Regulating to Limit Access to Child Pornography on the Internet: a multiple-case study

Fabio Andre Silva Reis

A thesis submitted in partial fulfilment of the requirements of Sheffield University for the Degree of Doctor of Philosophy

University of Sheffield

School of Law

June 2013

Dedicated to the memory of Samantha Xavier Reis

(1975 - 2006)

Wife

ACKNOWLEDGEMENTS

This thesis would not have been possible without the enduring help, support and encouragement of family, friends and colleagues too numerous to name. A large debt is owed to people from the School of Law at the University of Sheffield.

I must also thank my family: my father Joao Reis, my mother Gicelia Reis, my mother-in-law Ana Elisabete Xavier and my father-in-law Reginaldo Coutinho and, particularly, my much loved son Joao Eduardo Xavier Reis who never failed to give me strength and inspiration during the most difficult of times, including periods of reduced confidence, low morale and short temper that come with completing a doctoral thesis.

I am also indebted to my friends Dr Aurora Zen, Dr Claudio Wanderley, and Fabricio Sanchez who made Brazil not seem so far away from Sheffield.

My gratitude also goes to the Government of the State of Bahia (Brazil) which partially funded this investigation and made it possible to happen. I must thank the non-governmental organisation CEDECA-Bahia for the opportunity to increase my awareness about the protection of children in the online environment.

Most importantly, I wish to thank my supervisors Professor Lilian Edwards and Dr Natasha Semmens for their invaluable advice, insight and support during the first stage of this research. Also, I must thank my supervisors Dr Maggie Wykes and Dr Lindsay Stirton, who were taken onboard during the final stage of this investigation; without their commitment, invaluable advice, support and patience this thesis would never have been possible. My gratitude goes to Dr Gwen Robinson for her support and advice during times of reduced confidence.

My thanks also go to the experts from Australia, Brazil and the United Kingdom who helped me improving each of the case studies.

Of course, any errors or omissions are on my own.

DECLARATION

Parts of this thesis were presented as work in progress on two occasions. A version of Chapter 2 and some information from Chapter 4 were presented at the: (1) GiKII annual conference, IT University of Goteborg (Sweden), in June 2011; and (2) annual conference of the British Society of Criminology, Northumbria University-Newcastle upon Tyne (England), in July 2011.

REGULATING TO LIMIT ACCESS TO CHILD PORNOGRAPHY ON THE INTERNET: A MULTIPLE-CASE STUDY

SUMMARY

This investigation addresses the regulation of access to child pornography available on the Internet to evaluate the implications of hybrid regulation for free speech, privacy and democracy in the online environment.

It aims to investigate these implications in relation to current regulatory measures designed to limit access to child pornography available on the Internet. As such, it establishes evaluative criteria divided into three broad categories: (1) free speech - involving the issues of unchecked private censorship and scope creep; (2) privacy protection - involving the issues of increased unchecked and more invasive surveillance powers given to law enforcement authorities; and (3) general principles of good regulation and democratic values - involving issues around the lack of transparency, accountability, legitimacy, proper oversight, and citizen involvement as well as inefficiency and ineffectiveness of regulatory intervention.

Australia, Brazil and the United Kingdom were chosen as case studies because they had generally similar anti-child-pornography laws, both domestically and in terms of their commitments under international treaties, they were considered democratic countries subject to democratic controls of content, and access to data was relatively unproblematic in these jurisdictions. This provided a common ground for comparison. More importantly, they were chosen as case studies because despite so different constitutional frameworks and varied regulatory scope and mechanics, they all settled on similar approaches to child pornography. regulation. This provided an opportunity to explore different aspects and variations of hybrid regulation, and also to address its broader implications for free speech, privacy and democracy on the Internet.

There are a number of contributions made here. First, this research proposes evaluative criteria for anti-online child pornography regulations. Second, it suggests a scheme of safeguards to minimise negative regulatory consequences in relation to free speech, privacy and democracy in the online environment. It discusses the broad lessons and the economics of online child pornography regulation, the use of decentred and polycentric theories of regulation, and explores the adjudication of apparent illegality of online material by private actors, showing what regulatory and governance theorists as well as criminologist may learn from this research.

LIST OF ABBREVIATIONS

3G	Third generation mobile telecommunications
ABA	Australian Broadcasting Authority
ABRANET	Associação Brasileira de Internet (a Brazilian Internet industry association)
ACMA	Australian Communications and Media Authority
ACPO	Association of Chief Police Officers
AFP	Australian Federal Police
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
BRTF	Better Regulation Task Force
BT	British Telecom
CEDECA-BA	Centro de Defesa da Criança e do Adolescente da Bahia (a Brazilian children's rights non-governmental organisation)
CEOP	Child Exploitation and Online Protection Centre
CERN	European Organisation for Nuclear Research
CGI.br	Comitê Gestor da Internet no Brasil (a multi-stakeholder commission created by the federal government to coordinate all Internet services in Brazil)
CIRCAMP	COSPOL Internet Related Child Abuse Material Project
CoC	Code of Conduct
CoE	Council of Europe
CoP	Code of Practice
COSPOL	Comprehensive, Operational, Strategic Planning for the Police (European Police Chief Taskforce)
CPI	Comissão Parlamentar de Inquérito (a Brazilian Parliamentary Investigation Committee)
CPS	Crown Prosecution Service
CSEC	Commercial Sexual Exploitation of Children
DBCDE	Department of Broadband, Communications and the Digital Economy of the Australian Commonwealth Government
DPF	Departamento de Polícia Federal (the Brazilian Federal Police)
DPI	Deep Packet Inspection

ECHR	European Convention on Human Rights
EU	European Union
FOI	Freedom of Information
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
ICMEC	International Center for Missing and Exploited Children
ICP	Internet content provider
IETF	Internet Engineering Task Force
IHP	Internet host provider
IIA	Internet Industry Association
INHOPE	International Association of Internet Hotlines
INTERPOL	An international police organisation
INWG	International Network Working Group
IP	Internet Protocol
ISOC	Internet Society
ISP	Internet service provider
ISPA	Internet Service Providers Association
IWF	Internet Watch Foundation
MAPAP	Measure and Analysis of P2P Activity Against Paedophile
MPF-SP	Ministério Público Federal do Estado de São Paulo (Federal Public Prosecution Service in the State of São Paulo, Brazil)
NCP	Network Control Protocol
NGO	Non-governmental Organisation
NSA	National Security Agency
NTD	Notice and take down
P2P	Peer-to-peer
RC	Refused content
SNS	Social Network System
TCP	Transmission Control Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
ToS	Terms of Service
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Education, Scientific and Cultural Organisation
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator
US	United States of America
VCR	Video cassette recorder
WSIS	World Summit on the Information Society
WWW	World Wide Web
W3C	World Wide Web Consortium

CONTENTS

CHAPTER 1: INTRODUCTION

During its early days, the Internet was considered a free environment and regarded as a separate jurisdiction invulnerable to state regulation. Such initial enthusiasm about the self-regulatory and anarchic nature of the Internet can be explained by the historical and political contexts of that time. The Internet was not yet part of the everyday life of many people, many online content-related conflicts was outside the political agenda, and many governments were ill-prepared to enforce the law in cyberspace.

Nevertheless, the Internet is now part of the everyday life of modern industrialised countries, it has substantially changed the way people live and interact, and this has a number of implications not only for the media but economy, politics, national security and the law. As a result, regulators across the world, including state and private actors, have employed a number of regulatory strategies and tools, in an ongoing struggle for regulatory control, combining a variety of social resources and capacities as well as enrolling a range of online intermediaries to control different aspects of the Internet, whether in the pursuit of public policy goals or private interests.

There are a number of different regulatory targets in relation to the Internet environment, including the domain names, Internet infrastructure, technical protocols, and wider political issues of digital divide and market competition. Different regulatory actors are involved, both domestically and internationally, depending on the target being pursued (for example,. the Internet Corporation for Assigned Names and Numbers - ICANN, government statutory regulators, the Internet Engineering Task Force - IETF, the World Summit on the Information Society - WSIS, and Internet industry associations). More importantly, each of these domains have particular features and demands a regulatory analysis of its own.

One important focus of regulatory intervention concerns the control of content available on the Internet. Content often carries with it criminal or civil liability; it may infringe copyrights, be defamatory, incite racial hatred, or violate the privacy of individuals. It can be terrorism-related, involve classified information related to national security, or contain images of children. Given that these can be digitised, distributed and accessed on the Internet, regulators have attempted to control this material online, but this has proved problematic for a number of reasons.

First, digitisation of content has facilitated the transmission of information via the digital networks and the storage of a substantial volume of material. Digitised text, image, audio and video can be easily and rapidly transferred from one location to another across the world without degeneration of original information.

Second, the architecture and technical protocols of the Internet allow information to be transferred via an international network without a central point of control. This resilience of the network limits the ability of governments to control online content and facilitates the anonymity

of alleged offenders. There are a number of different points of control; more actors are now involved in the production and distribution of content such as the Internet service providers - ISP, Internet content providers - ICP, and Internet host providers - IHP.

Third, the Internet poses a multi-jurisdictional challenge to the enforcement of content-related laws. The Internet is an international network that connects people across different jurisdictions and it is subject to different regulatory schemes and legislation. It crosses national borders where national governments have no sovereign authority. In addition, many countries without updated laws may be safe havens for cybercriminality. Finding the origin of material and identifying the offender associated with the criminal content can be difficult to establish. Also, the question about which jurisdiction should prosecute is controversial. In short, these issues render the choice of jurisdiction and the enforcement of jurisdictional powers problematic when applied to online content.

Because of these challenges, many regulatory strategies have been employed. Regulation of copyrights infringement on the Internet has moved forward from the safe harbour principle (*i.e.* no liability of online intermediaries unless notified which lead to notice of take down schemes and no explicit obligation to monitor content) towards a new policy of 'constructive knowledge' via graduated responses (*e.g.* notice and disconnection), filtering, blocking, traffic monitoring and throttling undertaken by private actors.[1] For example, in a recent legislative attempt to minimise copyright infringements, enforce intellectual property rights on the Internet, and place policing responsibilities on ISPs, the British Parliament enacted the 2010 Digital Economy Act,[2] a piece of legislation that threatens domestic civil infringers with an escalation of technical measures that include monitoring and notifications by ISPs, slowing down Internet connection, Internet disconnection and blocking of websites by the ISPs.[3] There has been opposition from British ISPs (*e.g.* BT and TalkTalk) to implement this piece of legislation, but their legal challenge to the 2010 DEA was struck down by the courts in March 2012.[4]

Governments have also employed domestic legislation to control access to online adult pornography to protect children. For example, two pieces of legislation originally designed to block access to legal adult pornography by children, the US 1996 Communications Decency Act

---

[1] See Edwards, L., 'Role and Responsibility of Internet Intermediaires in the Field of Copyright and Related Rights', (Geneve: WIPO, 2011) at <http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf>, accessed 28 December 2011.

[2] Digital Economy Act (c. 24) 2010 (England and Wales).

[3] Edwards, L., 'Law and sausages: How Not to Legislate for the Digital Economy', at <http://blogscript.blogspot.com/>, accessed 03 May 2010. Nevertheless, according to the Ofcom initial obligation code, a further act of the UK Parliament is required to implement measures such as throttling or disconnection. See OFCOM, 'Online Infringement of Copyrights and the Digital Economy Act 2010: Draft Initial Obligations Code', (London: Ofcom, 2010) at <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf> Accessed 24 November 2012.

[4] Halliday, J., 'BT and TalkTalk lose challenge against Digital Economy Act', *The Guardian,* 06 March 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/mar/06/internet-provider-lose-challenge-digital-economy-act>, accessed 22 March 2012.

(CDA 1996)[5] and the US 1998 Child Online Protection Act (COPA 1998)[6] were enacted in the United States of America. Nevertheless, they did not pass the constitutional test of freedom of speech.[7] The US courts found both Acts to be over-broad in the sense that they placed excessive burden on the rights of adults to access constitutionally legal adult pornography, because of the blunt and costly technical measures available at that time for age verification and content classification.

In addition, *LICRA et UEJF v Yahoo! Inc. and Yahoo France* showed how a nation state attempted to assert its national laws in the online environment via the courts.[8] The French law prohibits the trafficking of Nazi memorabilia in France, but this material was easily available to all French Internet users via an auction website of Yahoo! hosted in the US, where the availability of Nazi goods was perfectly legal under the wide constitutional protection of free speech.[9] The US company argued that it was technically impossible to restrict access to their servers only to French customers. Nevertheless, on 20 November 2000, after consulting a panel of Internet experts who confirmed the feasibility and effectiveness of online content filtering based on geographical location, Judge Jean-Jacques Gomez issued a final decision ordering Yahoo! to employ its best efforts to block access to Nazi memorabilia in France and warned the US firm that it would have until February 2001 to comply before facing a substantial fine. Following this, on 02 January 2001, Yahoo! decided to remove the controversial content from its US auction website, apparently to avoid bad publicity and damage to its financial assets in France, despite bringing the issue before the US courts later on free speech protection grounds.[10]

Other regulatory strategies have been employed for privacy protection of personal data available on the Internet. The protection of privacy online has been enforced via a mix of self-regulation, community persuasion (online activism), terms of service, governmental oversight (*e.g.* pre-authorised contracts by a regulatory agency, domestic and international law) and privacy enhanced technologies (*e.g.* allowing data migration between different platforms and data expiration).[11]

Another regulatory target concerns state classified information. The whistleblower organisation Wikileaks has proved its resilience to host and provide access to classified information, particularly the War logs and the US diplomatic cables amidst widespread governmental threats

---

[5] Communication Decency Act 1996 § 502, 110 Stat. (United States of America).

[6] Child Online Protection Act 1998 (United States of America).

[7] Although the former was struck down by the US Supreme Court, the latter still struggles through the courts. See generally Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 644-47; Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 249-50.

[8] *LICRA et UEJF v Yahoo! Inc. and Yahoo France*, Tribunal de Grande Instance de Paris, Superior Court of Paris.

[9] See generally Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 626; Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006), p 1-10.

[10] CDT, 'Yahoo France case', at <http://www.cdt.org/grandchild/yahoo-france-case>, accessed 04 June 2010.

[11] See Chapter 2.

around the world.[12] Wikileaks employed sophisticated computational techniques and hosted their servers in nations with more protective speech laws to preserve the anonymity of informants and evade governmental control. As a result, it has been subject to intense pressure from governments.

These examples show the wide range of existing online content regulatory policies and the problematic interaction between private and state regulatory actors tackling controversial online content.

This investigation considered the models of online regulation according to the relevant regulatory actors involved.[13] This decision was taken to organise the numerous regulatory practices employed and thus facilitate the analysis. These models were (1) self-regulation; (2) state and multi-state regulation; and (3) hybrid-regulation. Generally (1) self-regulation was the regulation performed by private actors amongst themselves, particularly the Internet industry, via Codes of Conduct - CoC; (2) state and multi-state regulation was generally the traditional command-and-control regulation[14] that imposed standards by the threat of criminal sanctions and involved monitoring, enforcement and sanctioning by a single state or a group of states; and (3) hybrid regulation was a mix of the approaches in (1) and (2) in addition to the use of architecture-based regulatory tools and invasive surveillance powers by law enforcement authorities.

This investigation focuses on the hybrid regulatory strategies tackling child pornographic material available on the Internet. This is because the problem of child pornography involves a convincing regulatory rationale based on the protection of children that is pushing further the boundaries of online content regulation in ways that other problematic online content are not; online child pornography is therefore a critical case study to analyse the developments of content-related regulatory strategies on the Internet, and more generally the potential threat these measures pose for free speech and privacy protection as well as for democracy generally, for example in terms of transparency, legitimacy and accountability of regulatory policies.

Notably, there is an ongoing call to replace the term child pornography. It has been argued elsewhere that ‘child abuse images’ or ‘abusive material’ are both more inclusive and able to reflect the real nature of the problem in comparison to the term ‘child pornography’.[15] Although

---

[12] See Star, A. (ed.), *Open Secrets: Wikileaks, War, and American Diplomacy (The New York Times)* (Grove Press, 2011); and also Leigh, D. and Harding, L., *WikiLeaks: Inside Julian Assange's War on Secrecy* (London: Guardian Books, 2011).

