MEDIA@LSE
Department of Media and Communications

MEDIA@LSE Working Paper Series

Editors: Bart Cammaerts, Nick Anstead and Ruth Garland

The Policy Challenge of Content Restrictions:
How Private Actors Engage the Duties of States

Monica Horten

Other dissertations of the series are available online here:
http://www.lse.ac.uk/collections/media@lse/mediaWorkingPapers/

Monica Horten (M.Horten@lse.ac.uk) holds a PhD from the University of Westminster and is a Visiting Fellow at LSE. She is an independent expert with the Council of Europe Committee on Cross-border flow of Internet and Internet Freedoms. She is the author of three books on Internet policy: A Copyright Masquerade: How Corporate Lobbying Threatens Online Freedoms (Zed 2013); and The Copyright Enforcement Enigma: Internet Politics and the Telecoms Package (Palgrave Macmillan 2012), and a new one forthcoming from Polity Press 2016. This paper owes it origins to some of her earlier, unpublished work. She first began research into deep packet inspection in 2008, when she self-published a work-in-progress paper entitled 'Deep packet inspection, copyright and the Telecoms Package: How Europe's Internet could be restricted on behalf of industrial interests' and (with Benedetta Brevini): 'Net neutrality vs. traffic management policies: A briefing paper on the Telecoms Package Second Reading'. Furthermore, she presented a paper entitled 'Blocking the web, whose right is it anyway: a regulatory perspective' at the European Consortium for Political Research (ECPR) Regulation and Governance conference in Exeter 2012.

Published by Media@LSE, London School of Economics and Political Science ("LSE"), Houghton Street, London WC2A 2AE. The LSE is a School of the University of London. It is a Charity and is incorporated in England as a company limited by guarantee under the Companies Act (Reg number 70527).

The Policy Challenge of Content Restrictions:
How Private Actors Engage the Duties of States

Monica Horten

The development of online technologies, services and applications presents challenges for policy-making with regard to the protection of free speech rights. Those technologies, services and applications are enablers of free speech, but conversely they also contain powerful functionality to restrict it. It is this restrictive functionality that is the subject of this paper. The issue considered here is how to interpret the duty of States with regard to private actors, acting on behalf of States, in the context of Internet restrictions (network-level blocking and filtering) and the right to freedom of expression. In a human rights context, does it matter whether the private actor is applying content restrictions in response to a government request or doing so of its own accord?

To answer this question, the way in which restrictions placed on the Internet engage free speech rights from a legal and policy perspective is addressed. In particular, the ways in which the underlying network technology may restrict access to content and interfere with free speech rights is of relevance,. Besides this, the duties of States in this context will be considered as well. Answers to these issues will be provided in the context of liberal democracies such as the Member States of the European Union, where demands for such restrictions on access to content are creating challenges for policy-makers. Copyright enforcement will furthermore be used as an example of a policy perspective where industry stakeholder demands for restrictions to be imposed by network providers as third party private actors, have created a particular challenge for human rights compliance.

In this paper an inductive analysis of case law, regulatory and technical studies is presented in order to make connections between the underlying network technology and interference with free speech rights. Drawing on expert legal opinion, including United Nations guidelines for business and human rights, it considers how the duties of States duties might be interpreted in the Internet context. The findings indicate that States do have special to address private actors in this context and will add to the body of knowledge regarding Internet policy and content online.

INTRODUCTION

States are bound under international conventions to guarantee human rights, including the right to freedom of expression, and they also have the sovereign right to determine what content is acceptable within their own jurisdiction. However, when it comes to electronic communications networks, private actors are increasingly being asked to act on behalf of States in implementing content restrictions. These private actors are not bound by these international conventions, but they do fall under the jurisdiction of the State (Rundle and Birding, 2008: 74-77 and 84). Their position therefore could become pivotal with regard to freedom of expression online. In this paper the question of how to interpret the duty of States with regard to private actors, in the context of content restrictions and the right to freedom of expression is addressed. This question will be considered with regard to liberal democracies such as the Member States of the European Union, where demands for restrictions on access to content are creating some difficult policy challenges.

Specifically, the question being addressed is whether it matters if a private actor is applying content restrictions in response to a government request or if it is doing so of its own accord? (cf. Rundle and Birding, 2008: 77). Human rights law is intended to protect against interference with free speech. Under the European Convention on Human Rights (ECHR), the right to freedom of expression states 'without interference from a public authority'. Governments who are signatories to international human rights conventions, notably those who have signed the ECHR, have a duty to guarantee the right to freedom of expression and to protect against such interference. From a human rights perspective, the Internet is the communications medium of choice for the exercise of democratic citizenship and free speech[1]. It is also a communications system which facilitates every aspect of life. People in all walks of life rely on the Internet as a tool for essential everyday activities – banking, shopping, education, work, social life, paying taxes. It encompasses both public and private speech, ranging from the most trivial interjection to the highest forms of intellectual thought. The underlying network technologies that run the Internet are therefore essential enablers of free speech.

[1] For a legal perspective see the following sources: Council Of Europe 2009 p 2; Conseil Constitutionel 2009; EDPS 2014; European Court of Human Rights, Second Section, Case of Yildirim vs. Turkey (Application No. 3111/10) Judgment Strasbourg 18 December 2012 Final 18/03/2013, S.54

However, those underlying technologies present policy challenges in the form of ongoing developments that take the Internet from a neutral platform to one that has a sophisticated built-in intelligence. Notably, those technologies contain powerful functionality, such as blocking and filtering, to restrict users' activity[2]. It is this restrictive functionality that is the subject of this paper.

The restrictive possibilities within the technology are being translated into policy actions such as blocking injunctions and takedown notices, content filtering implementations, and graduated response or disconnection measures. These measures tend to be taken in response to certain specific concerns which include, but are not exclusive to, copyright enforcement, the need for counter-terrorism measures, or demands for parental controls. In the paper the ways in which this restrictive functionality could engage free speech rights is addressed. This does not mean that any speech goes. Nor does it mean that governments cannot impose restrictions. It does mean that governments wanting to impose restrictions must first of all test them for compliance with human rights law. The issue for policy-making is to understand the ways in which such engagement is created, and whether a law or policy addressed to private actors, is likely to meet the human rights compliance requirements.

An inductive analysis of case law, regulatory and technical studies is used to consider the ways in which the underlying network technology creates interference with free speech rights. It investigates the duties of states with regard to private actors and, drawing on expert opinion, including United Nations guidelines for business and human rights, it considers how those duties might be interpreted in the Internet context. In the paper copyright enforcement is used as a specific example of the policy demands and responses.

TECHNOLOGY AND POLICY CHALLENGES

The capacity of broadband providers to act on the traffic that transits their networks has dramatically increased to an extent that could not have been foreseen when the Internet was born in the early 1990s. (Mueller, et al., 2012: 349) They are able to automatically monitor user activity[3] and deter or prevent transmissions, and have at their disposal a range of functions to render websites inaccessible. These functions include the ability to put in place

[2] FCC Chairman, Tom Wheeler, speaking at the FCC Meeting on 26 February 2015 (watched by the author via webcast).

