 March 2010. http://www.iwf.org.uk/accountability/governance/board-minutes/2010-board-minutes/board-30-march-2010.
———. ‘Board Minutes 8 February 2011’, 8 February 2011. http://www.iwf.org.uk/accountability/governance/board-minutes/2011-board-meetings/board-minutes-8-february-2011.
———. ‘Board Minutes 8 July 2008’. *Internet Watch Foundation*, 8 July 2008. http://www.iwf.org.uk/corporate/page.203.595.htm.
———. ‘Board Minutes 9 December 2008’, 9 December 2008. http://www.iwf.org.uk/accountability/governance/board-minutes/2008-board-minutes/9-december-2008.
———. ‘Catherine Crawford OBE’. Accessed 8 December 2013. https://www.iwf.org.uk/accountability/governance/board-biographies/catherine-crawford.
———. ‘Chief Executive’s Report 14 May 2002’, 14 May 2002. http://web.archive.org/web/20020820125010/http://www.iwf.org.uk/about/CEO05-02.htm.
———. ‘Chief Executive’s Report 26 April 2005’, 26 April 2005. http://web.archive.org/web/20051227133042/http://www.iwf.org.uk/corporate/page.141.299.htm.
———. ‘Child Sexual Abuse Content URL List’, 10 April 2008. http://www.iwf.org.uk/corporate/page.49.233.htm.
———. ‘Child Sexual Abuse Content URL Service: Complaints, Appeals and Correction Procedures’, 7 December 2008. http://www.iwf.org.uk/public/page.148.341.htm.
———. ‘Code of Practice for Full Members’, January 2004.

———. ‘Combating Online Child Sexual Abuse Content at National and International Levels: IWF Experience, Tactical Suggestions and Wider Considerations’, 2010. http://www.iwf.org.uk/resources/tactical-briefing.
———. ‘Content Assessment Appeal Process’, 2010. http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process.
———. ‘FAQs Regarding the IWF’s Facilitation of the Blocking Initiative’, 2011. http://www.iwf.org.uk/services/blocking/blocking-faqs.
———. ‘Financial Statements for the Year Ended 31 March 2011’, 2011. https://www.iwf.org.uk/assets/media/accounts/2011%20IWF%20Final%20typesigned.pdf.
———. ‘Incitement to Racial Hatred Removed from IWF’s Remit’. *Internet Watch Foundation*, 11 April 2011. http://www.iwf.org.uk/about-iwf/news/post/302-incitement-to-racial-hatred-removed-from-iwfs-remit.
———. ‘Internet Watch Foundation (IWF) Brand Guidelines’. Accessed 15 February 2011. http://www.iwf.org.uk/resources/brand-guidelines#IWFMemberCompanies:Splashpages.
———. ‘Internet Watch Foundation Trustees’. Accessed 8 December 2013. http://www.iwf.org.uk/accountability/governance/board-biographies.
———. ‘IWF Facilitation of the Blocking Initiative’. *Internet Watch Foundation*, 4 January 2010. http://www.iwf.org.uk/public/page.148.437.htm.
———. ‘IWF Governance’. *Internet Watch Foundation*, 14 December 2009. http://www.iwf.org.uk/public/page.103.550.htm.
———. ‘IWF Highlights’. *Internet Watch Foundation*, 2011. http://www.iwf.org.uk/about-iwf/iwf-history/iwf-highlights.
———. ‘IWF Ready to Step up the Fight against Online Child Sexual Abuse Content’, 18 June 2013. http://www.iwf.org.uk/about-iwf/news/post/360-iwf-ready-to-step-up-the-fight-against-online-child-sexual-abuse-content.
———. ‘IWF Response to the Byron Review’, 2007. http://www.iwf.org.uk/accountability/consultations/byron-review-2007.
———. ‘IWF URL List Policy and Procedures’. Accessed 15 February 2011. http://www.iwf.org.uk/services/blocking/iwf-url-list-policy-and-procedures.
———. ‘IWF URL List Recipients’. *Internet Watch Foundation*, 2011. http://www.iwf.org.uk/services/blocking/iwf-list-recipients.
———. ‘Minutes of Board Meeting’, 16 January 2007. http://www.iwf.org.uk/corporate/page.170.htm.
———. ‘Newsgroups’, 13 November 2008. http://www.iwf.org.uk/corporate/page.49.231.htm.
———. ‘Peter Neyroud CBE, QPM’. Accessed 8 December 2013. https://www.iwf.org.uk/accountability/governance/board-biographies/peter-neyroud-cbe-qpm.
———. ‘Philip Geering’. Accessed 8 December 2013. https://www.iwf.org.uk/accountability/governance/board-biographies/philip-geering.