[13] Other taxonomies exist. For example, Hood and Margetts categorises regulatory intervention by policy instruments. See Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007).

[14] Of course, states do employ a number of other regulatory strategies; state regulation will be discussed further in Chapter 2.

[15] See *e.g.* Quayle, E., Loof, L., and Palmer, T., 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the III World Congress against Sexual Exploitation of Children and Adolescents', (Bangkok: ECPAT International, 2008) at <http://www.childcentre.info/public/Thematic_Paper_ICTPsy_ENG.pdf>, accessed 09 June 2010, p 17; See also IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 21 March 2010.

these are legitimate concerns, this investigation employs the term 'child pornography' because of its wide currency in legal documents, international policymaking and academic literature.[16] Use of the term 'child pornography' does not deny the cruelty and violence involved in the production of such material, and it is arguably closely related to the popular understanding of the problem. Furthermore, the criminal laws and regulations in place in the jurisdictions studied here rarely employ such a definition (*i.e.* 'child abuse images') and thus a term such as 'child pornography' may be a more useful for comparison.

The development of modern anti-child pornography laws can be traced back to the late 1970s following the exposure of child sexual abuse as a social problem.[17] As a result, domestic anti-child pornography laws were created in a number of developed countries. This reaction was arguably effective in limiting the availability of child pornographic content within national borders until the mid-1990s. Nevertheless, the developments associated with the Internet and digital communication technologies have facilitated the proliferation of child pornography and this led to enforcement of domestic anti-child pornography laws becoming largely ineffective. These developments were mentioned above and include the digitisation of content, anonymised access, and the decentralised and multi-jurisdictional architecture of the Internet which rendered the choice of jurisdiction and the acts of policing state agencies heavily problematic.

The resulting ineffectiveness of law enforcement led to a number of regulatory developments. First, domestic anti-child pornography laws escalated in some jurisdictions: new types of conduct and new classes of content associated with child pornography were criminalised in addition to the establishment of harsher penalties. Responses also came at the international level to tackle the multi-jurisdictional nature of the Internet and the disparities in domestic laws *e.g.* the 2000 United Nations (UN) Optional Protocol[18] and the 2001 Council of Europe (CoE) Cybercrime Convention.[19] Nonetheless, the enforcement of these international instruments fell short in terms of disparities in domestic laws, technological know-how and slow ratification of international treaties.[20] Second, Internet industry self-regulation was also employed via Internet industry CoCs and voluntary filtering schemes employed by online intermediaries. These strategies were however largely ineffective at stopping people producing, distributing or accessing online child pornography. Third, hybrid regulation was taken onboard via closer partnership between state and private regulatory actors, increased liability placed on online

---

[16] The same reason is given by O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 68; Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 11; Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009), p 32; and Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 629.

[17] See Chapter 2.

[18] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

[19] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[20] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 207 and 223.

intermediaries, more investigatory and surveillance powers given to law enforcement authorities, and the use of architecture-based regulatory technologies.

The academic literature discussed in Chapter 2 suggests that there are a number of rationales driving the hybrid regulatory expansion in relation to child pornographic material available online: (1) amplified dimension of perceived harms; (2) the new venues where child abuse can be performed whether against a real or a fictitious child; and (3) institutional agendas geared by symbolic politics (*i.e.* something has to be done about it whether it is effective or not), moral entrepreneurs, media-made criminality, the prospect of financial gain and survival (*e.g.* by Internet hotlines, politicians, and software and hardware companies), and also a legitimate interest in protecting children against sexual abuse. They involve rationales tackling market failure (*i.e.* the Internet industry was unable to tackle the spillovers or negative consequences derived from their operation) and also protecting human rights (*i.e.* the protection of children), and this is one of the reasons why the politics of regulatory choice in this area is a complex matter: these regulatory decisions are based not only in market efficiency or better allocation of goods and services, but also on ethical grounds and questions of justice,[21] involving trade-offs between children protection and civil liberties' principles.

Many critics have argued that regulation of child pornography should focus on the primary abuse of children and international cooperation, not on blocking access to online material, because the latter is costly, ineffective and deflects attention from more important issues, *e.g.* protecting children against traditional 'offline' sexual abuse.[22] This investigation shows that such 'hands-off' rhetoric in relation to state involvement on the Internet has been defeated: the regulation of child pornography available online is increasing across the world. Governments were convinced that online child pornography has implications in the 'offline' world, *i.e.* that there is a causal relationship between the online child pornography and sexual abuse committed against children, that these images were not only fulfilling 'sexual fantasies' but are part of a comprehensive sexual exploitation industry. Indeed, the regulation of online child pornography is 'an idea whose time has come' and whose proponents (for example politicians, public opinion, the media, and group pressure campaigns) were ready to 'ride the wave'.[23]

Although these regulatory rationales have been successful in justifying the expansion of anti-child pornography laws and regulations for the online environment, their implementation raises a number of questions. Do these hybrid regulatory policies designed to limit access to child pornographic material available on the Internet represent a threat to free speech, privacy and other democratic values, *e.g.* the accountability, legitimacy and transparency? Do these concerns about free speech, privacy and democracy hold cross-nationally? Are there any safeguards in

---

[21] See ch 2 in Baldwin, R., Cave, M., and Lodge, M., *Understanding Regulation: theory, strategy and practice* (2nd edn.; Oxford: OUP, 2012).

[22] See *e.g.* Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008).

[23] See generally Kingdon, J., *Agendas, Alternatives, and Public Policies* (Updated 2nd edn.; London: Longman, 2011).

place to protect such values? What are the mechanics and administrative constraints of these policies? Is hybrid regulation employed in similar ways across different jurisdictions? Are these strategies converging towards a single universal model of regulation? Who is bearing the financial costs to implement these regulatory measures? Are these policies efficient, effective and ethical? These are questions that will drive this research.

1 The scope of this investigation

This study addresses the regulation of child pornography available on the Internet to evaluate the implications of hybrid regulation for free speech, privacy and democracy in the online environment. Nevertheless, a few issues in relation to the scope of this investigation are worth stressing in advance.

First, the problem of child pornography available on the Internet involves not only the production but the distribution of, and the access to, child pornographic material. Each activity involves a number of features and is subject to multiple regulatory responses. The production and distribution of child pornography on the Internet is addressed only peripherally in this investigation because they are not the focus of this research; this study focuses on the regulatory measures designed to limit access to child pornography available on the Internet.

Second, this investigation is not limited to the public web environment, but it takes into account the availability of child pornographic material in non-web applications and platforms. Although most of the regulation addressed in the case studies are about the measures tackling the child pornography available in public websites (*i.e.* notice and take down - NTD, and website blocking strategies), child pornography can also be accessed via anonymised peer-to-peer (P2P) channels and encrypted digital repositories, which are outside the reach of current policy and are a matter of time-consuming police investigation. As such, although the policymaking addressed in this investigation is focused mainly on web-based applications, the more inclusive term 'Internet' will be employed hereinafter so the wider regulatory phenomenon is included in the analysis and the partial effectiveness of current measures is exposed.

Third, although the focus is on the regulations to limit access to online child pornography, this study also explores the laws against child pornography *per se*, the criminal liability of intermediaries and surveillance powers of law enforcement authorities, and court cases in each jurisdiction in order to present the overall environment where these regulations operate. As such, it covers not only the laws and regulations that directly aim to limit access to child pornography available online (*e.g.* prohibition of knowingly accessing, and the use of NTD and blocking strategies) but those which indirectly inhibit or have a deterrent effect in such conduct (*e.g.* the prohibition of mere possession, production and distribution of child pornography, the facilitation of surveillance powers of law enforcement authorities, and the increased criminal liability of online intermediaries).

The study of lawmaking, police operations, criminal prosecution, sentencing, convicted offenders and victims in relation to online child pornography offences are outside the scope of this research. Although these issues are touched upon for the case studies to provide the context where the content regulatory policies were employed, this investigation is mainly about the relationships established between public and private actors to limit access to online child pornography hosted domestically, or hosted overseas but accessed within the relevant jurisdiction.

Finally, although Chapter 2 stresses that the regulation of controversial material available on the Internet occurs in a decentred and polycentric environment, the case study material shows that the state plays a central regulatory role in relation to the problem of child pornography whether by increasing the surveillance powers of law enforcement authorities or in bringing the online intermediaries into line via legislation, or otherwise. This issue is discussed further in Chapter 6, but it is important to bear this in mind from the outset.

2 Australia, Brazil and the United Kingdom: the case studies

Australia, Brazil and the United Kingdom were chosen because they had generally similar anti-child-pornography laws both domestically and internationally, they were considered democratic countries subject to democratic controls of content, and access to data was relatively unproblematic in these jurisdictions. This provided a common ground for comparison. More importantly, they were chosen as case studies because they had fundamentally different approaches to the constitutional framework, scope and mechanics of regulatory policies designed to limit access to child pornographic material on the Internet, despite the fact that they had similar anti-child pornography laws. This provided an opportunity to explore the ways in which substantively similar standards can be interpreted and enforced in different constitutional and enforcement settings.[24]

In Australia, the Commonwealth government established the online content regulations via legislation in 1999 so as to extend the existing regulation of television broadcasting to the online environment; this legislation was amended in 2004 and 2007. The scheme was centred in the government, via a statutory body, the Australian Communications and Media Authority (ACMA), and relied on a substantial number of statutes and administrative regulations to control the access to child pornography available on the Internet. Although the Commonwealth government was the central regulatory actor, online intermediaries (*e.g.* ISPs, ICPs, IHPs and Internet industry associations) also played a significant regulatory role via industry Codes of Practice (CoP). The Australian regulatory scheme targeted not only illegal material, *e.g.* child pornography but a wider range of content considered inappropriate to minors, *e.g.* adult pornography and violent material. Child pornographic material found and hosted domestically was required to be notified to the Australian police forces and the relevant online intermediary.

[24] The justification for the case study country choices is explored in detail in Chapter 3.

Child pornography hosted overseas but accessible via the Internet by Australian residents was targeted via a voluntary filtering scheme at the user-level. Nevertheless, there was also a voluntary blocking scheme at the ISP-level targeting child pornography websites employed by major Australian ISPs after July 2011. In addition, the Commonwealth government had plans to implement via legislation a mandatory filtering scheme at the ISP-level.

In Brazil, the criminal liability of online intermediaries and the NTD regime in relation to child pornography hosted domestically were established by legislation, but there was no comprehensive law to regulate the activities of online intermediaries in relation to other controversial content. Generally, the regulations in relation to online child pornographic material were put into place via agreements, not legislation, negotiated between the law enforcement authorities and the relevant online intermediaries: these measures included NTD, procedures regarding the recording and disclosure of users access' logs, and the relevant notification scheme. The Brazilian regulatory scheme also targeted not only child pornography hosted anywhere in the world, but material which could incite racial hatred or religious intolerance that was available to Brazilian residents via the Internet. Child pornographic material found and hosted domestically was required to be notified to the relevant law enforcement authority and online intermediary. Child pornography hosted overseas but accessed by Brazilian residents was notified to the relevant foreign police authority and overseas Internet hotline, if such existed in the host country. Online content filtering software could be used voluntarily at the user-level, but there had not been in Brazil any comprehensive use of filtering strategies to limit access to child pornography hosted in overseas websites.

In the United Kingdom, the regulatory scheme was centred in the Internet Watch Foundation (IWF), a self-regulatory body created in 1996 by the UK Internet industry under threat of legislation if online intermediaries did not come with a solution of their own. The IWF managed the reporting scheme, and notified both the police and the relevant online intermediary about the availability of child pornographic material available online. The IWF targeted not only the child pornographic material hosted anywhere in the world, but both the criminally obscene adult content and the cartoon child pornography hosted in the UK. Child pornographic material found and hosted domestically was required to be notified to the relevant police force and online intermediary. Child pornography found and hosted overseas but accessed by UK residents was targeted via a voluntary blocking scheme at the ISP-level that covered around 98% of Internet users in the United Kingdom; the reported URLs were also voluntarily notified to overseas Internet hotlines, if such existed in the host country.

3 Evaluation of regulatory policies to limit access to online child pornography

Chapters 2 shows that the academic literature has been concerned with a number of potential problems in relation to control of online content via hybrid regulation. These issues involve: (1) problematic interaction of public and private actors; (2) excessive reliance on architecture-based

regulatory strategies and invasive surveillance powers; and (3) unintended regulatory consequences. The hybrid regulation of controversial material available on the Internet involves the delegation of regulatory powers from the state to private actors and a number of trade-offs, because both state and private actors have agendas of their own. As such, the problematic interaction of public and private regulators has a number of potentially troubling implications (*e.g.* increasing the democratic deficit of regulatory policies, and the lack of transparency, legitimacy and accountability of regulatory measures put in place). The intensive use of architecture-based regulatory tools and increased surveillance powers given to law enforcement authorities have also raised a number of criticisms in the academic literature (*e.g.* violation of privacy, scope creep, and unchecked private censorship). Other potential negative consequences of hybrid regulation are the displacement of crime to darker corners of the Internet, inhibition of international cooperation, and the inefficiency and ineffectiveness of regulatory policies.

Given that this research addresses the regulation of access to child pornographic material on the Internet to evaluate the implications of hybrid regulation for free speech, privacy and democracy in the online environment, it established evaluative criteria divided into three broad categories: (1) free speech - involving the issues of unchecked private censorship, scope creep and lack of focus; (2) privacy protection - involving the issues of increased unchecked and more invasive surveillance powers given to law enforcement authorities; and (3) general democratic values - involving issues around the lack of transparency, accountability and legitimacy; lack of judicial and legislative oversight, and of citizen involvement; and also the inefficiency and ineffectiveness of regulatory intervention. In short, this investigation evaluates current hybrid regulatory initiatives to limit access to online child pornography in three different jurisdictions based on such evaluative criteria.

This exercise was important to confront the ideas, concepts and assumptions from the academic literature with the case study material. It also made evident the need for a flexible evaluative criteria able to incorporate fieldwork issues not previously found in the literature so as to reflect the different priorities and agendas, cultural regulatory contexts and cultures in place in different jurisdictions. Notably, the evaluative criteria were not intended to privilege any jurisdiction in terms of 'best' regulatory practices according to a pre-established top-down criteria,[25] but rather to identify, evaluate and discuss relevant issues that should be taken into consideration when designing regulatory measures tackling online child pornography.

4 The thesis roadmap

The first part of Chapter 2 includes a review of the literature and presents the overall conceptual framework of this investigation. It addresses models for regulating the controversial material available on the Internet taking into account the regulatory actors involved (*i.e.* the self, state

[25] See Bulmer, R., 'Why the Cassowary is not a bird', in Mary Douglas (ed.), *Rules and Meanings: the anthropology of everyday knowledge* (Harmondsworth: Penguin Books, 1967), 163-67.

and multi-state, and hybrid regulation) and explores the decentred and resilient nature of the online environment that rendered these regulatory models problematic. It also explores the negative consequences that hybrid regulation of content may have for free speech, privacy and democracy on the Internet, and develops evaluative criteria to assess such consequences. The second part of Chapter 2 presents the problem of child pornography on the Internet and explores regulatory measures employed in general taking into account the typology of regulatory models developed in part 1.

In sum, Chapter 2 reviews the relevant academic literature, establishes the conceptual framework on which this investigation is grounded and makes a case for a comparative study of regulatory policymaking employed in relation to child pornography available on the Internet in Australia, Brazil and the United Kingdom. The literature review also shows the reasons why online child pornography regulation was chosen to evaluate the implications of hybrid regulation.

Following this, Chapter 3 explains the methodological and ethical choices made to conduct this research. In addition, it explains how the documentary analysis and the expert consultation were employed to explore the anti-child pornography laws and regulations in the chosen jurisdictions under the framework of a cross-national multiple-case study.

Chapters 4 presents the case study material. It explores in detail the development of anti-child pornography laws and regulations to limit access to child pornographic content available on the Internet in Australia, Brazil and the United Kingdom, respectively.

Chapter 5 develops the comparative analysis. It applies the evaluative criteria to the case study material and discusses the relevant findings so as to produce an evaluative report on each jurisdiction for each criteria.

Chapter 6 is the conclusion of this investigation. It is based on the relevant findings of the comparative analysis and where links are made with the theory explored in Chapter 2. Notably, it shows what regulatory, governance and criminology theorists may learn from this research.