[3] See: Peha and Mateus (2014) for a discussion of monitoring and detection of peer-to-peer file-sharing of copyrighted material.

an automated block (Ofcom, 2011) as well as to intercept the users' traffic when they try to view specific content, or alter the access speed to make it difficult for users to get certain types of content. This vast and sophisticated blocking capability has placed the broadband providers at the centre of the political debate about Internet content, and what should and should not be permitted. They have become a target for many third parties who have desires to prevent or stop content, and are seeking the means to do so.

Applying Lessig's (2006: 121-32) ideas of 'code is law', what is happening is that norms and markets are being disrupted to such an extent that the affected stakeholder interests are clamouring to policy-makers for legal changes to amend the 'code' of the network. For example, norms of acceptable behaviour are changing as a result of a series of technology developments. The camera in the mobile phone, and the platforms such as Instagram, have generated a new norm where people take photographs and publish them not just to friends and family but also to the world. Those images could be embarrassing or invasive of privacy. Social media platforms provide a new mechanism that transfers a quiet grudge spoken to a friend into a published comment that is potentially defamatory (House of Lords, House of Commons, 2011, S.92-107)[4] The potential for abuse in terms of breach of privacy and defamation, led to a judicial procedure for content take-down being built in to the 2013 Defamation Act.[5]

The potential of any of these new norms to be used for the purposes of terrorist activities, has led to calls from national security agencies for blocking and filtering of content. For example:

> [...] we need a new deal between democratic governments and the technology companies in the area of protecting our citizens. It should be a deal rooted in the democratic values we share. That means addressing some uncomfortable truths (Hannigan 2014: np)

Moreover, market disruption has occurred in relation to copyright, where distribution of creative works online and the alleged piracy has led to political demands for a variety of blocking options[6]. Hence governments have been receiving demands from groups of stakeholders seeking Internet restrictions to address policy goals such as parental controls

---

[4] See also McNair-Wilson, Laura (2011) Defamation & Twitter: First Love, on Inform Media Law Blog, 29 January: https://inforrm.wordpress.com/2011/01/29/defamation-and-twitter-first-love-laura-mcnair-wilson/ [Accessed 19 May 2015]

[5] Defamation Act 2013, Clause 13 Order to remove statement or cease distribution etc.

[6] See Horten (2013) for a discussion of the entertainment industry lobbying.

over children's access to content, stalking, harassment, as well as copyright enforcement. All of these demands present a policy challenge. States are seeking the co-operation of broadband providers to take action which may conflict with their duty to protect free speech rights.

Central to policy measures proposed in this context is the obligation being placed onto the broadband providers to take action. Broadband providers are the gateways to the Internet, and they fall within the jurisdiction of nation States and so they can be governed by law, contrary to the popular perception of the Internet as an ungoverned space.[7] In terms of Lessig's 'code is law', the law that can change the 'code' governing the disruptive behaviours is that which governs the broadband provider's networks. Hence, there is pressure on the providers to change the code in order to control the behaviours. Restrictions on access to or the distribution of content by blocking and filtering frequently features in these demands.

Broadband providers could either be asked to block access to the network or to block specific content which resides on the network. The blocks can be carried out such that an either entire website or individual webpage is unavailable to all users. There are different techniques to implement blocking, with varying levels of effectiveness and side-effects. One technique is using the IP address, which is the string of numbers that identifies any device connected to the Internet. The IP address system enables data to be sent around the network by any route, and arrive safely at the correct destination, because all IP addresses are unique. The data is divided into little packets that carry the IP address on them. It's similar to putting an address on an envelope to go in the post. The block works by the network provider modifying its routers to send the packets to a non-existent route. IP address blocking brings the risk that legitimate content residing in the same location may also be blocked (over-blocking), as happened when a block on a football streaming site also blocked the Radio Times (Cookson 2013).

Another blocking technique is to target the content by means of the universal resource locator (URL) – effectively, this is the address of the website or page, or of an individual item such as an image. This method operates by checking the individual URLs against a database of blocked items, and either dropping it, so that user gets an error page, or sending a warning page back to the user. URL blocking is more targeted than IP address blocking, but the risk is that erroneous classification or an over-broad implementation, for example, using the URL of

[7] For a discussion of network providers s and how they may be controlled by governments, see Goldsmith and Wu (2006: 68-84).

a whole website or platform, results in over-blocking. This happened in the case of Yildirim vs. Turkey, where the Turkish government sought to block a website that had allegedly insulted the memory of Atatürk, the father of the Turkish state. The offending content was only on one particular website, but the entire platform of Google Sites – http://sites.google.com – was blocked[8]. As a consequence, the applicant's website was blocked along with the offending content.

A third technique is to block the domain name system (DNS) so it is no longer be possible for a website to be found[9]. The DNS is the system that keeps a record of where the content for a web domains or website is physically located on the infrastructure. This is why a domain may be registered in one country, but the content will be on servers in another. DNS is essential for the Internet to operate. DNS blocking is done by 're-writing' the answers given by the system in response to a request by the user to view a website. The re-write tells the system to send a message that the site does not exist. Alternatively, it may tell the system to go to an alternative webpage that may contain a warning, or government message. Some experts use the analogy that it's like the system is telling a lie (Emert, 2011) and they express concern about the way that DNS blocking manipulates a system that is a core element of the functioning of the Internet – without DNS, there would be no Internet.

DNS blocking should not be confused with domain seizure. This is where the domain is taken offline at the request of the authorities and the website disappears because there is no means of finding it. This was the case with the domain seizures by the US Immigration and Customs Enforcement (ICE) in 2010 (Emert, 2011; Ofcom, 2011: 23-4; ICE, 2010). Both DNS blocking and domain seizures carry a risk of over-blocking because a domain may have several sub-domains and it may well be that some of those sub-domains are operating legitimate services (Ofcom 2011, p34). For example, in 2008 a British businessman operating legitimate holiday travel services to Cuba found that his domains had been taken down by order of the United States Treasury, rendering his websites unavailable and having the effect of shutting down his business (Liptak, 2008).