———. ‘Police’. Accessed 10 December 2013. https://www.iwf.org.uk/partnerships/police.
———. ‘Rating And Filtering Internet Content: A United Kingdom Perspective’. *Internet Watch Foundation*, March 1998. http://web.archive.org/web/19990421120909/http://www.internetwatch.org.uk/rating/rating_r.html.
———. ‘Remit, Vision and Mission’. *Internet Watch Foundation*, 2011. http://www.iwf.org.uk/about-iwf/remit-vision-and-mission.
———. ‘Self-Regulation’. *Internet Watch Foundation*. Accessed 2 November 2011. https://www.iwf.org.uk/members/self-regulation.
———. ‘The Hotline and the Law’, 10 December 2007. http://www.iwf.org.uk/public/page.31.htm.
———. ‘Written Evidence to the Select Committee on European Union’, 20 February 2000. http://www.publications.parliament.uk/pa/ld199900/ldselect/ldeucom/95/95we35.htm.
Internet Watch Foundation, and Association of Chief Police Officers. ‘Service Level Agreement between the Association of Chief Police Officers (ACPO) and the Internet Watch Foundation (IWF)’, 5 October 2010. http://www.acpo.police.uk/documents/crime/2010/201010CRIIWF01.pdf.
Interpol. ‘Criteria for Inclusion in the List’. Accessed 25 February 2011. http://www.interpol.int/Public/THBInternetAccessBlocking/Criteria.asp.
Jackson, Mark. ‘Banned Piracy Website Expands BT Circumvention Tool to Include The Pirate Bay’. *ISP Review*, 6 October 2011. http://www.ispreview.co.uk/story/2011/10/06/banned-piracy-website-expands-bt-circumvention-tool-to-include-the-pirate-bay.html.
Jewkes, Yvonne, and Carol Andrews. ‘Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales’. *Policing & Society* 15, no. 1 (March 2005): 42.
Johnson, Bobbie. ‘Wikipedia Falls Foul of British Censors over Alleged Child Pornography’. *The Guardian*, 8 December 2008. http://www.guardian.co.uk/technology/2008/dec/08/wikipedia-censorship.
Johnson, David R., and David G. Post. ‘Law and Borders - The Rise of Law in Cyberspace’. *Stanford Law Review* 48 (1996): 1367.
Joint Committee on Human Rights. *Any of Our Business? Human Rights and the UK Private Sector*. London: HMSO, 2009.
Keene, David. ‘Principles of Deference under the Human Rights Act’. In *Judicial Reasoning under the UK Human Rights Act*, edited by Helen Fenwick, Gavin Phillipson, and Roger Masterman. Cambridge: Cambridge University Press, 2007.
Kelly, Sanja, and Sarah Cook, eds. *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*. Freedom House, 2011.
Kierkegaard, Sylvia. ‘To Block or Not to Block – European Child Porno Law in Question’. *Computer Law & Security Review* 27, no. 6 (2011): 573.

Klang, Mathias. *Disruptive Technology: Effects of Technology Regulation on Democracy*. Göteborg University, 2006. http://www.digital-rights.net/wp-content/uploads/2007/12/klang_thesis2.pdf.

Kleinschmidt, Broder. 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content'. *International Journal of Law and Information Technology* 18, no. 4 (2010): 332.

Klug, Francesca. 'Judicial Deference under the Human Rights Act 1998'. *European Human Rights Law Review*, 2003, 125.

Kobie, Nicole. 'BT to Warn Users Attempting to View Child Abuse Images'. *PC Pro*, 14 June 2013. http://www.pcpro.co.uk/news/security/382459/bt-to-warn-users-attempting-to-view-child-abuse-images.

Koops, Bert-Jaap, Miriam Lips, Sjaak Nouwt, Corien Prins, and Maurice Schellekens. 'Should Self-Regulation Be the Starting Point?' In *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, edited by Bert-Jaap Koops, Miriam Lips, Corien Prins, and Maurice Schellekens. The Hague: T.M.C. Asser Press, 2006.

Korff, Douwe, and Ian Brown. 'Social Media and Human Rights'. In *Human Rights and a Changing Media Landscape*. Council of Europe, 2011.

KPMG Peat Marwick, and Denton Hall. *Review of the Internet Watch Foundation*. London, February 1999.

Kraakman, Reinier. 'Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy'. *Journal of Law, Economics and Organization* 2, no. 1 (1 January 1986): 53.

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

Lahtinen, Sebastien. 'Be Unlimited Causes Stir in Effort of Blocking Child Abuse Images'. *Thinkbroadband.com*, 11 October 2007. http://www.thinkbroadband.com/news/3235-be-unlimited-causes-stir-in-effort-of-blocking-child-abuse-images.html.

Laidlaw, Emily. 'Internet Gatekeepers, Human Rights and Corporate Social Responsibilities'. London School of Economics and Political Science (LSE), 2012. http://etheses.lse.ac.uk/317/.

———. 'The Responsibilities of Free Speech Regulators: An Analysis of the Internet Watch Foundation'. *International Journal of Law and Information Technology* 20, no. 4 (2012): 312.

Lambers, Rik. 'Code and Speech: Speech Control Through Network Architecture'. In *Coding Regulation: Essays on the Normative Role of Information Technology*, edited by Egbert Dommering and Lodewijk Asscher. Information Technology & Law 12. The Hague: T.M.C. Asser Press, 2006.

Le Sueur, Andrew. 'Courts, Tribunals, Ombudsmen, ADR: Administrative Justice, Constitutionalism and Informality'. In *The Changing Constitution*, edited by Jeffrey Jowell and Dawn Oliver, 6th ed. Oxford: Oxford University Press, 2007.

Lee, Gia. ‘Addressing Anonymous Messages in Cyberspace’. *Journal of Computer-Mediated Communication* 2, no. 1 (1996). http://www.ascusc.org/jcmc/vol2/issue1/anon.html.

Leigh, Ian. ‘The Standard of Judicial Review after the Human Rights Act’. In *Judicial Reasoning under the UK Human Rights Act.*, edited by Helen Fenwick, Gavin Phillipson, and Roger Masterman. Cambridge: Cambridge University Press, 2007.

LeMay, Renai. ‘Interpol Filter Scope Creep: ASIC Ordering Unilateral Website Blocks’. *Delimiter*, 15 May 2013. http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/.

Leslie, Justin. ‘Approaches to Section 6 HRA: Lessons from Weaver v London and Quadrant Housing Trust’. *Judicial Review* 14, no. 4 (2009): 327.

Lessig, Lawrence. *Code: And Other Laws of Cyberspace*. New York, N.Y: Basic Books, 1999.

———. *Code: Version 2.0*. 2nd ed. New York: BasicBooks, 2006.

———. ‘The Spam Wars’. *The Industry Standard*, 31 December 1998. http://www.lessig.org/content/standard/0,1902,3006,00.html.

Leyden, John. ‘BT’s Modest Plan to Clean up the Net’. *The Register*, 7 June 2004. http://www.theregister.co.uk/2004/06/07/bt_cleanfeed_analysis/.