Finally, Chapter 7 considers the strengths and limitations of this research, addresses its importance and contribution to knowledge, and suggests an agenda for further research in the field.

Overall, this research selected the problem of child pornography available on the Internet to address the negative consequences of current online content regulatory policies, to explore the problematic implementation of regulatory measures and the trade-offs involved in protecting both children and civil liberties in the online environment, and to test out a number of concepts, ideas and assumptions from the academic literature.

CHAPTER 2: REGULATION OF CHILD PORNOGRAPHY ON THE INTERNET

> […] societal communication is a practice regulated by political institutions in all countries because of the essential role communication plays in both the infrastructure and the culture of society.[26]

> […] child pornography offers a critical case study for efforts to regulate the Internet, to enforce law in cyberspace.[27]

Endowed with an alleged unregulable, borderless, control-averse and anarchic nature, the Internet has changed the way people live and interact. It is now part of the everyday life of modern industrialised countries and has a number of implications not only for the media but economy, politics, national security and the law. Unsurprisingly, governments across the world have implemented a number of strategies to regulate different aspects of the Internet, particularly online material, ranging from a period of incipient top-down state intervention and self-governing libertarian activism towards escalation of domestic law, harmonisation of international laws, increased criminal liability of online intermediaries, more investigatory powers given to law enforcement agencies, use of architecture-based regulatory tools and implementation of sophisticated hybrid institutional arrangements.

The regulation of online material is problematic and has attracted the attention of regulation scholars. The decentred, polycentric and resilient regulatory environment of the Internet has challenged the ability of both state, via state regulation, and private actors, via self-regulation, to achieve efficient and effective results in line with the protection of civil liberties and human rights. As this chapter shows, a hybrid regulatory approach has been employed involving state and private regulators, the use of architecture-based regulatory tools, increased use of invasive surveillance powers by law enforcement authorities, and more legal liability placed on online intermediaries for the content they host or distribute. Nevertheless, this regulatory approach has been criticised on free speech, privacy and democratic grounds and a number of recommendations have been made in the academic literature.

Against this background, this chapter will: (1) explore regulatory and governance models employed to control online content; (2) design a typology of regulatory models for online content; (3) develop evaluative criteria to assess hybrid regulation applied to online content; and (4) make the case for applying this evaluative criteria to assess the regulation of online child pornography.

---

[26] Castells, M., *Communication Power* (Oxford: OUP, 2009), p 99.

[27] Jenkins, P., *Beyond Tolerance: Child Pornography on the Internet* (New York: New York University Press, 2001), p 5.

Child pornography was chosen because it is pushing the boundaries of online content regulation in ways that other problematic online content cannot because of an almost public disgust at child sexual abuse that makes criticism of such legislative drives morally difficult. In jurisdictions, such as Brazil, whilst cybercrime legislation moved slowly through Brazilian Parliament, specific provisions against online child pornography were enacted in 2008; in Australia, a voluntary scheme at the ISP-level to block access to websites allegedly hosting child pornographic images has been implemented whilst discussions of a broader scheme are still under way; and in the UK, anti-child pornography laws and regulations have developed well in advance when compared to copyrights infringement.[28] Child pornography is therefore a critical case study with which to analyse the developments of content-related regulatory strategies on the Internet and the negative implications that anti-child pornography regulatory measures have for free speech and privacy protection as well as for online democracy and good regulation, for example in terms of transparency, legitimacy and accountability of regulatory policies.

1. Regulation

This section explores concepts, ideas and debates from the regulation and governance literature to develop a conceptual framework within which online content regulation can be explored further. They involve the decentred and polycentric nature of the regulatory environment and models of regulation.

1.1 Regulation in a decentred regulatory environment

Regulation is addressed by a variety of disciplines such as law, economics and political science, and defined in a number of different ways leading to an 'excessive theoretical diffusion'[29] and no consensual definition about the topic,[30] but it is usually associated with the law and a discrete mode of governmental activity. For example, Baldwin *et al* point out three meanings of regulation: (1) targeted rules and their subsequent enforcement usually by the state; (2) any form of state intervention in the economic activity in general; and (3) all forms of social control whether initiated, intentionally or not, by a central actor such as the state or non-state agents.[31] In addition, Baldwin and Cave suggest that regulation can be used in the sense of: (1) a specific set of commands; (2) a deliberate state influence; or (3) all forms of social control that aims at restricting or facilitating behaviour.[32] Similarly, Morgan and Yeung define regulation more

---

[28] These issues will be discussed in detail in the case study material.

[29] Baldwin, R., Scott, C., and Hood, C., 'Introduction', in Robert Baldwin, Colin Scott, and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: OUP, 1998), 1-55, p 35.

[30] See Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 2; Baldwin, R., Scott, C., and Hood, C., 'Introduction', in Robert Baldwin, Colin Scott, and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: OUP, 1998), 1-55, p 2; Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46, p 134-5.

[31] Baldwin, R., Scott, C., and Hood, C., 'Introduction', in Robert Baldwin, Colin Scott, and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: OUP, 1998), 1-55, p 3.

[32] Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 2.

broadly as the phenomenon of using all forms of social control (intentionally or not) by actors in an authoritative position (usually the state) via different enforcement mechanisms in the pursuit of policy goals and according to predefined rules.[33] Finally, Brownsword employs a working concept of regulation that defines the 'regulator' narrowly and 'regulation' broadly so that regulation is regarded as any controlling or channelling mechanisms used by regulators (in the narrower sense of agent or agency in a position to control and channel behaviour).[34]

Not only the definition of regulation but also that of regulatory environment is framed in different ways to cope with the complexity of the modern networked society. For Black, regulatory regimes are increasingly decentred because the state has no central role in regulation because authority is diffused throughout society, and polycentric because of multiple sites where regulation occurs at sub-national, national, supranational and transnational levels and is marked by fragmentation, complexity and interdependency between actors.[35] By exploring the transformations of modern regulation, particularly the failure of traditional command and control strategies, and the shift of regulatory authority within society, Black examines the concept of regulation under a decentred perspective (*i.e.* decentred from the state and diffused through society) and argues that such a decentred understanding of regulation is based on five elements: (1) complexity, referring to both causal complexity (*i.e.* social problems are a result of different factors) and complexity of interaction between actors; (2) fragmentation of knowledge because no single actor has all knowledge to solve the problem, and fragmentation of the exercise of power and control because the government has no monopoly of regulation; (3) autonomy of actors in the sense that actors will continue to develop and behave as self-determined bodies; (4) complexity of interactions and interdependencies amongst social actors; and (5) the rejection of a clear distinction between the public and private (for example, formation of institutional arrangements that combine governmental and non-governmental actors in a number of different ways).[36]

This concept is in line with approaches applied to the regulation of online child pornography which considers the regulatory environment as multi-layered: not only the state regulates but a wide range of private actors, such as online intermediaries, Internet industry associations and Internet users are enrolled in the regulatory process at both national and international levels.[37]

---

[33] Morgan, B. and Yeung, K., *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007), p 3.

[34] Brownsword, R., *Rights, regulation, and the technological revolution* (Oxford: OUP, 2008), p 7.

[35] See Black, J., 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Law Society Economy Legal Studies Working Paper No. 2/2008* (London: London School of Economics and Political Science, Law Department, 2008) at <http://www.lse.ac.uk/collections/law/>, accessed 03 April 2012, p 2, 3 and 6.

[36] Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46; and also Black, J., 'Critical reflections on regulation', *Australian Journal of Legal Philosophy,* 27 (2002), 1-35.

[37] See *e.g.* Akdeniz, Y., 'Governance of Pornography and Child Pornography on the Global Internet: a multi-layered approach', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: regulating cyberspace* (Oxford: Hart Publications, 1997), p. 223-41

Furthermore, there is a growing body of literature applying insights from both network and complexity theories to Internet regulation. For example, Murray describes the regulatory environment of the Internet in terms of a symbiotic system where relevant actors and regulatory instruments produce a complex array of interactions with both intended and unintended consequences.[38] Similarly, Guadamuz stresses that awareness of concepts such as network robustness and resilience, power laws and scale-free networks, spontaneous ordering and self-organising environments may help regulators understanding the implications of a particular regulatory initiative applied to the online environment and thus improve the ability of regulators to deliver better regulation.[39]

There is also an international dimension that adds up to the complexity of the regulatory environment as regulatory problems escape national boundaries. For Morgan and Yeung, regulatory tools designed to address such international dimension are more consensus and communication-orientated, informal dimensions of enforcement are explored further, and expert-based models of legitimacy are more common in international regulatory environments.[40] Similarly, Black points out that transnational regulatory regimes are: (1) organised around particular regulatory domains, for example environment, food and trade, rather than geographical regions; (2) characterised by an intertwined international, transnational, national and sub-national decisionmaking and jurisdictional overlapping; (3) found to have no pattern of institutional interrelationships; and (4) linked through negotiations and informal communications.[41]

This international dimension is a crucial element for the success of multi-state regulation of online child pornography. The multi-jurisdictional nature of the Internet challenges the enforcement of both national laws and international treaties because of the different definitions given to child pornographic material and types of criminal conduct associated with such material, and the varying levels of expertise and motivation of domestic police forces, to name a few examples.

The regulatory challenges posed by modern networked society-led regulation theorists frame the regulatory environment as a decentred and polycentric environment subject not only to government intervention but to multiple actors within a wider scope of governance. This occurs in relation to different regulatory domains be it environmental[42] or crime control. Indeed, as a

---

[38] Murray, A., 'Symbiotic Regulation', *The John Marshall Journal of Computer & Information Law,* XXVI(2) (2008), 208-28; See also Grabosky, P., 'Discussion Paper: Inside the Pyramid: Towards a Conceptual Framework for the Analysis of Regulatory Systems', *International Journal of Sociology of Law,* 25 (1997), 195-201.

[39] Guadamuz, A., *Networks, Complexity and Internet Regulation: Scale-Free Law* (Cheltenham, UK: Edward Elgar, 2011).

[40] Morgan, B. and Yeung, K., *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007), p 305.

[41] Black, J., 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Law Society Economy Legal Studies Working Paper No. 2/2008* (London: London School of Economics and Political Science, Law Department, 2008) at <http://www.lse.ac.uk/collections/law/>, accessed 03 April 2012, p 12.

[42] See for example Gunningham, N., Grabosky, P., and Darren, S., *Smart Regulations: Designing Environmental Policy* (Oxford: OUP, 1998).

result of numerous changes in social order (for example technological, cultural, social, political, and economic), new regulatory rationales and configurations have been implemented: *e.g.,* the monopoly of policing by state actors has given place to governance of security. As a result, police functions became more diverse and complex within society, because state police alone has been unable to tackle contemporary crime and maintain order.[43]

For example, control of controversial online content is performed not only by traditional law enforcement agencies, but by a multitude of private actors in a pluralistic and multilayered manner.[44] The responsibility for policing controversial online content has been delegated to online intermediaries, commercial firms and Internet users in a network of shared responsibilities and this occurs not only in relation to actual policing of content but in regards to provision of services and goods for crime prevention (for example, online content filtering and surveillance systems).[45] For Zedner, however, private policing has a much longer history. As she argues, state policing responsibility grew out of individual responsibility.[46] Yet, the fact is that this systematic and widespread dispersion of policing powers to private actors has a number of implications in contemporary society and this has became more evident in recent times.

Indeed, the decentred regulatory environment and displacement of regulatory responsibilities to private actors raise a number of issues in relation to democratic legitimacy, transparency and accountability, because of conflictual public and private interests involved. Each individual actor will ultimately push their own agendum forward in detriment of public interest. Accordingly, Dupont argues that traditional mechanisms of accountability and evaluation are unable to grasp the new morphology of security networks, because these mechanisms are generally focused on single organisations or individuals.[47] Loader points out that policing functions are being passed on to non-state actors which are not subject to traditional mechanisms of police accountability (such as legal restraints, a framework of democratic institutions and internal organisational devices).[48] Similar criticisms have also been made in relation to international regulatory regimes generally. For example, Black argues that there are issues in relation to non-transparent operation, poor consultation processes and decisionmaking not open to public scrutiny, undemocratic operation, inadequate systems of redress, and a lack of proper accountability. For Black, there are fundamental regulatory dilemmas and trade-offs associated with the emerging technologies that include finding a balance between flexibility and

---

[43] Reiner, R., *The Politics of the Police* (3rd edn.; Oxford: OUP, 2000), p 240.

[44] See Jewkes, Y., 'Public policing and Internet crime', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: WIllan Publishing, 2010), 525-45, p 539; Grabosky, P., *Electronic Crime* (Master Series in Criminology; Upper Saddle River, NJ: Pearson Prentice Hall, 2007), p 15; Akdeniz, Y., 'Governance of Pornography and Child Pornography on the Global Internet: a multi-layered approach', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: regulating cyberspace* (Oxford: Hart Publications, 1997), p. 223-41; and also McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 269-71.

[45] Yar, M., 'The private policing of Internet crime', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 546-61, p 546.

[46] Zedner, L., 'Policing Before and After the Police: the historical antecedents of contemporary crime control', *British Journal of Criminology,* 46 (2006), 78-96.

[47] Dupont, B., 'Security in the Age of Networks', *Policing & Society,* 14(1) (2004), 76-91, p 83.

[48] Loader, I., 'Plural Policing and Democratic Governance', *Social & Legal Studies,* 9(3) (2000), 323-45.

predictability; independence and accountability; expertise and detachment; and speed and due process.[49] For Stenning, however, this apparent lack of accountability of private policing bodies in comparison to public agencies is debatable, because there are a variety of mechanisms in place (*e.g.* criminal and civil liability, state regulation, industry self-regulation, labour law, contractual liability, and the market) whereby private actors may be held accountable; and also because public police accountability via constitutional and statutory regimes (whether political, judicial or administrative) may be exaggerated and ineffective.[50]

In sum, the analysis of online content regulation developed here is based on a broader definition of regulation (*i.e.* multiple regulatory actors and strategies) and of a decentred and polycentric regulatory environment (*i.e.* one approach that displaces the loci of regulatory authority away from the state and towards multiple locations).[51] It is also worth stressing that the decentred and resilient nature of the regulatory environment and the dispersal of regulatory powers away from the state are central to understanding which consequences regulatory intervention has for free speech, privacy protection and also for legitimacy, transparency and accountability of current policies.

1.2 Regulatory models

Another important issue to address in this investigation are the models of regulation applied to online content. Regulators employ a number of tools in the pursuit of their goals. For example, the government not only regulates when it enacts criminal law (*i.e.* primary legislation) but when it runs public awareness programmes and adopts product design strategies.[52] The government also regulates via administrative rules (*e.g.* second and tertiary legislation) and discretion. Lawmakers regulate via the production of primary legislation,[53] the courts regulate when they issue a sentence, private actors regulate when an industry association designs and approves a code of practice and try to enforce it against its members, and citizens also regulate via different participatory channels.[54] Morgan and Yeung classify regulatory tools into five categories: (1) command; (2) competition; (3) communication; (4) consensus; (5) and code (*i.e.*

---

[49] Black, J., 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Law Society Economy Legal Studies Working Paper No. 2/2008* (London: London School of Economics and Political Science, Law Department, 2008) at <http://www.lse.ac.uk/collections/law/>, accessed 03 April 2012, p 1-2 and 13.

[50] See Stenning, P., 'Powers and Accountability of Private Police', *European Journal on Criminal Policy and Research,* 8 (2000), 325-52. The recent inability of the private company G4S to provide enough security staff for the 2012 London Olympic Games is a good case study to test out these claims. See Topping, A., 'G4S Olympic scandal: Ed Miliband calls for rethink of police outsourcing', *The Guardian,* 2012, sec. Politics at <http://www.guardian.co.uk/politics/2012/jul/19/g4s-olympic-ed-miliband-police>, accessed 20 July 2012.

[51] In fact, narrower definitions of regulators (*i.e.* only state agents) neglects that regulation of online content is increasingly not centred in the state but dispersed throughout society, involving both state and private actors. See for example Raab, C. and De Hert, P., 'The Regulation of Technology: Policy Tools and Policy Actors', *Tilburg University Legal Studies Working Paper No. 004/2007; TILT Law & Technology Working Paper Series No. 003/2007* (The Nederlands: Tilburg University, 2007) , p 17.