To implement any kind of blocking system, a list or database of sites and pages needs to be compiled and maintained. The database will be classified into categories that define the

[8] European Court of Human Rights, Second Section, Case Of Yildirim V. Turkey (Application No. 3111/10) Judgment Strasbourg 18 December 2012 Final 18/03/2013, S.12-14

[9] This account is drawn from Ofcom, 2011: 28-37; and Case No: HC14C01382 in the High Court of Justice, Cartier International v British Sky Broadcasting, 17 October 2014, Judgement, S.25.

blocking criteria. In some countries, such as Russia, the list is compiled centrally by the State (Weaver and Clover, 2012; Tselikov, 2014: 10). There are four registries that are maintained by the Russian telecoms regulatory authority, Roskomnadzor. The data for the lists is supplied by other government agencies. The broadband providers are obligated to check the lists and implement the blocks within 24 hours. In Britain, the broadband providers obtain a single limited list of URLs to block from a third party, the Internet Watch Foundation for the purpose of addressing child pornography. However, there is a separate system for parental controls which operates quite different. In this case, each of the network providers operate their own bespoke blocking system, including determination of blocking criteria and database compilation. In the parental controls filtering, there is no shared list, and each of the network providers has to identify for themselves the content to be blocked, and compile their own list. The blocking criteria vary from one provider to another: BT has 17 categories and Virgin has eight. They do not share data between them, and in fact, the blocklist compilation is outsourced to third party security specialists.[10]

The actual sites to be blocked are typically found using keyword analysis. This analysis may be as simple as looking at the URL. If it contains a banned keyword, then it will be blocked, irrespective of whether its actual content is or is not legitimate. It may be that the banned keyword is picked up in the webpage or site content. However, with the notable exception of the Chinese state, few have the resources to conduct a detailed analysis of web content. Hence, there is a risk of false categorisation resulting in over-broad blocking (Zittrain and Palfrey, 2008: 38-43).

The possibility for abuse of powers to block legitimate content also exists. Erroneous classification can easily happen when inserting sites into the blocklist, as when a serious article in *The Guardian* about a school for lesbian and gay students was caught up in a keyword filter for a parental controls system.[11] In these circumstances, especially where there are multiple blocklists created by competing private actors, it is impossible for users to know what is being blocked and on what basis it is being done. In Britain, the providers do not share data about sites that have been erroneously blocked, and the blocking action is not foreseeable by website owner or user, nor is it notified to them.

[10] Case No: HC14C01382 in the High Court of Justice, Cartier International v British Sky Broadcasting, 17 October 2014, Judgement, S. 62, S.45; S.48 -49.

[11] This was a tweet from a Guardian reader, on 16 January 2015 of which the author holds a copy. It is cited because it illustrates how over-blocking can happen. There is not yet any case law on this point.

A network-level blocking system requires Internet service providers to systematically examine all of a user's communications traffic (Stalla-Bourdillon, 2013: Section 4) in order to identify the pages in the blocklist and cease the transmission. This is done using a content filtering system combined with another technology known as Deep Packet Inspection (DPI) (Bendrath and Mueller, 2011: 1145-6; Ofcom 2011: 29&39). A filtering system will identify the content requested by users, and will check each request against the database. The filtering can be implemented on the network routers, where all requests for pages on the blocklist will be intercepted, and dropped or diverted. Alternatively, it can be done at the level of the individual subscriber, in which case, the filtering system will hold a database of the websites and services which that individual is permitted to see, and will screen against it. Every page that the user tries to access will be checked before access is permitted.

Deep packet inspection is the technology that examines the data packets for particular characteristics. DPI is often explained using a metaphor of the post office – it's a bit like the post office examining the mail and opening the envelopes, and then deciding whether to permit it to continue on the basis of what it finds. This is a bit simplistic, but it broadly reflects the principle on which DPI operates. It looks at the header information – analogous to the address and other information on the envelope – and it can look deeper into the content (Stalla-Bourdillon, et al., 2014)[12].

If a DPI system it finds, for example, traffic destined for a website that is meant to be blocked, it can simply drop – and effectively block - that traffic[13]. According to an Ofcom report on site-blocking, this kind of blocking is technically 'trivial', but it carries the caveat that there must be careful consideration of the blocking criteria, and any failure on that part risks false positives or the erroneous over-blocking of legitimate traffic. (Ofcom, 2011: 39) Ofcom further warns that the use of deep packet inspection may raise privacy concerns (Ofcom, 2011: 50). The systems implemented by the British broadband providers to implement filtering for parental controls, use such a combination of deep packet inspection with either URL, IP address or DNS blocking[14].

[12] This paper provides a detailed explanation of DPI. See also TTA 2012 – this is the technical specification for DPI drafted under the auspices of the International Telecommunications Union.

[13] See also TTA 2012

[14] Case No: HC14C01382 in the High Court of Justice, Cartier International v British Sky Broadcasting, 17 October 2014, Judgement, S.38-51

INTERFERENCE AND HUMAN RIGHTS LAW

Given this analysis of the technology, it would suggest that content filtering and network-level blocking go hand in hand with surveillance practices (Zittrain and Palfrey, 2008: 50), such as monitoring and interception. The overall outcome can result in negative consequences for legitimate content (Stalla-Bourdillon, 2013: Section 4) such as over-blocking. It is these two factors that raise the human rights issues. Filtering and blocking practices, that render web content invisible or inaccessible, or cause it to disappear entirely, targeting users' ability to access or distribute content, combined with the risk of over-blocking, immediately creates an engagement with the right to freedom of expression. Over-blocking can happen due to technical error; it can also happen when the block is not sufficiently specific or the content has been erroneously classified. The surveillance practices raise obvious concerns regarding the right to privacy as a corollary right. In this context, it becomes evident that there is an inconsistency between the capabilities of the network providers and what the law permits (Mueller, et al., 2012: 349).

Human rights law in relation to freedom of expression is predicated on the notion of non-interference by the State. Article 10[15] of the European Convention on Human Rights (ECHR) states that freedom of expression must be guaranteed 'without interference by public authority'. Article 10 is a two-way right to access and to distribute information is an important one when considering freedom of expression on the Internet because individuals have the ability to upload content and in that context they can publish or distribute it, as well as passively access content to gain knowledge. A necessary corollary to the right to freedom of expression is ECHR Article 8, the right to privacy[16] because it protects not only the right to a private life, but a right to private correspondence, without interference from the State.

---

[15] ECHR Article 10:

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 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

.

[16] ECHR Article 8:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the

Legal scholars underscore that international norms with regard to freedom of expression are fully applicable to the Internet (Barron, 2010: 312). The European Court of Human Rights (ECtHR) has underlined the importance of the Internet in enhancing people's access to news, and in generally facilitating the dissemination of knowledge, based on its capacity to store and communicate vast amounts of information and its ease of access. The ECtHR confirmed that the right to freedom of expression applies not just to the content itself, but also to the means of transmission of data over the network and to the means of its reception.[17]

That would seem to confirm its applicability to the use of broadband networks, and to the broadband access connection. It's interesting that the ECtHR said that Article 10 rights also apply to putting in place the means for others to receive and impart information[18]. In this specific instance, it was referring to a file-sharing network, but it arguably could be a catch-all for Internet platforms, such as YouTube, that facilitate free speech (Schroeder, 2013: 67) in their role as intermediaries. Hence, the users right of Internet access can be important in the context of freedom of expression, as well as the network and the technology platform.

The EctHR furthermore stated that Article 10 rights apply to everyone, and there is '*no distinction for profit-making*'[19]. This was a reminder that the right to freedom of expression applies to someone 'speaking' in the context of running a business, as well as to individuals pasting their personal thoughts onto Facebook or Twitter. In particular, it applies to news media and journalists.