‘Lib Dem Peer on Why Site Blocking Is Needed’. *ZDNet.co.uk*, 4 March 2010. http://www.zdnet.co.uk/misc/print/0,1000000169,40070579-39001101c,00.htm.

Lievens, Eva, Jos Dumortier, and Patrick S. Ryan. ‘The Co-Protection of Minors in New Media: A European Approach to Co-Regulation’. *UC Davis Journal of Juvenile Law & Policy* 10 (2006): 97.

Lievens, Eva, and Peggy Valcke. ‘Regulatory Trends in a Social Media Context’. In *Routledge Handbook of Media Law*, edited by Monroe E Price and Stefaan Verhulst. Abingdon: Routledge, 2013.

LINX. ‘IWF to “proactively” Search for Illegal Content’. *LINX Public Affairs*, 20 June 2013. https://publicaffairs.linx.net/news/?p=9861.

Mac Sithigh, Daithi. ‘Co-Regulation, Video-on-Demand and the Legal Status of Audio-Visual Media’. *International Journal of Digital Television* 2, no. 1 (2011): 49–66.

———. ‘Datafin to Virgin Killer: Self-Regulation and Public Law’, 2009. http://ssrn.com/paper=1374846.

———. ‘Regulating the Medium: Reactions to Network Neutrality in the European Union and Canada’. *Journal of Internet Law* 14, no. 8 (2011): 3.

Maclay, Colin. ‘Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net?’ In *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*, edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: MIT Press, 2010.

Mann, Ronald J., and Seth R. Belzley. ‘The Promise of Internet Intermediary Liability’. *William and Mary Law Review* 47 (2005): 239.

Marsden, Christopher. 'Internet Co-Regulation and Constitutionalism: Towards European Judicial Review'. *International Review of Law, Computers & Technology* 26, no. 2–3 (2012): 211.

———. *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*. Cambridge: Cambridge University Press, 2011.

———. 'Net Neutrality Law: Past Policy, Present Proposals, Future Regulation?' Nusa Dua Bali, Indonesia, 2013. http://papers.ssrn.com/abstract=2335359.

———. *Net Neutrality: Towards a Co-Regulatory Solution*. London: Bloomsbury Academic, 2010.

———. 'Network Neutrality: A Research Guide'. In *Research Handbook on Governance of the Internet*, edited by Ian Brown. Cheltenham: Edward Elgar, 2013.

Marsden, Christopher, Steve Simmons, and Jonathan Cave. *Options for and Effectiveness of Internet Self- and Co-Regulation Inception Report*. RAND Europe, 30 April 2007. http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/inception_final.pdf.

Marsden, Christopher, Steve Simmons, Jonathan Cave, Eddy Nason, and Neil Robinson. *Options for and Effectiveness of Internet Self- and Co-Regulation Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet*. RAND Europe, 27 June 2007.

Marson, Ingrid. 'Child Porn: ISP Regulations Set for Commons Debate'. *Silicon.com*, 26 July 2005. http://www.silicon.com/management/cio-insights/2005/07/26/child-porn-isp-regulations-set-for-commons-debate-39150769/.

Martin, Nicole. 'Wikipedia Founder Considers Legal Action over Ban on "Pornographic" Album Cover'. *The Telegraph*, 9 December 2008. http://www.telegraph.co.uk/technology/3689527/Wikipedia-founder-considers-legal-action-over-ban-on-pornographic-album-cover.html.

'Max Mosley Wants Websites Closed down If They Flout New Press Watchdog Rules'. *The Mirror*, 19 March 2013. http://www.mirror.co.uk/news/uk-news/max-mosley-wants-websites-closed-1773836.

May, Matthew. 'Not in Front of the Children'. *The Times*, 11 August 1995.

May, Timothy C. 'Crypto Anarchy and Virtual Communities'. *Internet Security*, April 1995, 4–12.

McAuliffe, Wendy. 'IWF Lambasted for Plan to Ban Newsgroups'. *ZDNet.co.uk*, 19 July 2001. http://news.zdnet.co.uk/emergingtech/0,1000000183,2091634,00.htm.

McCormack, Andrew. Telephone Interview, 30 July 2009.

McGarry, John. '"Functions of a Public Nature" under the Human Rights Act 1998: The Decision of the House of Lords in YL v Birmingham City Council'. *Web Journal of Current Legal Issues* 5 (2007). http://webjcli.ncl.ac.uk/2007/issue5/mcgarry5.html.

McIntyre, TJ. 'Blocking Child Pornography on the Internet: European Union Developments'. *International Review of Law, Computers & Technology* 24, no. 3 (2010): 209.

———. ‘Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems’. In *Research Handbook on Governance of the Internet*, edited by Ian Brown. Cheltenham: Edward Elgar, 2013.

McIntyre, TJ, and Colin Scott. ‘Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility’. In *Regulating Technologies*, edited by Roger Brownsword and Karen Yeung. Oxford: Hart Publishing, 2008.

McNamee, Joe. ‘Blocking of Innocent Websites by O2 Ireland’. *EDRi: European Digital Rights*, 14 July 2010. http://www.edri.org/edrigram/number8.14/o2-blocking-websites-ireland.

———. ‘Controversial Draft Framework Decision on Child Sexual Exploitation’. *EDRi: European Digital Rights*, 7 October 2009. http://www.edri.org/edrigram/number7.19/draft-framework-decision-child-exploatation.

———. ‘Privatised Online Enforcement Series: Abandonment of the Rule of Law’. *EDRi: European Digital Rights*, 23 March 2011. http://www.edri.org/edrigram/number9.6/abandonment-rule-of-law.