[52] Brownsword, R., *Rights, regulation, and the technological revolution* (Oxford: OUP, 2008), p 8.

[53] Baldwin, R., *Rules and government* (Oxford socio-legal studies; Oxford: OUP, 1995), p 7.

[54] This takes into account a more decentred view of regulation, *i.e.* the basic features of the regulatory enterprise such as standard setting, detecting and changing behaviour are pulverised in society and enforced by different actors, not only the government.

architecture).[55] For Black, there are rules (legal, quasi-legal and non-legal), social and economic forces, and technologies.[56]

Lessig's online regulatory model has four modalities of regulation which includes the law, social norms, the market and architecture; each modality affects the regulatory target in a different way. Lessig gives the example of an anti-smoking regulatory policy that employs these regulatory modalities to limit smoking behaviour.[57] The law can prohibit the selling of cigarettes to children and restrict smoking to certain areas. In addition, social norms may affect smoking behaviour, because people have to ask permission for smoking in someone's car or may be judged negatively by non-smoking individuals. Similarly, the market can impose restrictions on smoking by altering its price. Finally, the architecture can also regulate smoking habits when cigarettes are designed to be odour-free or monitoring equipment is installed in a non-smoking area. Based on Lessig's four modalities of regulation, Murray and Scott identify fifteen (pure and hybrid) regulatory tools that may be used to control different aspects of the online environment.[58] Finally, Brownsword presents the concepts of regulatory (1) mode, (2) pitch, (3) phasing, and (4) range, adding new layers of complexity to regulators' toolbox.[59]

Hood and Margetts classify government regulatory tools under the concepts of detectors as '[…] all the instruments government uses for taking in information', and of effectors as '[…] all the tools government can use to try to make an impact on the world outside.'[60] Based on these instruments, they introduce four types of government resources used to regulate: nodality, authority, treasure and organisation. Nodality is the property of being in an advantageous regulatory position within the network. Authority is the ability to command and control via procedures and symbols. Treasure is generally the stock of moneys and organisation is the stock of land, building, equipment and specialised personnel available to the government. Notably, detectors and effectors (*i.e.* tools for information collection and shaping behaviour, respectively) are available in each one of these domains. As a result, governments can combine detectors and effectors within each domain in different manners to control controversial online content. For example, organisation like the police or a statutory regulator may be used to suppress information (*e.g.* Internet filtering in China) or to regulate access to online adult pornography (for example, Australia). Treasure may be used as an incentive for voluntary filtering usage (for example free online content filtering available in Australia) or adoption of a blocklist (for example only ISPs that implement the IWF blocklist can provide Internet services to the British

---

[55] Morgan, B. and Yeung, K., *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007), p 9.

[56] Black, J., 'Critical reflections on regulation', *Australian Journal of Legal Philosophy,* 27 (2002), 1-35, p 12.

[57] Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 122-3.

[58] Murray, A. and Scott, C., 'Controlling the New Media: Hybrid Responses to New Forms of Power', *Modern Law Review,* 65 (2002), 491.

[59] Brownsword, R., *Rights, regulation, and the technological revolution* (Oxford: OUP, 2008), p 12-3.

[60] Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007), p 3.

government).[61] Authority may be used to create the obligation to notify criminal content (for example, US ISPs are obliged by law to notify law enforcement about the availability of child pornographic content) and force online intermediaries to take down content. Governments are struggling to find nodality in an environment where regulatory power is dispersed and such nodal position can be gained via formal authority, such as forcing online intermediaries to work for the government as online gatekeepers.[62]

Hood and Margetts produced a useful conceptual framework around the use of regulatory tools not only because it mapped different ways in which governments regulate online content (and the government is often the main regulatory actor in such domain, despite regulatory dispersal) but because it could be used in cross-national comparison (for example comparing ways in which these tools are used cross-nationally). In addition, such a model can be used to characterise the varying institutional arrangements of content regulation, because of its focus on tools not the regulatory actor.

As the last few paragraphs show, there are a number of regulatory tools and approaches available to regulators and a mix of them will often be employed to address the regulatory target.[63] For example, different regulatory targets in relation to the online environment such as domain names, technical protocols, pornography, privacy protection and copyrights infringement, involve different actors and demand different strategies.[64] Ultimately, there is no easy solution that gives regulators an 'off-the-shelf' regulatory tool, because some targets may be more responsive to certain tools and there are sensitive cultural and political issues involved.

The politics of regulatory choice proved useful in guiding regulators vis-à-vis such variety of regulatory targets and tools available. For some, however, the choice over the proper regulatory mix often results not from pure rational choice but from 'irrational policymaking, faith and politics'.[65] Often technically inefficient instruments are chosen because of domestic constitutional constraints, human rights concerns, pressure from particular interests groups and political parties, or treaties' obligations, instead of more economically efficient choices with lower social costs.[66]

---

[61] See OGC, 'Procurement Policy Note – Blocking access to web pages depicting child sexual abuse. Action Note 05/10', (The Office of Government Commerce, 2010) at <http://www.ogc.gov.uk/documents/PPN_05_10_Blocking_illegal_sites.pdf> Accessed 09 July 2011.

[62] See Zittrain, J., 'A History of Online Gatekeeping', *Harvard Jornal of Law & Technology,* 19(2) (2006), 253.

[63] For Grabosky, *e.g.,* any solution to the problem of digital crimes involves a combination of regulatory instruments. See Grabosky, P. and Smith, R., *Crime in the Digital Age: controlling telecommunications and cyberspace illegalities* (New Brunswick-NJ and Sydney: Transaction Publishers and Federation Press, 1998), 223. See also Landau, M., 'Rationality, and the Problem of Duplication and Overlap', *Public Administration Review,* 29(4) (1969), 346-58.

[64] Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, MA: MIT Press, 2001), p 356.

[65] Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007), p 13.

[66] Trebilcock, M., et al., 'The Choice of Governing Instrument', (Ottawa: Canadian Government Pub. Centre, 1982) at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997355>, accessed 12 July 2012, p 27.

Indeed, there are a number of trade-offs and political struggles involved in the process of choosing regulatory tools and models of intervention,[67] and such politics of choice can be even more problematic within a cross-national regulatory environment, because similar regulatory problems may have quite dissimilar regulatory responses in different locations as a result of available resources available, social relationships as well as cultural and technological contingencies.[68]

Regulatory arrangements also reflect the jurisdiction they are based on.[69] For example, some governments regulate in a 'spirit of collaboration' (*e.g.* government and private actors participating in decisionmaking), whereas others address them in a spirit of 'threat' (*e.g.* government forcing private actors to follow a particular strategy under the threat of passing a draconian legislation). For example, Baldwin *et al* suggest that regulation in the United Kingdom tends to be generally less formal and less transparent because British regulators are prone to use self-regulation under the shadow of threats of legislative development, whereas in the US, regulation tends to be generally more formalised and legalistic.[70] Regulatory models tackling online child pornography also differ in jurisdictions such as Australia, Brazil and the United Kingdom, although they all settled on a similar approach to child pornography regulation.

Another issue worth mentioning is the redundancy of regulatory tools that may be a strength in some circumstances, such as flight security, data transmission and corruption control in government, as a device for the suppression of error.[71] Nevertheless, it may constitute excessive, unnecessary and costly control in other events, for example the regulation of controversial material available online, where duplication of reports, unchecked private censorship and delaying red tape are undesired.

This wide range of regulatory tools can be used by either state, such as the law, and private actors (for example, Internet industry Codes of Conduct); they combine a variety of social resources and capacities in the pursuit of policy goals and private interests, and these regulatory configurations, or models of regulation, can be classified according to different criteria.

For example, the literature classifies regulatory models for the online environment in different ways. Solum divides regulatory strategies for the Internet into: (1) self-governing; (2)

---

[67] Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007), p 161.

[68] Ibid , p 129. See also DiMaggio, P. and Powell, W., 'The Iron Cage Revisited: institutional Isomorphism and Collective Rationality in Organizational Fields', *American Sociological Review,* 48(2) (1983), 147-60.

[69] Braithwaite, J. and Ayres, I., *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: OUP, 1992), p 101; Cave, J., Marsden, C., and Simmons, S., 'Options for and Effectiveness of Internet Self- and Co-Regulation. Summary prepared for the European Commission', (Cambridge: RAND Europe, 2008) at <http://www.rand.org/pubs/technical_reports/2008/RAND_TR566.pdf>, accessed 04 June 2010, p 9.

[70] Baldwin, R., Scott, C., and Hood, C., 'Introduction', in Robert Baldwin, Colin Scott, and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: OUP, 1998), 1-55, p 22-3.

[71] See Landau, M., 'Rationality, and the Problem of Duplication and Overlap', *Public Administration Review,* 29(4) (1969), 346-58.

transnational and international institutions; (3) national regulation; (4) code; and (5) the market.[72] Weber also includes a self-governing strategy[73] and Lessig's four modalities of regulation is based on the law, social norms, the market and architecture.

They are classified here instead as state (state and multi-state regulation), non-state (self-regulation) or a mix of the two (hybrid regulation) and this classification takes into account the main regulatory actors involved, be it the state, private actors, or a mix. These models are therefore: (1) self-regulation; (2) state and multi-state regulation; and (3) hybrid-regulation. There are other classifications[74] but the choice of such taxonomy was to facilitate the analysis developed along this research.

State regulation is centred on the notion of the state imposing standards backed by the threat of criminal sanctions.[75] Its use often reflects the desire of state regulators to impose rules and prohibit behaviour with immediacy in a way that shows to public opinion that the government is acting forcefully,[76] and involves not only rule-making but also enforcement and sanctioning by the state.[77] This regulatory model has a number of limitations. It is prone to capture and legalism; it is difficult to set appropriate standards; it may be either excessively narrow or broad in scope which makes its enforcement problematic; its instruments may be inappropriate and unsophisticated; the government may lack the proper expertise; its implementation is often inadequate and the regulated may be insufficiently motivated to comply.[78] It may also fail for example to tackle the resilient and multi-jurisdictional nature of the Internet.

Self-regulation involves the development of rules by an organisation or association which attempts to enforce these rules against its own members,[79] and is commonly employed in a variety of areas such as advertising, financial services and professional occupations. As a policy option, it may be hard to define because it can materialise via intra-firm regulation, legal civil contracts (private contracting), soft-law, collective arrangements, unilateral adoption of standards, and involvement of industry in rule-formation.[80] Nevertheless, Ogus argues that although substantially different institutional arrangements may be labelled self-regulatory, they do share common features and tend to be employed whenever: (1) one activity is affected by

---

[72] Solum, L. B., 'Models of Internet Governance', in Lee A. Bygrave and John Bing (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 48-91, p 55.

[73] Weber, R., *Regulatory models for the online world* (New York: Kluwer Law International, 2002).

[74] Hood and Margetts *e.g.* categorised regulatory intervention by policy instruments. See Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007).

[75] States however employ other regulatory strategies as well.

[76] Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 35.

[77] Baldwin, R., Scott, C., and Hood, C., 'Introduction', in Robert Baldwin, Colin Scott, and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: OUP, 1998), 1-55, p 14.

[78] Generally see Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 36-8; Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46, p 106; and also Black, J., 'Critical reflections on regulation', *Australian Journal of Legal Philosophy,* 27 (2002), 1-35, p 2.

[79] Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 39.

[80] Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46, p 121.

market failure (usually due to externalities and information asymmetry); (2) private law instruments are inefficient or excessively costly; and (3) it is considered a better policy option when compared to state regulation.[81]

Generally self-regulatory rationales are based on the assumption that non-state actors have more expertise than public agents, enforcement costs are reduced, rules are more flexible and less formal, and the overall regulatory costs are not borne by taxpayers.[82] Nevertheless, Black argues that both state and non-state institutions may have similar levels of expertise and capabilities, because usually no actor within the decentred regulatory arena has the capabilities and resources to tackle alone the regulatory problems (*i.e.* the regulatory authority, expertise and resources are dispersed throughout society).[83] Similarly, Ogus argues that self-regulation may lack democratic legitimacy and accountability, show unfairness of procedure and fail to effectively enforce rules against disobedient members.[84]

Self-regulation involves the state to some extent, because private actors can rarely act out of purely private initiative, but rather within prior government mandate and legislative framework, be it veiled or clearly manifested act. For example, Baldwin and Cave argue that despite its state-less appearance, self-regulation may be in place as a result of government threat that '[…] if nothing is done state action will follow'.[85] Similarly, Price and Verhulst stress that there are different configurations for the 'self' of self-regulation.[86]

Finally, other regulatory strategies involve closer partnership amongst state and non-state institutions as regulatory actors, intensive use of architecture-based strategies, and increased surveillance measures; it is often referred as co-regulation or hybrid regulation and will be explored further in Section 3 below.

So far, this section has addressed two building blocks of this investigation: (1) the decentred nature of the regulatory environment that allows for a dispersal of regulatory powers which has, in its turn, implications for regulatory policies; and (2) a taxonomy of regulatory models. This analytical framework will be developed further in the next sections in relation to the regulation of online content.

2 Regulation and the Internet

---

[81] Ogus, A., 'Rethinking Self-Regulation', *Oxford Journal of Legal Studies,* 15(1) (1995), 97-108.

[82] See Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 199; and also Ogus, A., 'Rethinking Self-Regulation', *Oxford Journal of Legal Studies,* 15(1) (1995), 97-108.

[83] Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46, p 114.

[84] Ogus, A., 'Rethinking Self-Regulation', *Oxford Journal of Legal Studies,* 15(1) (1995), 97-108.

[85] Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 126.

[86] Price, M. and Verhulst, S., 'In the search of the self: Charting the course of self-regulation on the Internet in a global environment', in Chris Marsden (ed.), *Regulating the Global Information Society* (London: Routledge, 2000), 57-78.

Section 1 addressed a number of issues from the regulation literature in order to start a dialogue with the literature about online regulation. Nevertheless, before the latter is explored, it is important to explain what the Internet is and discuss the concept of Internet regulation used within the scope of this investigation.

2.1 Defining the Internet

> This "Internet" that everyone is talking about is, fundamentally, nothing more than a gigantic global machine designed to move zeroes and ones from one place to another.[87]

Human interaction is each day becoming more and more mediated by communication technologies and the Internet is perhaps the one that most radically and rapidly transformed the dynamic of interactivity between human beings.[88] It is increasingly common to find people working, interacting with friends, exchanging ideas, purchasing goods, paying taxes and developing a wide range of social relationships via and with the support of the Internet.

The Internet can be described as a distributed digital network derived from an academic, military and industry joint partnership that was later shaped by commercial actors in addition to the increasing activism and participation of the online community.[89] For example, Curran argues that the Internet is a contested space that reflects a combination of different values from scientists, political activists, market agents and the government.[90] In fact, Internet is an umbrella term that gives name to a range of different things interchangeably: it may be considered a computer network, a mechanism for information dissemination, a platform of collaborative work, a technological tool to facilitate interaction amongst individuals, a disruptive technology, but also a playground for paedophiles and a safe haven for illegal filesharing. It is also a resilient, international, and self-organising network that embraces numerous platforms and applications. These numerous different views emphasise specific features and uses of the technology and fulfils different agendas.[91]

For Post, there are different networks including home-, office-, local area-, wide area- and TCP/IP-networks that connect computers and also other networks around the world. The type of network that connects other networks are referred to as inter-network or internet. There are thousand upon thousands of internets connecting networks out there. Post refers to the big global-spanning network as the inter-network or simply, the Internet (capitalised) in order to

---

[87] Post, D., *In search of Jefferson's moose: notes on the state of cyberspace* (Oxford: OUP, 2009), p 86.

[88] See generally Wu, T., *The Master Switch: The Rise and Fall of Information Empires* (Digital Kindle edn.; London: Atlantic Books, 2010) about the evolution of information industries in the 20th century.

[89] For a detailed description about the history of the Internet see: Hafner, K. and Lyon, M., *Where Wizards Stay Up Late* (New York: Simon & Schuster, 1998); Leiner, B., et al., 'A Brief History of the Internet' *Internet Society* (2003); < http://www.isoc.org/internet/history/brief.shtml> accessed 02 December 2011; Mueller, M., *Rulling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, MA: MIT Press, 2002); and also Bing, J., 'Building Cyberspace: a brief history of the Internet', in John Bing and Lee A. Bygrave (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 8-47.