Finally, Article 10 applies 'regardless of frontiers'. [20] Restrictive measures can create cross-border effects such as over-blocking and upstream filtering. In 2008, the Pakistan authorities ordered a block on YouTube that resulted in the video streaming site being inaccessible worldwide – a global case of over-blocking. It was found to be due to routing errors in implementing the block, and it illustrates how blocking might have much wider effects than

---

economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[17] European Court of Human Rights, Neij & Sunde Kolmisoppi against Sweden in the European court of Human Rights , Application no. 40397/12, 2013, p9. This was an appeal made by two of operators of The Pirate Bay to the European Court of Human Rights in 2013. In this instance, the court also upheld the decision of the Swedish court, however, it is interesting that it confirmed the engagement of the right to freedom of expression.

[18] Ibid Neij & Sunde Kolmisoppi against Sweden, p.9

[19] Ibid Neij & Sunde Kolmisoppi against Sweden, p.9

[20] European Court of Human Rights, Second Section, Case Of Yildirim V. Turkey (Application No. 3111/10) Judgment Strasbourg 18 December 2012 Final 18/03/2013, S.67

intended.[21] Upstream filtering is where a network provider is filtering content according to rules in one jurisdiction and providing services for citizens in another. Those citizens in the second jurisdiction may find themselves unable to view content that is legitimate in their country but not in the one whose filtering rules are being applied. In other words, 'upstream filtering' by private actors could which could entail a violation of the rights of the 'downstream' citizens. States may have a duty to of due diligence in this regard, which, under international law, implies that they should do all that they reasonably can to avoid or minimise harm across national borders[22].

The central issue for policy-makers is the notion of 'interference', and notably to establish what constitutes 'interference' in the Internet space. The ECHR was drafted at a period in time just after World War II, when it was assumed that the interferer would be the State. The nature of the interference was assumed to physical, such as visits from the secret police or the burning of books in the streets, as happened in Germany in 1933. It was not foreseen that interference would come from commercial entities, nor that it could happen automatically on such a vast scale as to take out thousands of works at a time. The situation we face today is that the network providers are private actors who work in conjunction with States and other private interests to apply automated restrictions. The question concerns the duty of the State have to introduce some form of accountability for the actions of those private actors.

Given our analysis of the technology, it would seem that the use by network providers of blocking and filtering systems to restrict Internet content does constitute interference for the purpose of ECHR Article 10 (Rundle and Birding, 2008: 73). The interference is created through monitoring of content access as well as by interception and diversion, over-blocking, abuse of trust and false categorisation. Disconnection of Internet access or slowing of traffic speech can also represent a form of interference.

This view is borne out by legal opinion. For example, the former British public prosecutor, Lord Macdonald, stated that 'the power to have content removed from the Internet represents, on its face, a serious interference with the rights of others.' (Macdonald, 2013a, 5.2.8) Lord Macdonald added that even if the network provider believed the content were

[21] Open Net Initiative, YouTube Censored: a recent history https://opennet.net/youtube-censored-a-recent-history [Accessed 19 May 2015]

[22] Council of Europe Proposals for international and multi-stakeholder co-operation on cross-border Internet: Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services, pp.17-18 – pt.72.

criminally pornographic, the company would have to be absolutely certain that it had the remit to remove that content.

The ECtHR has said that 'any restriction imposed on access to content *'necessarily interferes with the right to receive and impart information*'[23]. This means that whenever blocking or filtering measures are considered, the right to freedom of expression is engaged and the measures must be evaluated against human rights law.

It begs the question as to whether *without interference* in the Internet era means no blocking at all, or whether there are circumstances when blocking might be justified. In this matter, the ECtHR has provided helpful guidance, it says that access to the network, is a necessary element for individuals to exercise their right to freedom of expression:

> [...] blocking access to the Internet, or parts of the Internet, for whole populations or segments of the public can never be justified, including in the interests of justice, public order or national security.

In the case of Yildirim vs. Turkey, where the applicant was unable to access his own website, which contained legitimate content, and the site was rendered invisible to the wider public, the ECtHR stated that this did constitute interference, and was a breach of Article 10, with a reminder that any blocking should be prescribed by law, pursue a legitimate aim and is necessary in a democratic society.[24]

The ECtHR has said that any restrictive measures must be clearly and tightly defined, including the method of blocking. The scope of any restricting order must be sufficiently clear that it is obvious what kind of content likely to be blocked, whether any particular types of content or publishers are being targeted, the geographical area to which they apply must be defined, and a time-limit should be given. There should be a clear process for implementation and a notification to those whose content is affected, and a possibility of appeal or judicial review.[25] Any 'indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or

---

[23] Ibid Neij & Sunde Kolmisoppi against Sweden, p.9

[24] European Court of Human Rights, Second Section, Case Of Yildirim vs. Turkey (Application No. 3111/10) Judgment Strasbourg 18 December 2012 Final 18/03/2013, S.56.

[25] European Court of Human Rights, Second Section, Case Of Yildirim vs. Turkey (Application No. 3111/10) Judgment Strasbourg 18 December 2012 Final 18/03/2013, p.28; See also United Nations (2011b) report of the UN Special Rapporteur Frank La Rue

platform' would not be legal, and 'blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship.' [26]

Filtering of traffic on the network may also constitute interference. The European Court of Justice (ECJ) said that a filtering system engages the right to freedom of expression because it may not be able to accurately distinguish between lawful and unlawful content. It would also engage the right to privacy since it would have to systematically examine all content and identify the IP addresses of the individual users.

The right to privacy is a necessary corollary to freedom of expression because it guarantees confidentiality of communications, notably that the State will not intercept private correspondence. The large-scale monitoring of individual behaviour and of their communications has been condemned by European data protection experts, who argue that these rights should not be surrendered 'through neglect' (EDPS, 2014).

In that regard, EU law does not permit an injunction ordering a network provider to filter all traffic 'indiscriminately, to all its customers, as a preventative measure, exclusively at its expense, and for an unlimited period'[27]. Effectively, this means that anything involving continuous monitoring, of all content, for unlimited period of time, would comprise a general obligation to monitor, and would be illegal under EU law. This does not preclude filtering measures being ordered, but there are strict legal criteria that should be met. The ECJ has stated that filtering measures must be necessary and proportionate, they should be targeted and the determination of the filtering criteria or the content to be filtered should be ordered by a court or a body independent of political influence, and should be subject to judicial oversight. In addition, the ECJ such measures should not impose excessive costs on the broadband providers (Angelopoulos, 2014: 4-5).