———. *The Slide from ‘Self-Regulation’ to Corporate Censorship*. European Digital Rights, 2011. http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

Meale, Darren. ‘Avast, Ye File Sharers! The Pirate Bay Is Sunk’. *Journal of Intellectual Property Law & Practice* 7, no. 9 (2012): 646.

———. ‘NewzBin2: The First Section 97A Injunction against an ISP’. *Journal of Intellectual Property Law & Practice* 6, no. 12 (2011): 854.

Merrick, Jane. ‘Internet Providers Face Child Porn Crackdown’. *The Independent*, 6 September 2009. http://www.independent.co.uk/news/uk/crime/internet-providers-face-child-porn-crackdown-1782530.html.

Merrills, John Graham. *The Development of International Law by the European Court of Human Rights*. Manchester University Press, 1988.

Metropolitan Police. ‘Pornographic Material on the Internet’, August 1996. http://www.cyber-rights.org/documents/themet.htm.

Metz, Cade. ‘Brit ISPs Censor Wikipedia over “Child Porn” Album Cover’. *The Register*, 7 December 2008. http://www.theregister.co.uk/2008/12/07/brit_isps_censor_wikipedia/.

———. ‘Brit Porn Filter Censors 13 Years of Net History’. *The Register*, 14 January 2009. http://www.theregister.co.uk/2009/01/14/demon_muzzles_wayback_machine/.

———. ‘Demon Ends Porn-Less Internet Archive Block’. *The Register*, 16 January 2009. http://www.theregister.co.uk/2009/01/16/demon_resolves_wayback_issue/.

———. ‘IWF Confirms Wayback Machine Porn Blacklisting’. *The Register*, 14 January 2009. http://www.theregister.co.uk/2009/01/14/iwf_details_archive_blacklisting/.

———. ‘IWF Pulls Wikipedia from Child Porn Blacklist’. *The Register*, 10 December 2008. http://www.theregister.co.uk/2008/12/10/iwf_reverses_wikiban/.

Mifsud Bonnici, Jeanne Pia. *Self-Regulation in Cyberspace*. Information Technology & Law Series 16. The Hague: TMC Asser Press, 2008.

Ministry of Justice. ‘Circular 2010/06: Coroners and Justice Act 2009’, 19 March 2010. http://www.justice.gov.uk/publications/docs/circular-06-2010-coroners-justice-act-provisions.pdf.

———. ‘Suicide and the Internet - Updating the Law’, 17 September 2008. http://www.justice.gov.uk/news/newsrelease170908a.htm.

Montero, Etienne, and Quentin Van Enis. ‘Enabling Freedom of Expression in Light of Filtering Measures Imposed on Internet Intermediaries: Squaring the Circle?’ *Computer Law & Security Review* 27, no. 1 (February 2011): 21.

Moody, Glyn. ‘Massive Overblocking Hits Hundreds Of UK Sites’. *Techdirt.*, 15 August 2013. http://www.techdirt.com/articles/20130815/09563524186/massive-overblocking-hits-hundreds-uk-sites.shtml.

Morgan, Bronwen, and Karen Yeung. *An Introduction to Law and Regulation: Text and Materials*. Cambridge: Cambridge University Press, 2007.

Morrison, Aimée Hope. ‘An Impossible Future: John Perry Barlow’s “Declaration of the Independence of Cyberspace”’. *New Media & Society* 11, no. 1–2 (2009): 53.

Mortimer, John. ‘Return To Oz’. *Index on Censorship* 37, no. 3 (2008): 32.

Moses, Asher. ‘Banned Hyperlinks Could Cost You $11,000 a Day’. *Sydney Morning Herald*, 17 March 2009. http://www.smh.com.au/articles/2009/03/17/1237054787635.html.

———. ‘Leaked Australian Blacklist Reveals Banned Sites’. *The Sydney Morning Herald*, 19 March 2009. http://www.smh.com.au/articles/2009/03/19/1237054961100.html.

Mowbray, Alistair R. *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights*. Human Rights in Perspective 2. Oxford: Hart Publishing, 2004.

Mueller, Milton. ‘Net Neutrality as Global Principle for Internet Governance’. Internet Governance Project, 5 November 2007. http://www.internetgovernance.org/wordpress/wp-content/uploads/NetNeutralityGlobalPrinciple.pdf.

———. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

Mulholland, Helene. ‘Government to Stamp down on Terror “Grooming” Websites’. *The Guardian*, 17 January 2008. http://www.guardian.co.uk/politics/2008/jan/17/uksecurity.terrorism.

Mumford, Richard, and Jaime Arancibia. *Self-Regulation in England and Wales*. NewGov: New Modes of Governance Project. Florence: European University Institute, 2007. http://www.eu-newgov.org/database/DELIV/DLTFIbD09a_Final_Chapters_on_self-regulation_England_and_Wales.pdf.

Murray, Andrew. *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon: GlassHouse, 2007.

———. ‘The Regulatory Edge of the Internet’. *International Journal of Information Technology* 11, no. 1 (2003): 87.

Murray, Andrew, and Colin Scott. ‘Controlling the New Media: Hybrid Responses to New Forms of Power’. *Modern Law Review* 65, no. 4 (2002): 491.