[90] Curran, J., 'Reinterpreting Internet history', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 17-37.

[91] See generally Lakoff, G. and Johnsson, M., *Metaphors We Live By* (Chicago: Chicago University Press, 1980).

differentiate it from the other existent internets,[92] and this is the definition used within the scope of this investigation. This is because such definition highlights the regulatory domain addressed in this research which involves not only the public but also the private networks that constitute the Internet.

The literature commonly refers to the social environment where human interactions occur as cyberspace, whereas the infrastructure, software, technical standards and protocols are referred to as the Internet. For example, Lessig considers cyberspace as the social environment where people interact, whereas the Internet is considered the medium of communication.[93] Taylor and Quayle assume a similar distinction whilst examining the role of the (1) infrastructure, protocols, software and technical standards (*i.e.* the Internet) in regard to the increased distributive nature of online child pornography, and the role of the (2) online social environment (*i.e.* cyberspace) affecting the way online sexual offenders normalise and validate their criminal conducts within the peer community.[94] The terms Internet and cyberspace will be used interchangeably within the scope of this investigation because they often overlap and it is often irrelevant to make this distinction when considering online content regulation.

Notably, this investigation assumes no clear-cut divide between the non-virtual and the virtual world;[95] it does not distinguish between the online and the offline environment, because to speak of cyberspace as a distinct place, disconnected from the 'real', offline, non-virtual space is becoming increasingly difficult to sustain. Human interaction is each day more and more mediated by communication technologies and 'online' behaviour has real implications for the 'offline' world.

2.2 Defining Internet regulation

Internet regulation involves regulation of human behaviour, regulatory institutional action, and the use of regulatory technologies on the Internet in the broader sense of the term, *i.e.* without making distinctions between the online and offline world. Internet regulation is considered here as the social phenomenon whereby regulators attempt to control and channel behaviour within the Internet, in the sense of its infrastructure, technical protocols and standards, and content, be they related to political, economic, technical or legal issues. As such, there are a number of different regulatory challenges and targets in relation to the Internet environment (for example infra-structure, technical protocols, controversial content, domain names) and each of them raises a regulatory analysis of their own.

---

[92] Post, D., *In search of Jefferson's moose: notes on the state of cyberspace* (Oxford: OUP, 2009), p 24-6.

[93] Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 83.

[94] See generally Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003).

[95] For Reed, this is the 'cyberspace fallacy'. See Reed, C., *Internet Law: Text and Materials* (2nd edn.; Cambridge: Cambridge University Press, 2004), p 7. See also Murray, A., *Information Technology Law: the law and society* (Oxford: OUP, 2010), p 56; Goldsmith, J., 'Regulation of the Internet: Three Persistent Fallacies', *Chicago-Kent Law Review,* 73 (1998), 1119-31.

It is also important to address the concept of Internet governance and explain how it relates to the concept of Internet regulation used here. Governance is usually perceived as an alternative to government but it has multiple meanings and uses, including the reform of government, the set of coordinating activities in regulatory networks, new trends in economic development and the dynamics of international institutions.[96] In addition, it is considered a by-product of recent challenges towards the concept of the state (*i.e.* institutions and personnel exercising authority within a territory) and the state's ability to influence behaviour by using alternative tools rather than traditional command-and-control instruments.[97] Governance may also indicate a transformation in policymaking from central state authority and coercive regulatory instruments towards a decentred and polycentric understanding of regulation (as discussed in Section 1.1 above), reflecting the patterns of regulation distributed amongst social actors where uncontested state authority is replaced by shared social responsibility.[98] In addition, it involves the interdependence amongst state and non-state actors, the blurred distinction between the public and the private and the autonomy from the state, which raises issues about the 'democratic deficit' (meaning the lack of legitimacy and accountability) in decentred regulatory regimes.[99] It should be clear by now that the concept of Internet regulation used in this investigation reflects this change in governmental role as well as the decentred nature of the regulatory environment. It is therefore in line with the idea of governance explored in political science literature.[100]

Regulation and governance may be used interchangeably to reflect this understanding of regulation where authority is diffused, the regulation is decentred and the environment is polycentric. Nevertheless, Internet regulation will be preferred so as to distinguish the regulatory target addressed here (the controversial content available online) from the broad use of Internet governance referring to issues around the infrastructure, protocols and technical standards of the Internet.[101] This is because Internet governance may refer to different domains

---

[96] Hirst, P., 'Democracy and Governance', in Jon Pierre (ed.), *Debating governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000), 13-35, p 13-8.

[97] Pierre, J., 'Introduction: Understanding Governance', in Jon Pierre (ed.), *Debating Governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000), p 1-2.

[98] Ibid, p 4.

[99] Black, J., 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Law Society Economy Legal Studies Working Paper No. 2/2008* (London: London School of Economics and Political Science, Law Department, 2008) at <http://www.lse.ac.uk/collections/law/>, accessed 03 April 2012; Rhodes, R. A. W., 'Governance and Public Administration', in Jon Pierre (ed.), *Debating Governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000), p 61.

[100] See generally Hirst, P., 'Democracy and Governance', in Jon Pierre (ed.), *Debating governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000), 13-35; Rhodes, R. A. W., 'Governance and Public Administration', in Jon Pierre (ed.), *Debating Governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000); Rhodes, R. A. W., *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Buckingham: Open University Press, 1997); Pierre, J., 'Introduction: Understanding Governance', in Jon Pierre (ed.), *Debating Governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000).

[101] See for example, WSIS, 'Working Group on Internet Governance: Report From the Working Group on Internet Governance', World Summit on the Information Society, at http://www.itu.int/wsis/docs2/pc3/html/off5/index.html, 2005) at <http://www.itu.int/wsis/index.html>; Bauer, J., 'Internet governance: theory and first principles', in Ravi Kumar Jain Bandamutha (ed.), *Internet governance: an introduction* (Hyderabad, India: The Icfai University, 2007), 40-59; Dutton, W. and Peltu, M., 'The Emerging Internet Governance Mosaic: Connecting the Pieces', *Forum Discussion Paper No. 5* Oxford Internet Institute, University of Oxford, 2005) ; Solum, L. B., 'Models of Internet Governance', in Lee A. Bygrave and John Bing (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 48-91 p 51-2; Glebstein, E. and Kurbalija, J., 'Internet Governance: issues, actors and divides', *DIPLO Report* DIPLO / GKP, 2005) at <http://www.diplomacy.edu/ISL/IG/>, p 10.

of regulatory intervention on the Internet and, depending on the issue at stake, such as domain names disputes, Internet infrastructure, technical protocols, or wider political issues of digital divide and market competition, regulatory analysis may involve different regulatory actors and strategies (for example, the Internet Corporation for Assigned Names and Numbers, government statutory regulators, Internet Engineering Task Force, or the Word Summit on the Information Society).[102] In short, this investigation addresses models of regulation applied only to controversial content available on the Internet. Regulation of Internet infrastructure, its protocols and technical standards, or public policies against the digital divide, to name a few examples, are outside the scope of this investigation.

3 Regulating online content

Which social actor is better equipped to deliver effective responses to online content regulation: the state, non-state actors, or both? Are the Internet community and industry able to resolve on their own the conflicts in relation to problematic online material? Should the state delegate this regulatory responsibility to non-state actors? What are the trade-offs involved? What are the implications of this dispersal of regulatory power for democratic legitimacy, accountability and transparency? These questions were briefly addressed in Section 1 above in relation to regulation generally; they are explored below in more detail in regards to online content regulation.

The self-governing mantra of cyberlibertarians argues that traditional command-and-control state-based regulation is ill-prepared and unable to tackle the complex regulatory issues found in cyberspace. The state therefore should give way to bottom-up, online community and Internet industry self-regulatory strategies. It puts forward a ‘hands-off’ rhetoric in relation to state involvement in the Internet. Nevertheless, the self-regulation argument failed to convince regulators, particularly after the Internet achieved substantial economic, social and political importance across the world after the mid-1990s. As a result, nation states updated their laws and regulations to tackle controversial content available online, whether it is related to pornography, violation of privacy, defamation, incitement to racial hatred, copyright infringement, politically sensitive material or child pornography. These measures were however challenged by the multi-jurisdictional nature of the Internet. This led governments to harmonise criminal laws and procedures via international treaties. Nevertheless, multi-state regulation also proved to be problematic for a number of reasons that will be explored later. Against this background, hybrid regulatory strategies were taken onboard to address the limitations of both self and state regulation.

3.1 Self-regulation

[102] See generally Feick, J. and Werle, R., 'Regulation of Cyberspace', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2010), 523-47.

After its inception, the Internet was considered a free environment by its own nature. It was regarded as a place invulnerable to state regulation, a separate jurisdiction, a control-averse and anarchic space. According to this standpoint, information should flow freely in cyberspace and state intervention was neither possible nor legitimate. The Declaration of the Independence of Cyberspace encapsulates this anarchic ethos[103] and influenced many scholars thereafter. According to this manifesto, the Internet was a place where governments '[…] have no moral right to rule us nor […] possess any methods of enforcement we have true reason to fear […].'[104] A number of features of the Internet such as no central point of control, the distributed way it transported digital content, its multi-jurisdictional nature, the claimed protection of anonymity of users and novelty of the media helped to advance the cyberlibertarians' discourse.

This initial enthusiasm about the self-regulatory and anarchic nature of the Internet can be explained by the historical and political contexts of that time. The Internet was not yet part of the everyday life of many people, many online content-related conflicts was outside the political agenda, and many governments were ill-prepared to enforce the law in cyberspace as individuals were enhanced in their power to overcome traditional state-based regulatory strategy.[105] Against this background, Post and Johnson argued that '[…] new rules will emerge to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world.'[106] For them, the proper way of policy-making in cyberspace is to leave it to develop on its own via bottom-up decisionmaking by the individuals directly involved;[107] a process also called spontaneous self-organisation, or 'spontaneous ordering.'[108]

Although often used interchangeably, self-regulation and spontaneous ordering are conceptually different. Spontaneous ordering, also self-organisation, means that the environment will regulate itself without external influence (for example Internet users regulating their own environment or online vigilantes tackling child pornographic content). On the other hand, Internet self-regulation means generally the initiative of private actors (*e.g.* Internet service and content providers, software and hardware manufacturers, schools and public libraries) adopting common guidelines and regulating themselves within an environment with little state interference.[109] The latter involves a degree of intentional regulatory action, whereas the former

---

[103] Sometimes called cyberspace libertarianism. See Spinello, R., *Regulating cyberspace: the policies and technologies of control* (Westport, Conn.: Quorum Books, 2002), p 34.

[104] Barlow, J., 'A Declaration of the Independence of Cyberspace ' (1996); <http://homes.eff.org/~barlow/Declaration-Final.html> accessed 04 June 2010.

[105] Shapiro, A., *The control revolution: how the Internet is putting individuals in charge and changing the world we know* (New York: PublicAffairs, 1999).

[106] Post, D. and Johnson, D., 'Law and borders: the rise of law in cyberspace', *Stanford Law Review,* 48 (1996), 1367-75, p 1367.

[107] Post, D. and Johnson, D., 'The New 'Civic Virtue' of the Internet: A Complex Systems Model for the Governance of Cyberspace', in C. Firestone (ed.), *The Emerging Internet (1998 Annual Review of the Institute for Information Studies)* (1998).

[108] Solum, L. B., 'Models of Internet Governance', in Lee A. Bygrave and John Bing (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 48-91, p 57.

[109] Cave, J., Marsden, C., and Simmons, S., 'Options for and Effectiveness of Internet Self- and Co-Regulation. Summary prepared for the European Commission', (Cambridge: RAND Europe, 2008) at <http://www.rand.org/pubs/technical_reports/2008/RAND_TR566.pdf>, accessed 04 June 2010, p 4.

means no-regulation at all. Yet, self-regulation is used here in a wider sense involving a number of similar regulatory strategies and thus also encompasses the notion of spontaneous ordering by the private actors involved.

The self-regulation approach assumes that the Internet is an organic force non-regulable and able to resist regulation.[110] It also assumes two distinct social environments (*i.e.* the traditional 'real' offline and the new virtual online space). Based on the assumption that '[…] cyberspace has no territorially based boundaries', Post and Johnson argue that the law and the sovereign states are unable to effectively regulate content and exercise territorial jurisdiction in the online world.[111] In addition, individual freedom is supposedly secured by the Internet's 'intrinsically' free nature, and cyberspace's rules derive from the Internet community. Although this argument has failed to reflect reality, for them, such a self-regulated environment would organically develop legal and regulatory institutions of its own.

> The development of a true "law of Cyberspace" therefore, depends upon a dividing line between this new online territory and the nonvirtual world. Our argument so far has been that the new online sphere is cut off, at least to some extent, from rule-making institutions in the material world and requires the creation of a distinct law applicable just to the online sphere.[112]

Similarly, Johnson *et al.* maintained that structures and relationships already in flux on the Internet are able to tackle online threats and problems, because new technologies and their resulting social interactions would enable a decentred and efficient decision-making process for the online environment. For them, the decentralised decisionmaking strategy is the best option for Internet governance when compared to the 'benevolent dictatorship' (*i.e.* single central authority over the Internet) or the 'representative democracy' (*i.e.* the transposition of democratic institutions to the online world), both of which are based on traditional state-regulation.[113]

For Post, the self-regulation strategy is still able to help understanding and managing the Internet regulatory dilemmas. Against the background of Jefferson's legacy he analyses current dilemmas posed by the Internet, such as those involving the law and governance, networks, and system design as a conversation between the Jeffersonian rationale (*i.e.* an approach based on liberty) which embraces chaos and diffusion of power, and the Hamiltonian rationale (*i.e.* an approach based on authority) which embraces order and concentration of power:

> I don't know, to be honest, what they'll come up with, what those lawmaking institutions and processes will look like, or should look like, in a virtual world […] What I do know

---

[110] See Spinello, R., *Regulating cyberspace: the policies and technologies of control* (Westport, Conn.: Quorum Books, 2002), p 34.

[111] Post, D. and Johnson, D., 'Law and borders: the rise of law in cyberspace', *Stanford Law Review,* 48 (1996), 1367-75, p 1370.

[112] Ibid , p 1395.

[113] Johnson, D., Crawford, S., and Palfrey, J., 'The Accountable Net: Peer Production of Internet Governance', *Berkman Center for Internet & Society at Harvard Law School Virginia Journal of Law and Technology,* 9(9) (2004), p 32.

> is that people have the right to make those decisions and answer those questions for themselves.[114]

The self-regulatory stance encapsulates important insights for online regulation and establishment of technical protocols of the Internet. The bottom-up decisionmaking, the principle of rough consensus and running code,[115] the self-organising ability to interpret censorship as damage and 'routes around it,'[116] and agreements negotiated via community self-regulatory mechanisms are considered by governance bodies (*e.g.* the ICANN and IETF) as innovative and efficient managerial practices to tackle the critical technical resources and operations of many technical aspects of the Internet.

During the early days of the Internet some states like the US were slow to regulate and let the Internet (meaning the Internet infrastructure and its commercial uses) develop by private investment in an environment relatively free from governmental influence. For example, Zittrain argues that there has been a historical forbearance assured by US Courts for lax state-regulation towards the Internet.[117] Similarly, self-regulatory strategies play an important role in maintaining order in online environments such as eBay,[118] Facebook and Wikipedia. These strategies also include the establishment and enforcement of terms of service and other private agreements, Internet industry CoCs, online communities own decisionmaking, parental and school content monitoring, and also individual users' choice have relevant roles to play here.

Nevertheless, self-regulation has proven to be problematic not only in relation to infrastructure issues,[119] but in regard to controversial content available on the Internet. Indeed, the protection of critical infrastructure and national cybersecurity, control of criminal activities, protection of privacy and the rights of copyright holders, amongst other things, demand direct state intervention and mediation, because self-regulation and self-governing strategies alone are unable to resolve the problems these issues bring about; the Internet has challenged traditional state-based regulatory approaches but it has also failed to be an entirely self-regulated environment.[120]

3.1.1 Limitations of self-regulatory strategies to control online content

---

[114] Post, D., *In search of Jefferson's moose: notes on the state of cyberspace* (Oxford: OUP, 2009), p 186.

[115] Russell, A. L., "Rough Consensus and Running Code' and the Internet-OSI Standards War', *IEEE Annals of the History of Computing,* 28(3) (2006), 48-61.