In other words, Article 10 is a qualified right, which means that States may circumscribe it, but only when it is prescribed by law, pursuing a legitimate aim and necessary in a

[26] European Court of Human Rights, Second Section, Case Of Yildirim vs. Turkey (Application No. 3111/10) Judgment Strasbourg 18 December 2012 - Final 18/03/2013, p.29

[27] Case number C-70/10 in the European Court of Justice, Scarlet Extended vs. Société Belge des Auteurs, Compositeurs, et Éditeurs (SABAM), S.55

democratic society:[28] The State must be pursuing a policy aim that clearly justifies the need to implement restrictions, and must provide that justification (House of Lords, House of Commons, 2010, S.1.37). Legal experts point out that the requirement for narrow and targeted measures is especially important where the justification for the restriction concerns public order, national security or public morals (Rundle and Birding, 2008): restrictive measures can be easily abused to protect the interests of the government rather than to protect citizens rights, and they may be co-opted to serve a favoured set of stakeholder interests, and avoid consideration of the human rights balance.

Hence, the policy-makers' role is to balance the different sets of interests when confronted with content blocking demands. They should establish a fair balance between freedom of expression and the competing interests involved[29]. In Britain, they must complete a Human Rights memorandum for any new law, and civil servants are urged to undertake this as an integral element of the policy-making process and not as a last-minute exercise.

COPYRIGHT

The kind of dilemmas that policy-makers face in finding the right balance are illustrated by the case of the so-called Internet Freedom[30] provision. This provision is a reminder in EU telecoms law - the law that addresses broadband service provision - that national measures to restrict the Internet must be subject to a prior, fair an impartial hearing.

The Internet Freedom provision was inserted after a political argument over specific copyright measures, known as graduated response, demanded by the entertainment industries for enforcement purposes. Graduated response was conceived as a system of warnings to an Internet user regarding alleged copyright infringement followed by disconnection or 'cutting off' Internet access (Giblin, 2014). The identification of the users was carried out via surveillance of peer-to-peer file-sharing networks. This process was exemplified in the French law Creation and Internet law[31] although the system created by it

[28] Neij & Sunde Kolmisoppi against Sweden in the European court of Human Rights , Application no. 40397/12, 2013.

[29] Ibid Case number C-70/10 in the European Court of Justice, Scarlet Extended vs. Société Belge des Auteurs, Compositeurs et Éditeurs (SABAM), S.53.

[30] Directive 2009/140/EC Article 1.3a. See Horten (2012)

[31] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la Création sur Internet - known in English as the Creation and Internet Law. (Legifrance, 2009a). It was disbanded under the Presidency of Francois Hollande.

has subsequently been disbanded. In some implementations, notably the US '6 strikes' Copyright Alert System (Bridy, 2013: 31-33), and the UK's Digital Economy Act (Horten, 2013: chapters 9-14), there is also a possibility to slow down or take some other restrictive action with regard to the user's connection, making it impossible for them to download content. A graduated response system therefore relies on the broadband provider to impose the disconnection. Disconnection engages free speech rights. It further engages the right privacy because of the requirement to identify the individual subscriber. Identification was presumed to be feasible via the IP address, although this has proved to be problematic in practice because the IP address relates to the connection which is not necessarily the same as the individual. Nevertheless, the engagement of these rights is underscored by a report of the Joint Parliamentary Committee on Human Rights, which stated that '[i]t is generally accepted that measures taken to limit individual access to internet services by the State will engage Articles 8 and 10 ECHR'[32]. If imposed as a sanction, disconnection would not only affect any unlawful downloading of copyrighted content, but also lawful activities such as work, education and banking (Barron, 2010: 338).

In formulating the Internet Freedom provision, the European Parliament was concerned about two elements. Firstly, the possibility of disconnections being ordered on the basis of a privately operated administrative procedure, thereby bypassing the courts. Moreover, such a private process would have a presumption of guilt built in, contrary to the principle of presumption of innocence, which is built in to European law[33]. On that basis, ECHR Article 6, the right to due process, was invoked and the European Parliament considered that disconnection should be carried out only following a *prior, fair and impartial hearing*[34]. Secondly, the European Parliament could foresee other types of Internet restrictions, such as network-level blocking and filtering. It was on that basis that the language in '*national measures'* was chosen, with the intention of addressing a range of other possibilities[35]. In ensuing reviews of intellectual property rights, the European Commission has been careful to state that all fundamental rights must be respected, including the right to a private life, freedom of expression and an effective remedy (European Commission, 2011c: 19, S3.5.3).

---

[32] House of Lords, House of Commons, 2010, S.1.36 The committee was considering the Technical Measures in the Digital Economy Act, S.10, that include slowing down of the broadband access service with intention to prevent the user from being able to use specific services, as well as disconnection from the network itself.

[33] European Convention on Human Rights (ECHR) Article 6.2

[34] Directive 2009/140/EC, Article 1.3a

[35] See Horten (2012, chapter 12) for a full account of the Internet Freedom provision and its genesis in the European Parliament.

It is now generally considered that in copyright enforcement cases, policy-makers and courts should balance the right to freedom of expression against the right to property. Copyright is a private right and would usually be addressed under civil law (Matthews, 2008: 30). It is generally argued that copyright is a property right under the ECHR Protocol 1, Article 1, which mandates the 'peaceful enjoyment of possessions'[36]. The European Union Charter of Fundamental Rights[37], adds a right to intellectual property, as a subset of the more general right to property, in Article 17.2[38]. According to a British Parliamentary committee, policy-makers must strike this balance with care. Governments may consider the right property in the context of a general public interest, but when it comes to the right to freedom of expression, the requirement to show that the proposed interference is prescribed by law, and necessary in a democratic society to meet a legitimate aim (House of Lords, House of Commons, 2010, S.1.33) is a higher level of legal test. Noting that the right to privacy is a corollary to freedom of expression, European case law says that courts should balance the right to privacy against the right to intellectual property, taking into account the principle of proportionality[39].

General filtering of Internet content on broadband networks for the purpose of copyright enforcement was ruled out by the ECJ in the case of Scarlet Extended[40]. As a consequence, copyright holders have turned to blocking injunctions under Article 8.3 of the EU copyright Directive. [41] This correlates to Article 11 of the IPR Enforcement directive, and to Articles 12-15 of the E-commerce directive, and Section 97a of the UK's Copyright, Designs and Patents Act. The entertainment industry's political lobbyists would like to see a fast-track injunction codified in law, such that a blocking order could be obtained within a short space of time –

---

[36] Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties (ECHR, Protoco1, Article 1).

[37] Charter Of Fundamental Rights Of The European Union, (2000/C 364/01) Article 17.2

[38] 1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest.

2. Intellectual property shall be protected. (Article 17, European Union Charter of Fundamental Rights).

[39] The case of Promusicae v Telefonica in the European Court of Justice, 2008. Case C-275/06, Referring court: Juzgado de lo Mercantil No 5 de Madrid. Applicant: Productores de Música de España (Promusicae). Defendant: Telefónica de España . ECJ ruling of 29 January 2008.