Nair, Abhilash. ‘Real Porn and Pseudo Porn: The Regulatory Road’. *International Review of Law, Computers & Technology* 24, no. 3 (2010): 223.
National Consumer Council. *Models of Self-Regulation: An Overview of Models in Business and the Professions*, 2000. http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf.
Nikki, Matti. ‘Lapsiporno.info and Finnish Censorship’. *Lapisporno.info*, 20 July 2009. http://lapsiporno.info/english-2008-02-15.html.
Nominet. ‘Current Policy Discussions and Consultations’, 2013. http://www.nominet.org.uk/how-participate/policy-development/current-policy-discussions-and-consultations.
‘Nominet Wins iTunes.co.uk Decision’. *OUT-LAW.COM*, 5 August 2005. http://www.out-law.com/page-5979.
Nowlin, Christopher. ‘The Protection of Morals under the European Convention for the Protection of Human Rights and Fundamental Freedoms’. *Human Rights Quarterly* 24, no. 1 (2002): 264–86.
Nunziato, Dawn C. ‘How (not) to Censor: First Amendment Values and Internet Censorship Worldwide’. *Georgetown Journal of International Law* 42 (2011): 1123.
O’Brien, Mark. ‘The Witchfinder-General and the Will-O’-the-Wisp: The Myth and Reality of Internet Control’. *Information & Communications Technology Law* 15, no. 3 (2006): 259.
O’Cinneide, Colm. ‘Taking Horizontal Effect Seriously: Private Law, Constitutional Rights and the European Convention on Human Rights’. *Hibernian Law Journal* 4, no. 1 (2003): 77.
O’Donnell, Ian, and Claire Milner. *Child Pornography: Crime, Computers and Society*. Cullompton: Willan, 2007.
O’Floinn, Michael. ‘Dealing with Domain Names Used in Connection with Criminal Activity: Background Report for Nominet’, 2011. http://webmedia.company.ja.net/edlabblogs/regulatory-developments/2011/03/26/nominet-domain-suspension-paper/.
O’Neill, Sean. ‘Government Ban on Internet Firms That Do Not Block Child Sex Sites’. *The Times*, 10 March 2010. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece.
‘O2 Now Blocking Sites’. *O2 Forum*, 17 September 2009. http://forums.o2online.ie/forums/showthread.php?6034-O2-now-blocking-sites&p=74137&viewfull=1#post74137.
Ofcom. ‘Criteria for Promoting Effective Co- and Self-Regulation’, 2004. http://stakeholders.ofcom.org.uk/binaries/consultations/co-reg/statement/co_self_reg.pdf.
———. ‘Identifying Appropriate Regulatory Solutions: Principles for Analysing Self- and Co-Regulation’, 10 December 2008. http://stakeholders.ofcom.org.uk/consultations/coregulation/.

———. ‘Ofcom’s Approach to Net Neutrality’, 24 November 2011. http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf.
———. *‘Site Blocking’ to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act*. London, 2011.
Office of the e-Envoy. ‘E-Policy Principles: A Policymakers Guide to the Internet’, December 2001. http://tna.europarchive.org/20050311005439/http://www.cabinetoffice.gov.uk/regulation/ria-guidance/documents/pdf/epolicy.pdf.
Office of the Independent Adjudicator for Higher Education. ‘Annual Report 2004’, 2005. http://www.oiahe.org.uk/media/1180/oia-annual-report-2004.pdf.
Ogus, Anthony. ‘Rethinking Self-Regulation’. *Oxford Journal of Legal Studies* 15, no. 1 (1995): 97–108.
Ohm, Paul. ‘The Rise and Fall of Invasive ISP Surveillance’. *University of Illinois Law Review*, 2009.
Oliver, Dawn. ‘England and Wales: The Human Rights Act and the Private Sphere’. In *Human Rights and the Private Sphere: A Comparative Study*, edited by Dawn Oliver and Jörg Fedtke. Abingdon: Routledge-Cavendish, 2007.
———. ‘What, If Any, Public-Private Divides Exist in English Law?’ In *The Public-Private Law Divide: Potential for Transformation?*, edited by Matthias Ruffert. London: British Institute of International and Comparative Law, 2009.
‘Online Child Abuse Images Warning’. *BBC News*, 23 February 2009. http://news.bbc.co.uk/1/hi/technology/7904607.stm.
OpenNet Initiative. ‘Internet Filtering in Saudi Arabia in 2004’. *Berkman Center for Internet and Society*, 2004. https://opennet.net/studies/saudi.
Ost, Suzanne. *Child Pornography and Sexual Grooming: Legal and Societal Responses*. Cambridge University Press, 2009.
———. ‘Children at Risk: Legal and Societal Perceptions of the Potential Threat That the Possession of Child Pornography Poses to Society’. *Journal of Law and Society* 29, no. 3 (2002): 436.
Ozimek, Jane. ‘UK Judges Quietly Declare Text Chat Can Be Obscene’. *The Register*, 3 August 2012. http://www.theregister.co.uk/2012/08/03/text_talk_legal_status/.
Ozimek, John. ‘A Censorship Model’. *The Guardian*, 2 August 2009. http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/02/internet-censor.
———. ‘Girls Aloud Net Obscenity Case Falls at First Hurdle’. *The Register*, 29 June 2009. http://www.theregister.co.uk/2009/06/29/obscenity_trial_off/.
———. ‘IWF Chief: We Don’t Need Crusaders’. *The Register*, 8 September 2009. http://www.theregister.co.uk/2009/09/08/iwf_perter_robbins_interview/.
———. ‘IWF Takes “Pragmatic” Stance on Level One Images’. *The Register*, 10 September 2009. http://www.theregister.co.uk/2009/09/10/iwf_policy_clarification/.
———. ‘Net Suicide Bill Would Breathe Life into Government Censorship’. *The Register*, 24 September 2008. http://www.theregister.co.uk/2008/09/24/suicide_bill_censorship/.

———. ‘Scorpions Tale Leaves IWF Exposed’. *The Register*, 9 December 2008. http://www.theregister.co.uk/2008/12/09/iwf/.

Page, Alan C. ‘Self-Regulation: The Constitutional Dimension’. *Modern Law Review* 49 (1986): 141.

Paine, Thomas. ‘Liberty of the Press’. In *The Writings of Thomas Paine*, Vol. IV. New York: GP Putnam’s Sons, 1894.

Palmer, Elizabeth. ‘Should Public Health Be a Private Concern? Developing a Public Service Paradigm in English Law’. *Oxford Journal of Legal Studies* 22, no. 4 (2002): 663.