[116] Quote from the cyber-activist John Gilmore (Electronic Frontier Foundation) at Elmer-Dewitt, P., 'First Nation in Cyberspace', *Time Magazine*, 49 (1996) at <http://www.chemie.fu-berlin.de/outerspace/Internet-article.html> accessed 22 March 2012.

[117] Zittrain, J., 'A History of Online Gatekeeping', *Harvard Jornal of Law & Technology,* 19(2) (2006), 253, p 298.

[118] See the example of eBay's online community at Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006), p 135.

[119] See *e.g.* the need of state intervention to secure broadband access in deprived areas and reduce the so-called digital divide.

[120] Solum, L. B., 'Models of Internet Governance', in Lee A. Bygrave and John Bing (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 48-91, p 59.

The conclusion that this notion of two separated spaces (*i.e.* one online and one offline environment) is not reflected in reality undermined the self-regulation argument. Online human behaviour has implications for the offline world because they are intertwined. As noted in Section 2.2 above, 'offline' actions have implications in the 'real' world. The Internet has always been regulated by governments since its inception:[121] it is 'full of laws'.[122] Self-regulation hardly operates without any type of state-based regulatory framework. For example, Oswell argues that self-regulation occurs within a context of statutory powers and law enforcement agencies, otherwise private actors would have limited powers and no criteria about how to operate.[123] Similarly, Price and Verhulst argue that self-regulation occurs in different configurations and via different levels of involvement with state actors (*e.g.* regulatory agency oversight and judicial review), because it rarely exists in a vacuum.[124] Ultimately a nation state will exercise its authority over the Internet if online transactions reach its territory, pose a threat to its national security or interests, or affect its nationals.

For example, Brazilian criminal courts requested overseas online intermediaries operating in Brazil (such as Google and Microsoft) both the connection and content data about Brazilian residents involved in online-related criminal offences, and also requested removal of alleged criminal material from their overseas hosts, but accessed from within Brazil, whenever the reported material violated Brazilian domestic laws.[125] In 1999, the Australian government updated its offline censorship laws to enforce them in relation to the online environment.[126] Similarly, the controversial content restrictions enforced in 'offline' China are employed in the Chinese 'online' environment.[127] The US and British governments responded to the growing threat that cyber-attacks pose to their critical national infrastructure, and to society in general, with the creation of specialised units, and increased surveillance powers.[128]

---

[121] Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009), p 106.

[122] Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012), p 13-4.

[123] Oswell, D., 'Media and Communications Regulation and Child Protection: An Overview of the Field', in Sonia Livingstone and Kirsten Drotner (eds.), *International Handbook of Children, Media and Culture* (London: Sage, 2008), 469-86, p 478.

[124] Price, M. and Verhulst, S., *Self Regulation and the Internet* (The Hage, The Netherlands: Kluwer Law International, 2005), p 3-6.

[125] The Brazilian law enforcement authorities and courts have made a number of requests to Google Inc. See *e.g.* Drummond, D., 'Greater transparency around government requests', *The Official Google Blog* (2010) at <http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html> Accessed 24 Aug 2010.

[126] Broadcasting Services Amendment (Online Services) Act 1999 (Cth Australia).

[127] See generally Bambauer, D., et al., 'Internet Filtering in China in 2004-2005: A Country Study', *Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2005-10*, 2005) at <http://ssrn.com/paper=706681>; Faris, R., Roberts, H., and Wang, S., 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', *The OpenNet Initiative Bulletin* The OpenNet Initiative, 2009) ; ONI, 'Internet Filtering in China', OpenNet Initiative, 2009) at <http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf>, accessed 04 June 2010; Zittrain, J. and Edelman, B., 'Empirical Analysis of Internet Filtering in China', *IEEE Internet Computing,* (November 2002 2003).

[128] Beaumont, P., 'US appoints first cyber warfare general', *The Observer,* 23 May 2010 at <http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general>, accessed 24 Aug 2010; See also the surveillance project at the US NSA at Bamford, J., 'The Black Box', *Wired Magazine*, April (2012) at <http://www.wired.com> accessed 03 April 2012; and current plans to expand surveillance powers in the UK at Syal, R., Halliday, J., and Siddique, H., 'Theresa May defends email surveilance plans', *The Gardian,* 04 Aprii 2012, sec. UK Police at <http://www.guardian.co.uk/uk/2012/apr/03/theresa-may-email-surveillance-plans>, accessed 04 April 2012.

Self-regulation alone was unable to tackle copyrights' violation on the Internet and the state had to come onboard. See for example the case of the 2010 Digital Economy Act.[129] This piece of legislation threatens alleged domestic civil infringers with an escalation of technical measures that include notifications by ISPs, slowing down Internet connection, Internet disconnection and blocking of websites.[130] Nevertheless, according to an initial obligation code, a further act of the UK Parliament is required to implement measures such as throttling or disconnection.[131]

In addition, a British court has recently ordered domestic ISPs to block access to the alleged illegal filesharing website Pirate Bay.[132] The British attempt to regulate online copyright infringement via legislation and the courts exposed the failure of the market to regulate illegal filesharing of copyrighted material on the Internet on its own. Given that the Internet service and content providers, Internet users, right-holders, and the media industry were unable to resolve the conflicts in relation to copyright protection on the Internet by themselves, governments were forced to intervene via legislation and the courts.

The limitations of self-regulatory strategies to control online content are also in relation to privacy protection on the Internet. Self-regulation can be employed to protect privacy online via different regulatory tools (*e.g.* commitments, codes of conduct, standards, seals, guidelines and terms of service).[133] For Charlesworth, the scope of self-regulation has expanded and broadened over the years to protect online privacy. He points out the move from mere symbolic commitments towards codes of conduct, standardisation of practices and the identification of non-compliant members as well as from a focus on organisations towards sectors and functions at the national and international levels, respectively.[134] For example, it has been reported that Google, Microsoft, Yahoo and AOL have agreed to sign a voluntary agreement, created by the US federal government, to set minimum standards in relation to privacy protection of US customers.[135]

Nevertheless, self-regulation of privacy protection on the Internet is not without criticisms. There is little evidence to support the conclusion that free market regulation is able to tackle commercial private abusers and preserve the public interest of Internet users. In addition, it is increasingly hard to believe that industry funded agencies will effectively enforce privacy

---

[129] Digital Economy Act (c. 24) 2010 (England and Wales).

[130] Edwards, L., 'Law and sausages: How Not to Legislate for the Digital Economy', at <http://blogscript.blogspot.com/>, accessed 03 May 2010.

[131] See OFCOM, 'Online Infringement of Copyrights and the Digital Economy Act 2010: Draft Initial Obligations Code', (London: Ofcom, 2010) at <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf> Accessed 24 November 2012.

[132] Halliday, J., 'British ISPs will block The Pirate Bay within weeks', *The Guardian,* 30 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/30/british-isps-block-pirate-bay>, accessed 01 May 2012.

[133] Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: The MIT Press, 2006).

[134] Charlesworth, A., 'Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: A Framework for Electronic Commerce.* (2nd edn.; Oxford: Hart Publishing, 2000), p 81.

[135] See Arthur, C. and others, 'Google, Microsoft, Yahoo and AOL back US 'consumer privacy bill of rights'', *The Guardian,* 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/feb/23/google-microsoft-yahoo-aol-privacy>, accessed 22 March 2012.

policies, particularly when the costs of compliance exceed the benefits of breaching the policies, so it may be the case that regular oversight from government is necessary when incentives for compliance are weak.[136] For Bennett and Raab, there is a perception that self-regulation of online privacy is more symbolic than real because those responsible for the implementation of protective policies have real interest in processing personal data with as little regulation as possible.[137] For example, the US Federal Trade Commission has notified Facebook about violations of privacy[138] and this is one of the reasons why the politics of privacy protection on the Internet involves not only self-regulation, but domestic statutory protection via legislation, regulatory agencies, jurisprudence as well as transnational and technical instruments.[139] The House of Lords and House of Commons Joint Committee on Privacy and Injunctions has recently recommend that there should be legislation forcing search engines like Google to block search results containing information found by the courts to be violating the privacy of individuals.[140]

In sum, a lack of governmental oversight on the Internet may leave online users vulnerable to market interests. This is true not only in regards to the protection of online privacy and the regulation of illegal content, but in respect of management of the network infrastructure. According to Weiser, private actors have been working with the network management with little government interference. Taking the example of the Spring/Cogent Internet backbone issue and the Comcast/Bit Torrent network management case, both of which are conflicts between private actors managing a infrastructure which is considered to be a public resource, he argues that a lax governmental policy may harm Internet users' interests.[141] Similarly, the poor availability of Internet access in economically deprived areas is also a case of the private overcoming the public interest and of a necessary state intervention to achieve a balance.

Self-regulation seems to be not only ineffective but also a source of unintended consequences. For example, Marsden *et al.* argue that whilst self-regulatory strategies seem to be more responsive and flexible, it is less transparent and often operates with lower procedural standards.[142] Similarly, Cave *et al.* points out that the use of self-regulation to control online content may also result in privacy and free speech violations, function creep, private censorship,

---

[136] Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: The MIT Press, 2006).

[137] For Ball, the Internet 'giants' such as Google and Facebook may be clueless about what to do with the sheer volume of private data they have, but this argument is debatable. See Ball, J., 'Me and my data: how much do the internet giants really know?', *The Guardian,* 22 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/22/me-and-my-data-internet-giants>, accessed 01 May 2012.

[138] Rushe, D., 'Facebook reaches deal with FTC over 'unfair and deceptive' privacy claims', Ibid2011 at <http://www.guardian.co.uk/technology/2011/nov/29/facebook-ftc-privacy-settlement>, accessed 28 December 2011.

[139] Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: The MIT Press, 2006).

[140] 'Privacy and injunctions: Session 2012-12', *Joint Committee on Privacy and Injunctions* (London: House of Lords and House of Commons, 2012) at <http://www.publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/273.pdf>, accessed 01 May 2012, p 56.

[141] Weiser, P., 'The Future of Internet Regulation', *University of Colorado Law Legal Studies Research Paper No. 09-02,* (2009), p 4.

[142] Marsden, C., Tambini, D., and Leonardi, D., *Codifying cyberspace: communications self-regulation in the age of internet convergence* (New York: Routledge, 2007), p 291.

and the same content may be subject to numerous CoCs and accountable to several different bodies in a self-regulatory regime.[143] This is why many propositions have been made in this regard. For example, Marsden *et al.* suggest that in order to strengthen efficiency of self-regulation intervention, such practices should: (1) suffer external auditing; (2) be able to fulfil public interest criteria; (3) publish clear benchmarks over transparency, accountability and due process; (4) share public guidelines on transparency and due process; (5) avoid capture by industry; and (6) empower consumer groups.[144] Similarly, Price and Verhulst suggest that self-regulatory instruments need more consumer and citizen involvement, stronger commitment of industry members, effective accountable channels, effective monitoring rules and proper enforcing standards to improve current policies.[145]

Although self-regulation has an exciting libertarian appeal in the sense of freedom from government interference and more flexible governance arrangements, state intervention is not only necessary to mediate conflicts and avoid abuses but it is a *sine qua non* condition for overall stability and development of the online environment. For Goldsmith and Wu, state coercion is needed for any source of governance on the Internet, because '[…] the greatest dangers for the future of the Internet come not when governments overreact, but when they don't react at all.'[146] The next section explores state and multi-state regulation applied to online material.

3.2 State and multi-state regulation

> Other technologies have challenged government's authority; other pioneers have gleefully declared the death of the state. What their stories show us, though, it that while technology can gravely wound governments, it rarely kills them. Instead, governments survive because, ironically, both society and entrepreneurs want them. Governments provide the property rights that entrepreneurs eventually want, the legal stability that commerce craves, and the stability that society demands. For in the end, even pirates and pioneers want order. Once they have staked their claim or claimed their loot, they want someone else to protect it. And that someone else is usually the state.[147]

---

[143] Cave, J., Marsden, C., and Simmons, S., 'Options for and Effectiveness of Internet Self- and Co-Regulation. Summary prepared for the European Commission', (Cambridge: RAND Europe, 2008) at <http://www.rand.org/pubs/technical_reports/2008/RAND_TR566.pdf>, accessed 04 June 2010, p 119, 112 and 121.

[144] Marsden, C., Tambini, D., and Leonardi, D., *Codifying cyberspace: communications self-regulation in the age of internet convergence* (New York: Routledge, 2007), p 298-305.

[145] Price, M. and Verhulst, S., 'In the search of the self: Charting the course of self-regulation on the Internet in a global environment', in Chris Marsden (ed.), *Regulating the Global Information Society* (London: Routledge, 2000), 57-78, p 75.

[146] Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006), p 145 and 181.

[147] Spar, D., *Ruling the Waves: From the Compass to the Internet, a History of Business and Politics along the Technological Frontier* (New York: Harcourt, 2001), p 5. Wu calls this historical process in relation to the information industry of 'The Cycle' and asks whether the Internet will have the same regulatory destiny of older media, *i.e.* from 'revolutionary novelty and youthful utopianism to centralized and integrated industry'. See Wu, T., *The Master Switch: The Rise and Fall of Information Empires* (Digital Kindle edn.; London: Atlantic Books, 2010), p 6. Sonin (1999), cited by Roland, showed that this may not be always the case: '[…] Russian oligarchs benefit from low security of property rights, since low security allows them to convert corporate and social assets to their private use.' See Roland, G., 'The Political Economy of Transition', *Journal of Economic Perspectives,* 16(1) (2002), 29-50, p 32.

Self-regulation neglected the role that governments were playing since the beginning of Internet and many potential regulatory mechanisms available to regulators. Although little governmental intervention was evident during the early days of the Internet, the state was involved whether financing its creation or providing the legal framework whereby private actors could exploit it commercially. The cyber-libertarian rhetoric in relation to online content regulation failed to reflect reality as nations across the world are increasingly exercising national sovereignty over their territories and nationals via lawmaking, enforcement and sentencing, making way to '[…] a bordered network where territorial law, government, power, and international relations matter as much as technological invention.'[148]

Governments have employed domestic legislation to control access to online adult pornographic to protect children. For example, two pieces of legislation originally designed to block access to legal adult pornography by children, the US 1996 Communications Decency Act (CDA 1996)[149] and the US 1998 Child Online Protection Act (COPA 1998)[150] were enacted in the United States of America. In a similar vein, *LICRA et UEJF v Yahoo! Inc. and Yahoo France* showed how a nation state attempted to assert its national laws in the online environment via the courts.[151] The French law prohibits the trafficking of Nazi memorabilia in France, but this material was easily available to all French Internet users via an auction website of Yahoo! hosted in the US, where the availability of Nazi goods is perfectly legal under the wide constitutional protection of free speech.

The Internet has no geographical boundaries and it reaches a number of different jurisdictions. Child pornography for example became a notorious problem in the online environment across the world. As a result, different jurisdictions criminalised conducts (*e.g.* production, distribution and access), types of material (*e.g.* photographs, pseudo-photographs, cartoon pornography, text and audio recordings) and increased criminal penalties associated with online child pornographic content.[152] The escalation of anti-child pornography laws occurred not only domestically but internationally. The 2001 CoE's Cybercrime Convention[153] and the UN 2000 Optional Protocol[154] are examples of such attempt to harmonise anti-child pornography laws at the international level in order to face the multi-jurisdictional challenge posed by the Internet.

State regulation is not limited to lawmaking and sentencing but enforcement. Specialised police agencies were created in many jurisdictions to tackle online child pornographic content,

---

[148] Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006), p vii.

[149] Communication Decency Act 1996 § 502, 110 Stat. (United States of America).

[150] Child Online Protection Act 1998 (United States of America).

[151] *LICRA et UEJF v Yahoo! Inc. and Yahoo France*, Tribunal de Grande Instance de Paris, Superior Court of Paris.

[152] The regulation of online child pornographic content will be explored in detail in Chapter 3.

[153] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[154] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

incitement to racial hatred, online financial crimes and copyrights infringement. International police operations were conducted to tackle online content-related crimes and the harmonisation of procedural criminal law has been pursued.[155]

Although state regulation of online content is increasing, this model has a number of limitations. The proliferation of laws, court decisions and policing of online material domestically have been challenged by the resilient nature of the Internet. Similarly, international harmonisation of online content-related criminal laws and the police cooperation at the international level fall short because of the slow ratification process of international treaties and of different levels of expertise and financial resources available to law enforcement agencies. The next section will explore these limitations further.