[40] Case number C-70/10 in the European Court of Justice, Scarlet Extended vs. Société Belge des Auteurs, Compositeurs et Éditeurs (SABAM), S.55

[41] Directive 2001/29/EC on Copyright in the Information Society

days or even hours. This was the intention behind the Provisional Measures in the now-defunct Anti-counterfeiting Trade Agreement [42] and also Section 102 of the also-now-defunct Stop Online Piracy Act in the United States.[43] However, injunctions are made in consideration of human rights law. In the UK, injunctions will be implemented by some network providers using the same technology that is in place for content filtering measures as outlined above. They therefore entail a form of interference with the user's communications, and engage Article 8[44] and 10[45] rights. Hence, the UK courts have found that content blocking injunctions may be ordered, but they must be narrow in scope and specific to the aim.[46]

STATES AND PRIVATE ACTORS

By constraining injunctions in this way, States may fulfil their duty to guarantee the rights to freedom of expression, as established by the European Convention on Human Rights. In this context, that duty can be interpreted to mean that States are obligated to guarantee non-interference with Internet content as well as with Internet access. However, when policy-makers are faced with demands for blocking legislation, and they will need to understand how this obligation applies when the restrictions are imposed by law on broadband providers who are private actors.

Guidance is provided by the United Nations, which has drafted some general principles for business and human rights. The essential principle is that States must protect against human rights abuses by third parties in their jurisdiction (United Nations, 2011a: I.A.1-2) and that they should set out an expectation that businesses operating within their jurisdiction would respect human rights. The broadband providers are regulated under telecoms policy and in the European Union, they are legally considered to be 'mere conduits'. That means they carry content, but do not have any interest in it, and member state governments are expressly forbidden from giving them any general obligation to monitor content[47]. The mere conduit provision would seem *de facto* to have the effect of protecting freedom of expression, whether

[42] ACTA, December 2010 version, Article 12

[43] 12th congress, 1st Session, HR 3261, A Bill To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes. Also known as the Stop Online Piracy Act (SOPA).

[44] Case No: A3/2012/1477, In the Court of Appeal, GoldenEye International Ltd vs. Telefonica , S.117;

[45] Case No: HC10C04385 In the High Court of Justice, 20th Century Fox v BT S.119

[46] Case no. H C08C03346, 20th Century Fox vs. Newzbin, Judgement of Kitchin J., 29 March 2010, S.135

[47] E-commerce directive 2000/31/EC, Articles 12 and 15.

or not that was its intended purpose, but if that status is altered, then it will pose issues for policy-makers.

The notion of 'general monitoring' is another important legal distinction. EU law says that telecoms providers may not be given a 'general obligation to monitor'[48]. Blocking and filtering systems will fall foul of any net neutrality law, and notably the proposed law in the EU[49] would mean that measures undertaken by the broadband providers without statutory backing would be illegal.

If making laws to restrict the Internet, policy-makers have to weigh up the rights of the intermediary to conduct business, enshrined under the EU Charter of Fundamental Rights [50] along with freedom of expression and any other rights such as copyright. They have to find the most appropriate balance between the conflicting rights and interests involved. Within this context, there are tensions (Angelopoulos, 2014: 5) between the freedom of expression rights of the individual Internet user, as well as the rights of others (where others could be children in this context, or they could be copyright holders). Hence, when a government is considering restrictive measures, for example to protect copyright, it must balance that policy objective against both of these fundamental rights and it has a duty to justify its reasons for interfering with them (House of Lords, House of Commons, 2010, S.1.19, S.1.33, S.1.36-1.37). What's important is that the legal tests for interfering with freedom of expression – necessity, proportionality and legitimate aim – are of a higher order than the public interest test for protecting copyright.

The United Nations guidelines state that businesses should respect human rights (United Nations, 2011a: II.A.11) and avoid adverse human rights impacts. Blocking and filtering measures may result in a *de facto* requirement for broadband providers to exercise a quasi-legal judgement in multiple cases. As private organisations, they are generally are not set up or competent to act as a content censors[51] and noting the risk of over-blocking outlined above, such decision-making requirement would create uncertainty for the business, potentially exposing them to liabilities under civil law, as well as possible violations of the rights of users.

---

[48] Directive 2000/31/EC of * June 2000 (the E-commerce Directive), Article 15

[49] See European Parliament (2014) Amendment 241 – also known as the Del Castillo report

[50] European Union (2001), Article 16. This analysis draws on Angelopoulos (2014: 5)

[51] Macdonald (2013a: S3.9 and 2013b: 2) provides an interesting insight into the issue of private actors being asked to act as censors.

According to the U.N. guidelines, States should enforce laws aimed at guarantees for human rights, support businesses on how to respect human rights, and encourage business to communicate how they address human rights impacts (United Nations, 2011a: I.B.3 & B.5). This would suggest a requirement for regulatory safeguards. States will be under an obligation to ensure that restrictive measures such as blocking and filtering are not implemented in an arbitrary or over-broad manner (Rundle and Birding, 2008: 85). There should be a rigorous justification process, evaluating the proposed blocking measures against a legitimate aim, ensuring that they are necessary to achieve that aim and proportionate to it. This means they must be the minimum needed to achieve the aim (United Nations, 2011b: S.69; Kuczerawy 2015: 55). Citizens should be clearly informed of the policy justification (United Nations 2011a: I .B.3).

Both citizens and Internet service providers should be in a position to know whether their actions are legal or not. This means that citizens should be informed of the blocking criteria (Rundle and Birding, 2008: 85) and know what to do if they either encounter blocked content, or find that their own content is blocked. States should take appropriate steps to prevent and deal with any abuses (United Nations, 2011a: I.A.1-2) through legislation and other policy instruments. Decisions on the blocking criteria and the specific content to be blocked should be overseen by a judicial process (Macdonald, 2013a: S.5.3.3) or by an administrative body that is independent of any stakeholder interests in the blocking measures. There should be an independent process to handle complaints, challenges or appeals. These processes may be administrative or judicial, as long as they are in compliance with ECHR Article 6. The entire process should be subject to judicial review.

From the perspective of policy-makers, putting the matter in the hands of an administrative body may look like an attractive option but a case in Spain illustrates how an administrative body may not meet the compliance requirements for due process under ECHR Article 6. The issue arose when the Spanish government wanted to pass a law to have websites blocked [52] for copyright enforcement purposes. In Spain, freedom of expression is constitutionally guaranteed. Article 20 of the Spanish Constitution states that 'seizure of publications, recordings, or other means of information may only be adopted by a judicial decision'

[52] The law known as Ley Sinde, or Sinde's law *It's official title is - Ley 2/2011, de 4 de Marzo de Economia Sostenible, Annex 43*., It was appended to the Law on the Sustainable Economy, which was a much larger piece of legislation addressing the economy as a whole. Ley Sinde was derived from the name of the (then) culture minister, Angelez Gonzalez-Sinde. (See Horten, 2013: chapter 8).