Palmer, Stephanie. ‘Public, Private and the Human Rights Act 1998: An Ideological Divide’. *Cambridge Law Journal* 66 (2007): 559.

Papadopoulos, Linda. *Sexualisation of Young People Review*. Home Office, 2010.

Parliamentary Assembly of the Council of Europe. ‘Resolution 1877 on the Protection of Freedom of Expression and Information on the Internet and Online Media’, 2012. http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=18323.

Parti, Katalin, and Luisa Marin. ‘Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers’ Removal of Illegal Internet Content’. *Journal of Contemporary European Research* 9, no. 1 (7 January 2013): 138.

Patterson, Lyman Ray. *Copyright in Historical Perspective*. Vanderbilt University Press, 1968.

Perry, Roland. Telephone Interview, 1 March 2009.

Petley, Julian. ‘Web Control’. *Index on Censorship* 38, no. 1 (2009): 78.

Phillipson, Gavin. ‘Max Mosley Goes to Strasbourg: Article 8, Claimant Notification and Interim Injunctions’. *Journal of Media Law* 1, no. 1 (2009): 73.

Phillipson, Gavin, and Alexander Williams. ‘Horizontal Effect and the Constitutional Constraint’. *Modern Law Review* 74, no. 6 (2011): 878.

Pontifical Council for Social Communications. ‘Ethics in Internet’, 22 February 2002. http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_en.html.

Pool, Ithiel de Sola. *Technologies of Freedom*. Cambridge, Mass: Belknap Press of Harvard University Press, 1983.

Price, Monroe Edwin, and Stefaan Verhulst. *Self-Regulation and the Internet*. The Hague: Kluwer Law International, 2005.

Prime Minister’s Task Force on Tackling Radicalisation and Extremism. *Tackling Extremism in the UK*. London: Cabinet Office, 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/263181/ETF_FINAL.pdf.

Prins, Corien. ‘Should ICT Regulation Be Undertaken at an International Level?’ In *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, edited by Bert-Jaap Koops, Miriam Lips, Corien Prins, and Maurice Schellekens. Information Technology and Law 9. The Hague: T.M.C. Asser Press, 2006.

Prosser, Tony. ‘Constitutional Guarantees in the Light of Privatisation: The UK Experience’. presented at the VII World Congress of the International Association of Constitutional Law, Athens, 11 June 2007.

http://www.enelsyn.gr/papers/w10/Paper%20by%20Prof.%20Tony%20Prosser.pdf.

———. ‘Self-Regulation, Co-Regulation and the Audio-Visual Media Services Directive’. *Journal of Consumer Policy* 31 (2008): 99.

Public Service. ‘Using the Internet to Reduce the Threat of Terrorism’. *Public Service*, 9 November 2009. http://www.publicservice.co.uk/feature_story.asp?id=12949.

‘Radio Times Casualty of Piracy Fight’. *BBC*, 14 August 2013. http://www.bbc.co.uk/news/technology-23699681.

Reidenberg, Joel R. ‘Lex Informatica: The Formulation of Information Policy Rules Through Technology’. *Texas Law Review* 76, no. 3 (1998): 553.

———. ‘States and Internet Enforcement’. *University of Ottawa Law & Technology Journal* 1 (2004): 213.

———. ‘Yahoo and Democracy on the Internet’. *Jurimetrics* 42 (2002): 261.

Reynolds, Nigel. ‘Sir Elton John’s Young Girl Art: No Charges’. *The Telegraph*, 26 October 2007. http://www.telegraph.co.uk/news/uknews/1567383/Sir-Elton-Johns-young-girl-art-No-charges.html.

Richardson, Tim. ‘BT on Child Porn Stats’. *The Register*, 22 July 2004. http://www.theregister.co.uk/2004/07/22/bt_ispa_cleanfeed/.

———. ‘ISPA Seeks Analysis of BT’s “Cleanfeed” Stats’. *The Register*, 21 July 2004. http://www.theregister.co.uk/2004/07/21/ispa_bt_cleanfeed/.

Robbins, Peter, and Roger Darlington. ‘The Role of Industry and the Internet Watch Foundation’. In *Policing Paedophiles on the Internet*, edited by Allyson MacVean and Peter Spindler. Bristol: New Police Bookshop, 2003.

Robertson, Geoffrey, and Andrew Nicol. *Media Law*. 4th ed. London: Penguin, 2002.

Romero Moreno, Felipe. ‘Unblocking the Digital Economy Act 2010; Human Rights Issues in the UK’. *International Review of Law, Computers & Technology* 27, no. 1–2 (2013): 18.

Ruggie, John. ‘Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework’. United Nations Human Rights Council, 2011. http://www.business-humanrights.org/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf.

Russell, Diana E.H., and Natalie J. Purcell. ‘Exposure to Pornography as a Cause of Child Sexual Victimization’. In *Handbook of Children, Culture, and Violence*, edited by Nancy E. Dowd, Dorothy G. Singer, and Robin Fretwell Wilson, 59. London: Sage, 2005.

Schellekens, Maurice. ‘What Holds off-Line, Also Holds on-Line?’ In *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, edited by Bert-Jaap Koops, Miriam Lips, Corien Prins, and Maurice Schellekens. The Hague: TMC Asser, 2006.

Scott, Colin. ‘Regulation in the Age of Governance: The Rise of the Post-Regulatory State’. In *The Politics of Regulation: Examining Regulatory Institutions and Instruments in the Age of Governance*, edited by Jacint Jordana and David Levi-Faur. Cheltenham: Edward Elgar, 2004.

Select Committee on Culture, Media and Sport. *Harmful Content on the Internet and in Video Games*. London: HMSO, 2008. http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/35302.htm.

Senden, Linda. 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?' *Electronic Journal of Comparative Law* 9, no. 1 (2004).