3.2.1 Limitations of state and multi-state regulatory strategies to control online content

Enforcement of domestic laws targeting production, distribution and access to problematic content was arguably relatively effective and straightforward before the Internet. Access to adult pornographic material by children was easier to control because of architectural constraints such as the presentation of a valid identification for age verification,[156] and the proliferation of child pornography was limited by the constraints of the print copies, analog cameras, and mail services available. Nevertheless, following the exponential growth of the Internet after the mid-1990s, the enforcement of domestic laws in relation to controversial content became problematic.

> […] it is extremely difficult and costly to enforce traditional legal-regulatory control systems within cyberspace, due to a variety of factors including a relative degree of anonymity, lack of physicality, digitisation of content, environmental plasticity and the international or cross-border nature of the network.[157]

First, digitisation of content facilitated the transmission of information, be it photographs, video, print documents or music, via the digital networks. Digitised text, image, audio and video could be easily and rapidly transferred from one location to another without degeneration of original information. This also facilitated storage of information. For example, a large volume of print pornographic material could be stored in a small hard disk after being digitised.

Second, the architecture and technical protocols of the Internet allowed information to be transferred via an international network without a central point of control. This limited the ability of governments to control problematic content and facilitated the anonymity of alleged offenders. The Internet protocol (IP) address identifies not the person that produced, distributed or accessed the content on the Internet but only the machine where data is sent or received (*i.e.*

---

[155] See for example the 24/7 International Police Network established by the Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[156] See for example how code can help enforcing the law in the case of adult pornography regulation in Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 249-255.

[157] Murray, A., *The regulation of cyberspace: control in the online environment* (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006), p 205.

the user's digital identity is not necessarily his/her physical world identity).[158] The Internet can be accessed via different encrypted channels to protect anonymity and make identification difficult. There are also a number of different points of control, because more actors are now involved in producing and distributing content. There are different online intermediaries responsible for receiving, hosting and passing on packets of data (*e.g.* Internet service and content providers, Internet backbones, transmission hosts, resource hosts, communication services, social networking and online payment systems).[159]

Third, the Internet poses a multi-jurisdictional challenge to enforcement of content-related laws. The Internet is an international network that connects people across different jurisdictions and it is subject to different regulatory schemes and legislation. It crosses national borders where national governments have no sovereign authority.[160] Many countries with underdeveloped laws can become safe havens for cybercriminality, finding the origin and the offender associated with the criminal material can be problematic, and the question of which jurisdiction should prosecute is open to debate.[161] In short, these issues render the choice of jurisdiction and enforcement of jurisdictional powers heavily problematic when applied to criminal content available online.

Although state regulation is necessary to frame a cadre of privacy responsibilities and rights, it hardly prevents inappropriate collection and use of personal data online. Governmental initiatives to protect personal data online have limitations. For example, the 1995 EU Data Protection Directive[162] is based on the concept of informed users but people hardly read the terms of service when signing up for an online service, and given that personal data is both a human rights and a commercial construct, ultimately, governments have to balance the pros and cons of prioritising the protection of personal data or the commercial interest, because this could attract or repel global investments.[163]

The Internet challenged not only enforcement of domestic laws but law-making processes. The choice of whether to enforce the old or create new laws, the design of proportionate criminal retribution and deterrent measures, the flexibility to cope with technological changes, the protection of civil liberties, and the need to harmonise laws at the international level are examples of challenges that lawmakers face.[164] For Reed, the difficulties of enforcing the law in

---

[158] Reed, C., *Internet Law: Text and Materials* (2nd edn.; Cambridge: Cambridge University Press, 2004).

[159] See Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69; and also ch 4 in Reed, C., *Internet Law: Text and Materials* (2nd edn.; Cambridge: Cambridge University Press, 2004).

[160] Spar, D., *Ruling the Waves: From the Compass to the Internet, a History of Business and Politics along the Technological Frontier* (New York: Harcourt, 2001), p 5.

[161] Grabosky, P., 'The Global Dimension of Cybercrime', *Global Crime,* 6(1) (2004), 146-57, p 150 to 153.

[162] European Data Protection Directive (Directive 95/46/EC), 24 October 1995 (European Union).

[163] Charlesworth, A., 'Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: A Framework for Electronic Commerce.* (2nd edn.; Oxford: Hart Publishing, 2000); and Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: The MIT Press, 2006).

[164] Samuelson, P., 'Five Challenges for Regulating the Global Information Society', in Chris Marsden (ed.), *Regulating the Global Information Society* (London: Routledge, 2000).

cyberspace made it nearly impossible to achieve minimum levels of effectiveness in areas such as tackling copyrights infringement via online filesharing, and thus it is necessary to include the cyberspace actor's perspective and a normative understanding into the lawmaking equation to increase the chances of people acting lawfully.[165] The ever changing online environment is far ahead of the lawmaking process and this creates a problematic regulatory gap that produces an arguably irrational escalation of content-related criminal laws. For example, although no real child is involved, computer-generated images and cartoon imagery associated with child pornography have been criminalised in the UK.

The multi-jurisdictional nature of the Internet has forced governments to design content-related criminal laws at the international level via a *sui generis* non-country specific body of law or the harmonisation of existing laws.[166] The 2001 CoE's Cybercrime Convention[167] contains substantive and procedural criminal law to tackle online child pornography and copyrights infringement. It was supplemented by the 2006 Additional Protocol[168] to cover racist and xenophobic content available on the Internet. The 2001 Convention shows how problematic multi-state regulation is on the Internet. The signature, ratification and implementation by member and non-member states is slow and the right to exclude certain provisions may lead to discrepancies amongst states which undermines cross-national policing and mutual assistance.[169] For example, multi-state regulation of online child pornography via international law (*e.g.* the 2000 UN Optional Protocol and the 2001 CoE's Cybercrime Convention) faces numerous difficulties to be enforced internationally, because moral, cultural, political and legal domestic environments may render a uniform criminal regulatory approach towards legal definition and types of child pornographic content as well as the relevant criminal conducts and penalties particularly problematic on the Internet.[170] Indeed, discrepancies in terms of substantive and procedural criminal laws can limit the success of the law as a form of state-regulation in a borderless international environment.[171] The future implementation of the 2001

---

[165] Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012), p 49 and 219.

[166] Zittrain, J., 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', in Adam Thierer and C. Wayne Crews Jr (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: CATO Institute, 2003), 13-31, p 18 and 21.

[167] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[168] Additional Protocol to the Convention of Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature commited through computer systems 2003 (opened for signature on 28/01/2003, entered into force on 01/03/2006, CETS No. 189, Strasbourg) (European Union).

[169] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 199-202; Dutton, W. and Peltu, M., 'The Emerging Internet Governance Mosaic: Connecting the Pieces', *Forum Discussion Paper No. 5* Oxford Internet Institute, University of Oxford, 2005) , p 22; Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006), p 166-67.

[170] Murray, A., *The regulation of cyberspace: control in the online environment* (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006), p 209; Gillespie, A., 'Defining Child Pornography: Challenges for the Law', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010.

[171] Murray, A., *The regulation of cyberspace: control in the online environment* (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006), p 225.

CoE's Cybercrime Convention by non-European states has been undermined, because some countries are for the establishment of a new agreement based on a non-Eurocentric process.[172]

In sum, the Internet has challenged the ability of self, state and multi-state regulatory strategies to control problematic content available online. Against this background, a number of other strategies have been taken onboard. First, governments legislated domestically to increase the criminal liability of online intermediaries as well as the investigatory powers of law enforcement agencies so as to identify alleged offenders, collect criminal evidence and take-down alleged criminal content available online. Second, regulators started to force online intermediaries to police online content bypassing conventional judicial and legislative channels. Third, both state and non-state actors used a number of architecture-based regulatory tools extensively (for example online filtering and blocking systems as well as tethered appliances) at both the ISP and user-levels to control content available online. The problematic enforcement of content-related criminal laws on a decentred regulatory environment led to the implementation of a multitude of regulatory strategies by state and private actors. These hybrid strategies will be explored in detail below.

3.3 Hybrid regulation

The sections above showed that self, state, and multi-state regulatory strategies have been employed across the world to control controversial content available online, and that these strategies showed a number of limitations. The problematic enforcement of such strategies has lead to a multitude of regulatory arrangements involving state and private actors and this combination is regarded elsewhere as the best regulatory strategy not only in relation to the online environment but other domains.[173] For Murray, for example, *de facto* control over online content can only be achieved via '[…] a web of terms and conditions of service and thorough Lessigian code-based solutions […]' not merely thorough legal documents whether domestically or internationally.[174]

Some hybrid regulatory armaments encourage relevant private actors to implement regulatory systems of their own that can be scrutinised by regulators, blend persuasion and coercion, and release, at least partially, the state from the burden of exclusive direct enforcement.[175]

---

[172] UN, 'Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, 12-19 April 2010)', at <http://www.unodc.org/unodc/en/crime-congress/crime-congresses.html>, accessed 04 December 2011.

[173] Solum, L. B., 'Models of Internet Governance', in Lee A. Bygrave and John Bing (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 48-91, p 56, 87; Murray, A., *The regulation of cyberspace: control in the online environment* (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006), p 229; Gunningham, N. and Grabosky, P., *Smart Regulations: Designing Environmental Policy* (Oxford: OUP, 1998).

[174] Murray, A., 'Uses and Abuses of Cyberspace: Comingo to Grips with the Present Dangers', in Antonio Cassese (ed.), *Realizing Utopia: The Future of Internacional Law* (Oxford: OUP, 2012), 496-507, p 497.

[175] Gunningham, N., 'Enforcement and Compliance Strategies', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2012), 120-45, p 140.

In sum, hybrid regulation (also co-regulation, smart regulation, or meta-regulation) is a regulatory strategy that involves both state and non-state actors as active regulators. For Marsden *et al.*, it is a:

> […] a middle way between state regulation and 'pure' industry self-regulation […] expresses a dialogue between stakeholders, which results in a form of regulation which is not state command-and-control regulation in its bureaucratic central […] specialised functions, but it is also not 'pure' self-regulation as we observed in industry-led standard setting in Internet infrastructure.[176]

Perritt Jr. also employs the concept of hybrid regulation but with a different meaning. For him, hybrid regulation is the public law framework that inhibits excessive control of content undertaken by private actors. He regards hybrid regulation as a public remedy to deficiencies of self-regulation (*e.g.* when private control is enforced via filtering systems that excessively block access to online content in opaque and unaccountable manners).[177] Nevertheless, this investigation takes a more sceptical view of governmental agency, because the 'government itself is a power that must be checked'.[178] The state may also use private actors to control content so as to bypass due process and democratic values. As such, it is the hybrid regulation (state and private actors acting together), not self-regulation (unchecked censorship by private actors), that needs a public law framework to protect democratic values.

For Ayres and Braithwaite, alternative regulatory strategies should be employed in order to advance the unfruitful debate between strict government regulation and pure market regulation. For them,

> Good policy analysis is not choosing between the free market and government regulation. Nor is it simply deciding what the law should proscribe. If we accept that sound policy analysis is about understanding private regulation - by industry associations, by firms, by peers, and individual consciences - and how it is interdependent with state regulation, then interesting possibilities open up to steer the mix of private and public regulation.[179]

Their proposition is materialised in the concept of 'enforced self-regulation', a hybrid regulatory strategy that blends together features of state-regulation and market self-regulation. This approach places significant responsibility upon individual firms, which are responsible for establishing specific regulatory rules towards their own environment. These rules are then reviewed and approved by the government and are later subject to state sanctions if violated. The concept of enforced self-regulation has thus two important features (*i.e.* 'public enforcement of privately written rules' and 'publicly mandated and publicly monitored private enforcement of those rules'). This strategy tackles the poor compliance commonly found in self-

---

[176] Marsden, C., Tambini, D., and Leonardi, D., *Codifying cyberspace: communications self-regulation in the age of internet convergence* (New York: Routledge, 2007), p 43.

[177] Perritt Jr., H. H., 'Towards a hybrid regulatory scheme for the Internet', *University of Chicago Legal Forum,* (2001), 215-332.

[178] Wu, T., *The Master Switch: The Rise and Fall of Information Empires* (Digital Kindle edn.; London: Atlantic Books, 2010), p 304.

[179] Braithwaite, J. and Ayres, I., *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: OUP, 1992), p 3.

regulatory schemes (*e.g.* ISP non-compliance with Internet industry codes of conduct), because the state will be able to escalate power to sanction when delegated regulation fails. In addition, it tackles the inflexible nature of command-and-control regulation, because private actors have key roles in decisionmaking, monitoring and enforcing processes.[180] Another potential advantage is that public regulators can escalate the enforcement response if the industry fails to self-regulate, so they can start with advisory and persuasive measures and then escalate towards mild administrative sanctions and punitive sanctions at the top to secure compliance.[181]

Generally hybrid regulatory strategies come into existence as more creative, inclusive, flexible and imaginative regulatory responses to problems not properly addressed by traditional forms of regulation and have been largely based on the assumption that '[…] the use of multiple, rather than single policy instruments, and a broad range of regulatory actors, will produce better regulation'.[182] Indeed, regulatory redundancy may be welcome in some circumstances,[183] but this assumption is debatable and hybrid regulation has shortcomings of their own as will be discussed later.

Nevertheless, hybrid strategies are already in place to tackle controversial content available on the Internet in Europe.[184] There has also been increased use of online intermediaries to police online content via legislation that increased their criminal and civil liability in relation to controversial content, and to strengthen their cooperation with law enforcement agencies for surveillance. For Marsden, there has been an increased latitude for private censorship during the 2000s, be it 'aided, abated, funded, and cheer led by governments'.[185]

Hybrid regulation has been enforced by the Chinese government to control problematic material available online. It employs a wide set of techniques ranging from direct governmental intervention to heavy and extensive architecture-based regulation, carried out at different points of control and involving thousands of state agents and private personnel.[186] Similarly, co-regulation and 'after the fact adjudication' have been implemented to resolve infrastructure

---

[180] Ibid , p 116 and 158.

[181] Gunningham, N., 'Enforcement and Compliance Strategies', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2012), 120-45.

[182] Gunningham, N., Grabosky, P., and Darren, S., *Smart Regulations: Designing Environmental Policy* (Oxford: OUP, 1998), p 4.

[183] See Landau, M., 'Rationality, and the Problem of Duplication and Overlap', *Public Administration Review,* 29(4) (1969), 346-58.

[184] Cave, J., Marsden, C., and Simmons, S., 'Options for and Effectiveness of Internet Self- and Co-Regulation. Summary prepared for the European Commission', (Cambridge: RAND Europe, 2008) at <http://www.rand.org/pubs/technical_reports/2008/RAND_TR566.pdf>, accessed 04 June 2010; Marsden, C., Tambini, D., and Leonardi, D., *Codifying cyberspace: communications self-regulation in the age of internet convergence* (New York: Routledge, 2007), p 4.

[185] Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009), p 27 and 105.

[186] Bambauer, D., et al., 'Internet Filtering in China in 2004-2005: A Country Study', *Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2005-10*, 2005) at <http://ssrn.com/paper=706681>; Faris, R., Roberts, H., and Wang, S., 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', *The OpenNet Initiative Bulletin* The OpenNet Initiative, 2009) ; Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006), p 97.

disputes around the US Internet backbone regulation making the government act as a facilitator rather than directly enforcing state-regulation.[187]

Hybrid regulation has been employed for privacy protection of personal data available on the Internet. Self-regulatory instruments have been supplemented by state and multi-state mechanisms in addition to architecture-based regulatory tools (*e.g.* privacy enhanced technologies).[188] The protection of privacy online is enforced via a mix of self-regulation, community persuasion (online activism), terms of service, governmental oversight (*e.g.* pre-authorised contracts by a regulatory agency, domestic and international law) and privacy enhanced technologies (*e.g.* allowing the data migration between different platforms and data expiration).[189]

Moreover, hybrid strategies have been used to stop the publication of other types of controversial content on the Internet (*e.g.* state classified information). The whistleblower organisation Wikileaks has proved its resilience to host and provide access to classified information, particularly the War logs and the US diplomatic cables amidst widespread governmental threats around the world.[190] Wikileaks employed sophisticated computational techniques and hosted their servers in nations with more protective speech laws to preserve the anonymity of informants and evade governmental control. As a result, it has been subject to intense pressure from governments. Julian Assange, editor-in-chief of the Wikileaks, has been fighting in the UK against his extradition not to the US but to Sweden, where he faces criminal charges in relation to an alleged sexual offence.