(Peguera, 2010: 164, S.90). The government had proposed that a purely administrative body could order the shutting-down of websites (Peguera, 2010: 163-4) but the constitution was invoked and it was determined that the blocking order had to be authorised by the judicial authorities. This view was confirmed in a report by the public prosecutor at the request of the Ministry of Justice (Consejo Fiscal, 2010: 18&25).

There is another temptation for policy-makers to opt for a privately-run process, operated by the broadband providers together with the relevant stakeholder interests. This is sometimes euphemistically referred to as 'voluntary measures' or 'co-operative efforts' (Kaminsky, 2011: 21). However, the Spanish experience[53] shows that voluntary agreements in this context are extremely difficult to broker. The broadband providers are unsurprisingly resistant to any such agreement, and the rights-holders unwilling to compromise. In Spain, negotiations began in 2007, and by 2009, they had reached no conclusion, so the government introduced legislation. A similar attempt by the European Commission to broker a 'voluntary' agreement at European level (European Commission, 2011a) also broke down. After heated arguments between the rights-holders and the telecoms industry groups, the Commission decided that it was no longer viable to continue, concluding that there were '*fundamental differences of opinion remain on most of the topics*' (European Commission, 2011b)[54]. The Commission acknowledged the difficulties in reaching a consensus.

Aside from the difficulties in reaching a deal, these voluntary agreements are problematic in other ways. Arguably, they are an attempt by the State to shift responsibility for a policy action onto the private sector, where the broadband providers would consent to take the demanded actions without the backing of legislation. As they are non-legislative agreements, they rely on industry stakeholder good-will. In this regard, voluntary agreements would seem to run counter to, the United Nations guidelines, which suggests that States should exercise oversight and provide guidance 'when contracting with businesses to provide services that may impact on human rights' (United Nations 2011a: I.B.5).

A voluntary agreement reliant on good-will, is not subject to judicial oversight. Arguably too, they create a policy dynamic where industry is able to set the terms for that good-will, and may rely on inter-personal relationships in order to function. It's arguable that this

[53] Research carried out by the author indicates that discussions were ongoing in Britain from 2007-2008, and in Spain from 2007-2009.

[54] Additional source: author's personal conversations with participants.

dependency mitigates in favour of a 'state-promoted private ordering' with non-disclosure and non-transparent regulation, 'insulated from public scrutiny and that can be tailored, by virtue of that insulation, to serve corporate interests at the public's expense' (Bridy, 2011: 577).

However, if a voluntary agreement is put in place, the UN guidelines call for private actors to avoid causing adverse impacts to freedom of expression, and seek to mitigate them if they occur. They also call for businesses to communicate externally on their policies with regard to freedom of expression and restrictive measures (United Nations, 2011a: II.B.21). This could be interpreted to mean that broadband providers must communicate details of their blocking criteria and blocklists to internet users and content providers and they must take clear steps to avoid over-blocking, and to protect against abuse by employees or contractors. The State would remain under a duty to ensure that those obligations were met, which implies regulatory supervision as minimum level of compliance.

CONCLUSION: BALANCING INTERFERENCE AND STATE DUTIES

It would seem therefore, that both voluntary and statutory measures for restricting the Internet carry a requirement for regulatory oversight. In particular, safeguards are needed against error and misuse. These safeguards would take the form of judicial or regulatory oversight, including compliance with due process under ECHR Article 6, combined with requirements placed on private actors to inform the public such that citizens can reasonably foresee the consequences of their actions. This would enable the measures to fall in line with the guiding principles adopted by the United Nations for business and human rights.

The form that these safeguards would take does not yet have a model, however, individual Internet users would need to know the circumstances under which their content could be blocked. By inference, Internet users would also need to be informed which websites, services and applications were being blocked. If this kind of information was available, they would be able to take informed decisions when uploading their own content – whether for private use or for public distribution. They would also be able to know whether or not downloading of content was legitimate.

These safeguards are critical because Internet restrictions may not only cause interference with the ability to access content, but also with the ability to publish or distribute it. The

interference is created by the network infrastructure technology, which, by means of surveillance, monitoring and interception, makes it possible to bar requests and hide content from view – not actually destroying it, but as good as doing so from the user's or publisher's perspective. The balance of rights turns on the level of *interference*. Content restrictions lack the dramatic impact of piles of burning books, but in terms of their potential to effect censorship on a wide scale, the harm they could generate is much deeper. Leaving them in the hands of private actors without adequate safeguards would seem to entail inherent risks to freedom of expression. It is for that reason that governments, pressed with demands to block or filter Internet content, have special duties with regard to private actors.

REFERENCES

Angelopoulos, C. (2014) Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape, *Journal of Intellectual Property Law & Practice* 9(10): 812-21.

Barron, A. (2010) 'Graduated response' à l'Anglaise: online copyright infringement and the Digital Economy Act 2010, *Journal of media law* 3(2): 305-47.

Bendrath, R. and Mueller, M. (2011) The end of the net as we know it? Deep packet inspection and internet governance, *New Media & Society* 13(7): 1142–60.

Bridy, A. (2011) Acta And The Specter Of Graduated Response, *American University International Law Review* 26(3): 558-77.

Bridy, A. (2013) Six Strikes Measured Against Five Norms, *Fordham Intellectual Property, Media & Entertainment Law Journal* 23(1): 1-67.

Conseil Constitutionel (2009) Decision n° 2009-580 de 10 Juin 2009, Loi favorisant la diffusion et la protection de la création sur internet [Decision no 2009-580 of 10th June 2009, Law promoting the distribution and protection of creation on the Internet]

Consejo Fiscal (2010) Informe Del Consejo Fiscal Anteproyecto De Ley De Economia Sostenible y Anteproyecto De Ley Orgánica Complementaria De La Ley De Economia Sostenible, [Report of the of the Law of the Sustainable Economy][Report Of The Fiscal Council on the Draft Bill On the Sustainable Economy And Complementary Draft Organic Law on the Sustainable Economy] 12 February.

Cookson, R. (2013) Anti-piracy drive sees Premier League mistakenly block websites, *Financial Times,* 15 August.

Council of Europe (2009), MCM(2009)011, 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services A new notion of media? (28 and 29 May 2009, Reykjavik, Iceland), Reykjavik, 29 May.

EDPS (2014) Urgent reform of EU data protection framework is essential for a connected continent, Press release EDPS/2014/02, 16 January.

Emert, M. (2011) Filtering and Blocking Closer To The Core Of The Internet?, *Intellectual Property Watch*, 20 November.

European Commission (2011a) Réponse donnée par M.Barnier au nom de la Commission [Response given by Mr Barnier in the name of the Commission], P-0805/11FR, 7 March 2011

European Commission (2011b) Synthesis Report on the Stakeholders' Dialogue on Illegal Up- and Downloading 2009 - 2010, Ref. Ares(2011)367168, 4 April 2011

European Commission (2011c) Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, A Single Market for Intellectual Property Rights Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe com (2011)287 FINAL, 24 May 2011

European Commission (2011d) Commission Communication To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 942,

European Parliament. (2014) Legislative resolution of 3 April 2014 on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent. (Ordinary legislative procedure: first reading).