Sentencing Guidelines Council. 'Sexual Offences Act 2003: Definitive Guidance', April 2007.

Simpson, Brian. 'Controlling Fantasy in Cyberspace: Cartoons, Imagination and Child Pornography'. *Information & Communications Technology Law* 18, no. 3 (2009): 255.

Sinclair, Darren. 'Self-Regulation versus Command and Control? Beyond False Dichotomies'. *Law & Policy* 19, no. 4 (1997): 529.

Sluijs, Jasper P. 'From Competition to Freedom of Expression: Introducing Article 10 ECHR in the European Network Neutrality Debate'. *Human Rights Law Review* 12, no. 3 (2012): 509.

Smith, David J. 'Changing Situations and Changing People'. In *Ethical and Social Perspectives on Situational Crime Prevention*, edited by Andrew von Hirsch, David Garland, and Alison Wakefield. Studies in Penal Theory and Penal Ethics. Oxford: Hart Publishing, 2000.

Smith, Rachael Craufurd. 'Reflections on the Icelandic Modern Media Initiative: A Template for Modern Media Law Reform?' *Journal of Media Law* 2, no. 2 (1 December 2010): 199.

Sommer, Peter. 'Evidence: A Case for the Defence'. In *Policing Paedophiles on the Internet*, edited by Allyson MacVean and Peter Spindler. Bristol: New Police Bookshop, 2003.

———. 'Re: Cleanfeed and Wikipedia', 8 December 2008. http://markmail.org/message/kobuqgxlorakesnx.

———. 'Re: Cleanfeed and Wikipedia', 9 December 2008. http://markmail.org/message/pd5vhqrofd7brqxm.

———. Telephone interview, 2 November 2009.

Stalla-Bourdillon, Sophie. 'Chilling ISPs... When Private Regulators Act without Adequate Public Framework'. *Computer Law & Security Review* 26 (2010): 290.

———. 'Liability Exemptions Wanted! Internet Intermediaries' Liability under UK Law'. *Journal of International Commercial Law and Technology* 7, no. 4 (2012): 289.

Stol, Wouter, Rik Kaspersen, Joyce Kerstens, Rutger Leukfeldt, and Arno Lodder. 'Filtering Child Pornography on the Intenet: An Investigation of National and International Techniques and Regulations'. CyREN – Cybersafety Research and Education Network, 26 May 2008. http://www.wodc.nl/onderzoeksdatabase/internetfilters-tegen-kinderporno.aspx?cp=44&cs=6780.

———. 'Governmental Filtering of Websites: The Dutch Case'. *Computer Law & Security Review* 25 (2009): 251.

Stothard, Michael. ‘Mosley Takes Google Privacy Battle to French Court’. *Financial Times*, 4 September 2013. http://www.ft.com/intl/cms/s/0/23705a3c-1581-11e3-950a-00144feabdc0.html?siteedition=intl.

Sunde, Inger Marie. ‘Enforcing Legal Protection against Online Violation of Privacy’. In *Nordic Yearbook of Law and Informatics 2010–2012: Internationalisation of Law in the Digital Information Society*, edited by Dan Jerker B Svantesson and Stanley Greenstein. Copenhagen: Ex Tuto Publishing, 2013. http://brage.bibsys.no/politihs/bitstream/URN:NBN:no-bibsys_brage_40052/1/enforcing_legal_protection.pdf.

Sutherland, John. *Offensive Literature: Decensorship in Britain, 1960-1982*. Rowman & Littlefield, 1983.

Sutter, Gavin. ‘Don’t Shoot the Messenger? The UK and Online Intermediary Liability’. *International Review of Law, Computers & Technology* 17 (2003): 73.

———. ‘“Nothing New under the Sun”: Old Fears and New Media’. *International Journal of Law and Information Technology* 8, no. 3 (2000): 338.

Svantesson, Dan Jerker B. ‘How Does the Accuracy of Geo-Location Technologies Affect the Law’. *Masaryk University Journal of Law & Technology* 2 (2008): 11.

Swire, Peter P. ‘Of Elephants, Mice, and Privacy: International Choice of Law and the Internet’. *The International Lawyer* 32 (1998): 991.

Tambini, Damian, Danilo Leonardi, and Christopher Marsden. *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence*. London: Routledge, 2008.

Taylor, Max, and Ethel Quayle. *Child Pornography: An Internet Crime*. Hove: Brunner-Routledge, 2003.

———. ‘Criminogenic Qualities of the Internet in the Collection and Distribution of Abuse Images of Children’. *Irish Journal of Psychology* 29, no. 1–2 (2008): 119.

———. ‘The Internet and Abuse Images of Children: Search, Precriminal Situations and Opportunity’. In *Situational Prevention of Child Sexual Abuse*, edited by Richard Wortley and Stephen Smallbone, Vol. 19. Crime Prevention Studies. Monsey, N.Y.: Criminal Justice Press, 2006.

Thomas, Donald. *Freedom’s Frontier: Censorship in Modern Britain*. London: John Murray, 2007.

Tien, Lee. ‘Architectural Regulation and the Evolution of Social Norms’. *Yale Journal of Law and Technology* 7 (2005): 1.

Truman, Nick. Telephone interview, 8 February 2010.

———. ‘The Experience of BT in Online Child Protection’. presented at the Effective Strategies for the Prevention on Child Online Trafficking Pornography and Abuse, Bahrain, 9 May 2009. http://www.befreecenter.org/Upload/Conference/papers/BT.ppt.

‘U.S. Government Shuts Down 84,000 Websites, “By Mistake”’. *Torrentfreak*, 16 February 2011. http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/.

‘UK ISP Block of Fileserve Site Blamed on Internet Watch Foundation Filter’. *ISP Review*, 19 November 2011. http://www.ispreview.co.uk/story/2011/11/19/uk-isp-block-of-fileserve-website-blamed-on-internet-watch-foundation-filter.html.

‘UK ISPs Block Huge Movie Site Movie2K, Proxy Immediately Unblocks’. *TorrentFreak*, 20 May 2013. http://torrentfreak.com/uk-isps-block-huge-movie-site-movie2k-proxy-immediately-unblocks-130520/.

United Nations Human Rights Committee. *General Comment No. 34 - Article 19: Freedoms of Opinion and Expression*, 12 September 2011. http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

———. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 2011. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Vaile, David, and Renée Watt. ‘Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra’. *Telecommunications Journal of Australia* 59, no. 2 (2009).

Van Daalen, Ot. ‘Translations of Key Dutch Internet Freedom Provisions’. *Bits of Freedom*, 27 June 2011. https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/.

Van der Kroft, Daphne. ‘Net Neutrality in The Netherlands: State of Play’. *Bits of Freedom*, 15 June 2011. https://www.bof.nl/2011/06/15/net-neutrality-in-the-netherlands-state-of-play/.

Van Hoboken, Joris. ‘Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines’. University of Amsterdam, 2012.

Vick, Douglas. ‘Regulatory Convergence?’ *Legal Studies* 26, no. 1 (2006): 26.

Villeneuve, Nart. ‘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.

———. ‘The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace’. *First Monday* 11, no. 1 (2006). http://firstmonday.org/ojs/index.php/fm/article/view/1307/1227.

Von Hirsch, Andrew, David Garland, and Alison Wakefield, eds. *Ethical and Social Perspectives on Situational Crime Prevention*. Studies in Penal Theory and Penal Ethics. Oxford: Hart Publishing, 2000.

Wagner, R. Polk. ‘Filters and the First Amendment’. *Minnesota Law Review* 83 (1999): 755.

Walden, Ian. *Computer Crimes and Digital Investigations*. Oxford: Oxford University Press, 2007.

———. ‘The Future of Freedom of Speech’. presented at the SCL 6th Annual Policy Forum: ‘The New Shape of European Internet Regulation’, London, 15 September 2011. http://www.scl.org/files/scl_policy_forum_2011/The_Future_of_Freedom_of_Speech_-_Professor_Ian_Waldren.mp3.

Watt, Nicholas, and Juliette Garside. ‘Google to Tackle Images of Child Sexual Abuse with Search and Youtube Changes’. *The Guardian*, 18 November 2013. http://www.theguardian.com/technology/2013/nov/18/uk-us-dark-web-online-child-abuse-internet.

Watt, Nicholas, Josh Halliday, and Juliette Garside. 'Web Firms Pledge £1m to Help Block Child Abuse Images'. *The Guardian*, 18 June 2013. http://www.theguardian.com/technology/2013/jun/18/internet-service-providers-child-abuse-images.

'Wayback Machine'. *Internet Archive*. Accessed 19 October 2013. http://archive.org/web/.

'Wikipedia Child Image Censored'. *BBC News*, 8 December 2008. http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.

William, Nigel. 'Review of the Internet Watch Foundation: Submission from Childnet International to the Review Team', October 1998. http://www.childnet-int.org/downloads/iwf.pdf.

Williams, Chris. 'Hollywood Studios Ask High Court to Block Film Website'. *The Telegraph*, 27 June 2011. http://www.telegraph.co.uk/technology/news/8597596/Hollywood-studios-ask-High-Court-to-block-film-website.html.

———. 'Home Office Backs down on Net Censorship Laws'. *The Register*, 16 October 2009. http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.

———. 'IWF Denies Wielding Pirate Bay Banhammer'. *The Register*, 21 April 2009. http://www.theregister.co.uk/2009/04/21/iwf_pirate_bay/.

———. 'Jacqui's Jihad on Web Extremism Flops'. *The Register*, 13 February 2009. http://www.theregister.co.uk/2009/02/13/jacqui_smith_web_extremism/.

———. 'New Web Filter Laws Questioned by Top Child Abuse Cop'. *The Register*, 9 September 2009. http://www.theregister.co.uk/2009/09/09/ceop_iwf/.

———. 'Nominet Appoints Itself Web Policeman'. *The Register*, 21 January 2010. http://www.theregister.co.uk/2010/01/21/nominet_lock/.

———. 'Small ISPs Reject Call to Filter out Child Abuse Sites'. *The Register*, 25 February 2009. http://www.theregister.co.uk/2009/02/25/iwf_small_isps/.

———. 'Terrorism Chiefs Don't Know What They've Censored Online'. *The Register*, 12 November 2009. http://www.theregister.co.uk/2009/11/12/west_terror/.

Winner, Langdon. 'Cyberlibertarian Myths and the Prospects for Community'. *ACM SIGCAS Computers and Society* 27, no. 3 (1997): 14–19.

Wortley, Richard. 'Situational Prevention of Child Sexual Abuse in the New Technologies'. Chapel Hill, North Carolina, 2009.

Wortley, Richard, and Stephen Smallbone. *Child Pornography on the Internet*. Washington, DC: US Department of Justice, 2006. http://www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

Yeung, Karen. 'Government by Publicity Management: Sunlight or Spin?' *Public Law*, 2005, 360.

Zeldin, Wendy. 'Global Legal Monitor: Netherlands: Amended Telecommunications Act Prescribes Net Neutrality, Stricter Cookie Provisions'. *Library of Congress Global Legal Monitor*, 15 May 2012. http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403143_text.

Zittrain, Jonathan. 'A History of Online Gatekeeping'. *Harvard Journal of Law and Technology* 19, no. 2 (2006): 253.

———. 'Internet Points of Control'. *Boston College Law Review* 44 (2003): 653.

Zittrain, Jonathan, and John Palfrey. 'Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet'. In *Access Denied: The Practice and Policy of Global Internet Filtering*, edited by Ronald J Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 103. Cambridge, Mass: MIT Press, 2008.