Ferran, B. (2012) Le Bilan Contraste de l'action de l'Hadopi [The contrasting outcomes of Hadopi's actions], *Le Figaro*, 28 March.

Giblin, R. (2014) Beyond Graduated Response, *Columbia Journal Of Law & The Arts* 37(2): 148-210.

Goldsmith, J. and Wu, T. (2006) *Who Controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press.

Hannigan, R. (2014), The web is a terrorist's command-and-control network of choice, *The Financial Times,* 3 November.

Horten, M. (2012) *The Copyright Enforcement Enigma - Internet Politics and the Telecoms Package*. Basingstoke: Palgrave Macmillan.

Horten, M. (2013) *A Copyright Masquerade: How Corporate Lobbying Threatens Online Freedoms*. London: Zed Books.

House of Lords, House of Commons. (2010) Joint Committee on Human Rights, Legislative Scrutiny: Digital Economy Bill, Fifth Report of session 2009-2010, 5 February.

House of Lords, House of Commons. (2011) Joint Committee on the Draft Defamation Bill - First Report Draft Defamation Bill, 12 October.

ICE (2010) ICE seizes 82 website domains involved in selling counterfeit goods as part of Cyber Monday crackdown, US Department of Immigration & Customs Enforcement, press release, 29 November.

Kaminsky, M. (2011) An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement (ACTA), *PIJIP Research Paper no. 19. American University Washington College of Law*, Washington, DC.

Kuczerawy, A. (2015) Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative, *Computer law & Security Review* 31(1): 46-56.

Legifrance. (2009a), Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet [Law no. 2009-69 of !" June 2009 promoting the distribution and protection of creation on the Internet], 12 June.

Lessig, L. (2006) *Code Version 2.0*. Cambridge, MA: Basic Books.

Liptak, A. (2008) A wave of the watchlist and speech disappears, *The New York Times*, 4 March.

Macdonald, K. (2013a) A Human Rights Audit of the Internet Watch Foundation, November.

Macdonald, K. (2013b) Review of .UK Registration Policy, December.

MacKinnon, R., Hickok, E., Bar, A. and Lim, H. (2014) *Fostering Freedom Online, The Role of Internet Intermediaries*, Paris: Unesco Publishing, see: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

Matthews, D. (2008) The Fight Against Counterfeiting And Piracy In The Bilateral Trade Agreements Of The EU, Brussels: European Parliament.

Mueller, M., Kuehn, A. and Stephanie S. (2012) Policing the Network: Using DPI for Copyright Enforcement, *Surveillance & Society* 9(4): 348-64.

Ofcom (2011) Site Blocking to reduce online copyright infringement A review of sections 17 and 18 of the Digital Economy Act, 27 May.

Peguera, M. (2010) Internet Service Providers Liability in Spain: Recent Case Law and Future Perspectives, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 1(3): 145-50.

Peha, J. and Mateus, A. (2014) Policy implications of technology for detecting P2P and copyright violations, *Telecommunications Policy* 38(1): 66-85.

Rundle, M. and Birding, M. (2008) Filtering and the International System, pp. 73-102 in R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain (eds) *Access Denied: the Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Schroeder, J. (2013) Choosing an Internet Shaped by Freedom: A Legal Rationale to Rein in Copyright Gatekeeping, *Berkeley Journal of Entertainment and Sports Law* 2(1): 48-85.

Stalla-Bourdillon, S. (2013) Online monitoring, filtering, blocking ….What is the difference? Where to draw the line?, *Computer Law & Security Review* 29(6): 702-12.

Stalla-Bourdillon, S., Papadakia, E., and Chown, T. (2014) From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy … The case of deep packet inspection technologies, *Computer Law & Security Review* 30(6): 670-86.

Tselikov, A. (2014) The Tightening web of Russian Internet Regulation, Berkmann Centre for Internet and Society, Research Publication No. 2014-15, 20 November.

TTA (2012) NGN: Requirements for Deep Packet Inspection in Next Generation Networks, Telecommunications Technology Association Standard 2012-1357.Y.2770.

United Nations (2011a) Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, J. Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations Protect, Respect and Remedy Framework, A/HRC/17/31, United Nations General Assembly: 21 March.

United Nations (2011b) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, United Nations General Assembly: 16 May.

Weaver, C. and Clover, C. (2012) Russia's 'Internet blacklst' sparks fears, *The Financial Times*, 11 July.

Zittrain, J. and Palfrey, J. (2008) Internet Filtering: the politics and mechanisms of control, pp. 29-56 in R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain (eds) *Access Denied: the Practice and Policy of Global Internet Filtering,* Cambridge, MA: MIT Press.

Media@LSE Working Paper Series

Media@LSE Working Paper Series will:

- Present high quality research and writing (including research in-progress) to a wide audience of academics, policy-makers and commercial/media organisations.
- Set the agenda in the broad field of media and communication studies.
- Stimulate and inform debate and policy. All papers will be published electronically as PDF files, subject to review and approval by the Editors and will be given an ISSN.

An advantage of the series is a quick turnaround between submission and publication. Authors retain copyright, and publication here does not preclude the subsequent development of the paper for publication elsewhere.

The Editor of the series is Bart Cammaerts. The Deputy Editors are Nick Anstead and Ruth Garland. The editorial board is made up of other LSE academics and friends of Media@LSE with a wide range of interests in information and communication technologies, the media and communications from a variety of disciplinary perspectives (including economics, geography, law, politics, sociology, politics and information systems, cultural, gender and development studies).

Notes for contributors:

Contributors are encouraged to submit papers that address the social, political, economic and cultural context of the media and communication, including their forms, institutions, audiences and experiences, and their global, national, regional and local development. Papers addressing any of the themes mentioned below are welcome, but other themes related to media and communication are also acceptable:

- Communication and Difference
- Globalisation and Comparative Studies
- Innovation, Governance and Policy
- Democracy, Politics and Journalism Ethics
- Mediation and Resistance
- Media and Identity
- Media and New Media Literacies
- The Cultural Economy

Contributions are welcomed from academics and PhD students. In the Michaelmas Term each year we will invited selected Master's students from the preceding year to submit their dissertations which will be hosted in a separate part of this site as 'dissertations' rather than as Working Papers. Contributors should bear in mind when they are preparing their paper that it will be read online.

Papers should conform to the following format:

- 6,000-10,000 words (excluding bibliography, including footnotes)
- 150-200 word abstract
- Headings and sub-headings are encouraged
- The Harvard system of referencing should be used
- Papers should be prepared as a Word file
- Graphs, pictures and tables should be included as appropriate in the same file as the paper
- The paper should be sent by email to Bart Cammaerts (b.cammaerts@lse.ac.uk), the editor of the Media@LSE Working Paper-Series

ISSN: 1474-1938/1946