The battle against Wikileaks following the ‘diplomatic cables’ affair showed how governments are bypassing courts to control the availability of controversial content via online intermediaries. For Benkler, the US government would be defeated in a court challenge against Wikileaks (in relation to the unauthorised release of US confidential diplomatic messages by Wikileaks) on free speech grounds, and instead of going to the US courts, the US government bypassed the US judicial control employing a multi-stakeholder attack against the organisation via online intermediaries (*e.g.* Amazon and online payment systems) by the mere insinuation of illegality.[191] As such, the US government mobilised private resources to regulate online content and achieved a success (*i.e.* Wikileaks stopped its operation because of financial hardship) not likely to occur via US courts.

---

[187] Weiser, P., 'The Future of Internet Regulation', *University of Colorado Law Legal Studies Research Paper No. 09-02,* (2009), p 53.

[188] Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: The MIT Press, 2006).

[189] Edwards, L., 'Anti-social Networking: Inaugural Lecture', (Sheffield: University of Sheffield, 2010) .

[190] See Star, A. (ed.), *Open Secrets: Wikileaks, War, and American Diplomacy (The New York Times)* (Grove Press, 2011); and also Leigh, D. and Harding, L., *WikiLeaks: Inside Julian Assange's War on Secrecy* (London: Guardian Books, 2011).

[191] Benkler, Y., *'Fear of a Networked Fourth Estate',* (2011) (Audio, Radio Berkman #182, 29 April 2011), at <http://blogs.law.harvard.edu/mediaberkman/2011/04/29/radio-berkman-182-was-wikileaks-unprecedented/>, accessed 07 June 2011.

Regulation of copyrights infringement on the Internet is another example of hybrid regulation applied to the online content. In a recent legislative attempt to minimise copyright infringements, enforce intellectual property rights on the Internet, and place policing responsibilities on ISPs, the British Parliament enacted the 2010 Digital Economy Act,[192] a piece of legislation that threatens domestic civil infringers with an escalation of technical measures that include monitoring and notifications by ISPs, slowing down Internet connection, Internet disconnection and blocking of websites by the ISPs.[193]

Similarly, the 2011 e-G8 Meeting in France showed how governments are increasingly forcing Internet companies (*e.g.* Facebook and Google) to follow governments' requests in relation to disclosure of users' data, violation of privacy and illegal filesharing without resorting to judicial control.[194] Legislation has been proposed in the US (*i.e.* the Cyber Intelligence Sharing and Protection Bill - CISPA)[195] to facilitate the sharing of information between private companies and the federal government so as to increase cybersecurity, and similarly the UK coalition government has unveiled plans to increase regulation of online intermediaries by law enforcement authorities.[196] Some online intermediaries (*e.g.* Google) promised to fight any attempt to use website blocking technologies to stop illegal downloading of copyright protected works[197] but the company shows a different approach in relation to alleged child pornographic material given that it employs the IWF blocklist in its search engine available in the UK. Generally, companies are inclined to cooperate and agree to follow censorship demands of governments, because of economic interests and also to avoid the risk of criminal liability.[198] Nevertheless, there is opposition from online intermediaries particularly when regulatory measures may result in extra costs being imposed on them. Three major UK ISPs requested a judicial review in relation to the 2010 Digital Economy Act to avoid such costs.[199] It is estimated that the costs to implement the measures required by the legislation is of around £6 million.[200]

---

[192] Digital Economy Act (c. 24) 2010 (England and Wales).

[193] Edwards, L., 'Law and sausages: How Not to Legislate for the Digital Economy', at <http://blogscript.blogspot.com/>, accessed 03 May 2010.

[194] Wintour, P., 'David Cameron to resist French plan for internet regulation: Nicolas Sarkozy calls for worldwide web controls at G8 summit, but Google chairman urges leaders to resist legislation', *The Guardian,* 24 May 2011 at <http://www.guardian.co.uk/technology/2011/may/24/david-cameron-resist-internet-regulation>, accessed 07 June 2011.

[195] 'Cispa cybersecurity bill passed by House of Representatives', *The Guardian,* 27 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/27/cispa-cybersecurity-bill-passed-senate>, accessed 01 May 2012.

[196] Booth, R., 'Government plans increased email and social network surveillance', Ibid01 April, sec. World News at <http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance>.

[197] Halliday, J., 'Google faces pressure to block filesharing sites', Ibid13 September 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/sep/13/google-block-filesharing-sites>, accessed 28 December 2011; also Halliday, J., 'Google boss: anti-piracy laws would be disaster for free speech', *The Guardian,* 18 May 2011 at <http://www.guardian.co.uk/technology/2011/may/18/google-eric-schmidt-piracy>, accessed 07 June 2011.

[198] See McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 273.

[199] Halliday, J., 'BT and TalkTalk denied Digital Economy Act appeal', *The Guardian,* 12 June 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jun/21/bt-talk-talk-digital-economy-act>, accessed 21 June 2011.

[200] Halliday, J., 'Digital Economy Act will cost nearly £6m', *The Guardian,* 17 June 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jun/17/digital-economy-act-cost>, accessed 20 June 2011.

Another feature of the hybrid regulatory strategies is the extensive use of architecture-based regulatory tools by both state and private actors to control material available on the Internet as well as increased surveillance and monitoring capabilities of law enforcement authorities.

The self-regulation school argues that governments are unable to regulate cyberspace, because of the alleged non-regulable architecture of the Internet. Nevertheless, this architecture is not derived from Nature. On the contrary, it was built according to political and technical choices available at a particular historical context. As such, this architecture (meaning the Internet's infrastructure, technical standards and protocols) can be modified so as to produce a more regulable environment; an environment more responsive to regulation. For Lessig:

> Whether cyberspace can be regulated depends upon its architecture […] The original architecture of the Internet made regulation extremely difficult. But that original architecture can change. And there is all the evidence in the world that it is changing. Indeed, under the architecture that I believe will emerge, cyberspace will be the most regulable space humans have ever known.[201]

For Lessig, the hardware and software that build the Internet are the code or the 'law of cyberspace' and it is one modality of regulation that can enforce its control directly over online content.[202] The architecture-based regulatory tools have different forms and enforcement features. For Yeung, they can be classified under different criteria whether it encourages behavioural change, changes the impact of the harm generating behaviour or prevents the harm generating behaviour.[203] Similarly, Brownsword stresses that these tools may be enforced *ex ante*, during the action, or *ex post*.[204] Filtering can be implemented at different points of the network (*e.g.* at the ISP-, user- and backbone levels). These architecture-based regulatory tools have been associated with self-regulatory strategies[205] but they can be designed and employed by both state and non-state actors under voluntary or mandatory schemes.

Online filtering is an example of an architecture-based regulatory tool to control access to online material. Generally a filtering system allows the free flow of uncensored material but blocks the censored content via different techniques (*e.g.* blacklisting, whitelisting or content analysis).[206] Notably, they have been largely implemented on the Internet. For example, Faris and Villeneuve reported in 2008 that online content filtering systems were active in 26 countries targeting different categories of content related to politics and power; social norms and morals; and security concerns. In addition, they reported that filtering has been implemented by non-

---

[201] Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 32.

[202] Ibid , p 110.

[203] Yeung, K., 'Towards an Understanding of Regulation by Design', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008).

[204] Brownsword, R., 'Neither East Nor West: Is Mid-West Best?', *SCRIPT-ed,* 15(3:1) (2006), p 21.

[205] See for example the ethically based self-regulatory model (*i.e.* involving self-regulation backed by code and ethical principles) proposed by Spinello, R., *Regulating cyberspace: the policies and technologies of control* (Westport, Conn.: Quorum Books, 2002).

[206] Klang, M., 'Controlling Online Information: Censorship and Cultural Protection', *The World Summit on the Information Society: A Summit of Solutions?* (Uppsala, Sweden and Kampala, Uganda: Collegium for Development Studies, 2005), 43-50 , p 44-5.

state and state actors either domestically or internationally.[207] Similarly, Zittrain and Palfrey argue that the Internet has been increasingly 'balkanised' by governmental and private filtering mechanisms making the alleged unregulated nature of the Internet far from reality.[208] Deibert and Rohozinski stressed that concerns over cybersecurity and censorship are leading to the militarisation of the Internet where the exercise of power over content is being enforced via more pervasive ways.[209] These architectures of content control are increasingly taking the place of traditional law enforcement goals such as removing controversial content at its source and building online walls to protect from overseas controversial content.[210]

Website blocking has also been employed to tackle copyrights infringement on the Internet whether via self-regulation, legislation or court orders. For example, Mr. Judge Arnold has recently ordered British Telecom to block access to an alleged copyrights infringement website under the s. 97A (injunctions against service providers) of the 1988 CDPA,[211] which confirmed the legality and actual use of website blocking in relation to copyrights infringement.[212] This measure has also been implemented via legislation, *e.g.* Section 10 of the 2010 DEA[213] which established that the Secretary of State may order ISPs to limit Internet access in order to tackle the problem of online copyright infringement.[214] Yet, Edwards argues that website blocking has only limited effect and may be disproportionate, resulting in displacement of filesharing to other platforms, increased costs to online intermediaries, private censorship and other unintended consequences.[215]

Other examples of architecture-based regulatory tools are tethered appliances and surveillance equipment. Tethered appliances facilitate the enforcement of content regulation at the user-level, because their internal configuration may be prompted from afar, they are subject to instantaneous revision and they make surveillance extremely easy to perform.[216] For Zittrain:

---

[207] Faris, R. and Villeneuve, N., 'Measuring Global Internet Filtering', in Ronald Deibert, et al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), 5-28.

[208] Zittrain, J., 'Internet Filtering: The Politics and Mechanisms of Control', Ibid, 29-56.

[209] Deibert, R. and Rohozinski, R., 'Beyond Denial: Introducing Next Generation Information Access Controls', in Ronald J. Deibert, et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010), 3-13.

[210] Edwards, L., Rauhofer, J., and Yar, M., 'Recent developments in UK cybercrime law', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 413-36, p 420.

[211] Copyright, Design and Patents Act 1988 (England and Wales).

[212] *Twentieth Century Fox et al v BT [2011] EWHC 1981* (Ch).

[213] Digital Economy Act (c. 24) 2010 (England and Wales).

[214] The UK ISPs BT and TalkTalk have lost their legal challenge against the 2010 DEA in March 2012. See Halliday, J., 'BT and TalkTalk lose challenge against Digital Economy Act', *The Guardian,* 06 March 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/mar/06/internet-provider-lose-challenge-digital-economy-act>, accessed 22 March 2012.

[215] See Edwards, L., 'Newzbin 2: Landmark or Laughing Stock?', *Pangloss* (2011) at <http://blogscript.blogspot.com/2011/07/newzbin-2-landmark-or-laughing-stock.html> Accessed 28 December 2011; and also Kaye, L., 'Blocking Newzbin2 paves the way for internet censorship', *The Guardian,* 29 July 2011, sec. Liberty Central at <http://www.guardian.co.uk/commentisfree/libertycentral/2011/jul/29/newzbin2-internet-censorship-bt>, accessed 28 December 2011.

[216] Zittrain, J., 'Perfect Enforcement on Tomorrow's Internet', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008), p 132.

> Tethered appliances belong to a new class of technology. They are appliances in that they are easy to use, while not easy to tinker with. They are tethered because it is easy for their vendors to change them from afar, long after the devices have left warehouses and showrooms.[217]

The iPhone and iPad are examples of closed technologies where the user has less control over the equipment, its functionalities, and the type of content it can access.[218] Similarly, Amazon.com was subject to intense criticism over the changes it made remotely to a digital book already purchased by its customers via the Kindle service.[219]

The usage of mobile phones has increased over the years and it is becoming the way most people access the Internet. This means that online content may be easier to regulate in the future via these devices and mobile networks.[220] For example, all mobile operators in the UK already employ the controversial IWF blocklist within their networks to limit access to online child pornography; this means 100% coverage in relation to Internet access made via 3G and some wi-fi providers.[221] In addition, the growing usage of smartphones, tablets and 'pre-approved apps' to access and use of the Internet makes evident the diminished role that the world wide web plays at the moment.[222]

Such devices are used not only to limit access to controversial online material but for surveillance. The spacial location of mobile phones are recorded by network operators for the operation of the system and this information is usually only obtained via court orders in special cases such as criminal investigation, but there is no guarantee that this information is kept confidential. For example, it has been found that the iPhone was recording spatial data without any level of encryption.[223] In addition, these devices can be used by law enforcement agencies in cooperation with mobile operators to investigate alleged offenders by activating the microphone and camera of the device without the knowledge of its owner. It is also the case that increased investigatory powers given to law enforcement agencies has lead not only to a

---

[217] Zittrain, J., *The future of the internet - and how to stop it* (New Haven, CT: Yale University Press, 2009), p 106.

[218] Arthur, C., 'I want the iPad porn-free, says Apple's Steve Jobs: Apps for the new iPad have had to self-censor ', *The Guardian,* Tuesday 25 May 2010 2010 ; Zittrain, J., 'A fight over freedom at Apple's core', *Financial Times,* 03 February 2010 2010 at <http://www.ft.com/cms/s/2/fcabc720-10fb-11df-9a9e-00144feab49a.html?nclick_check=1>, accessed 14 December 2011; Dredge, S., 'Apple bans satirical iPhone game Phone Story from its App Store', *The Guardian,* 2011, sec. Apps Blog at <http://www.guardian.co.uk/technology/appsblog/2011/sep/14/apple-phone-story-rejection>, accessed 28 December 2011.

[219] Stone, B., 'Amazon Erases Orwell Books From Kindle', *The New York Times,* 2009, sec. Technology at <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?adxnnl=1&adxnnlx=1325158251-ts7AYblRq6cBBmaPrJP1SQ>, accessed 29 December 2011.

[220] See Zittrain, J., 'The Personal Computer Is Dead', *The Future of the Internet and How to Stop It* (2011) at <http://futureoftheinternet.org/blog> Accessed 29 December 2011; Naughton, J., 'Smartphones can do everything – except safeguard the web', *The Guardian,* 17 July 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jul/17/smartphones-internet-corporate-threat>, accessed 28 December 2011.

[221] Carr, J., 'BlackBerry has some explaining to do', *Desiderata* (2011) at <https://johnc1912.wordpress.com/2011/12/09/blackberry-has-some-explaining-to-do/> Accessed 28 December 2011.

[222] Guadamuz, A., *Networks, Complexity and Internet Regulation: Scale-Free Law* (Cheltenham, UK: Edward Elgar, 2011), p 209.

[223] See Arthur, C., 'iPhone keeps record of everywhere you go', *Guardian News and Media Limited,* 20 April 2011 at <http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears>, accessed 21 April 2011; See also Warden, P., 'iPhone Tracker', at <http://petewarden.github.com/iPhoneTracker/>, accessed 21 April 2011.

growing cooperation between them and online intermediaries but also to increased use of monitoring equipment to detect alleged offenders, collect criminal evidence and take-down controversial online content. For example, it has been alleged that during the 2011 London riots, the Metropolitan Police used equipment able to shut off mobile phones remotely and track movements from individual phones.[224] Although these measures may be allowed under RIPA 2000,[225] it raises a number of issues in relation to proportionality and fairness.

Governments around the world are investing massively in more invasive surveillance equipment and strategies to cope with perceived threats (for example, terrorism, child pornography, political dissent etc.) associated with the Internet and digital technologies. See for example the surveillance project developed by the US National Security Agency, a massive datacenter to intercept, store and analyse online communications from around the world,[226] and also the current attempt of British government to expand existing surveillance powers of law enforcement authorities.[227] Other more extreme examples include governments cutting off the Internet entirely.[228]

4 The negative consequences of hybrid regulation

The cyberlibertarian self-governing rhetoric in relation to online content regulation did not materialise. On the contrary, censorship of online content by both state and private actors is increasing in either democratic or authoritarian states across the world.[229] After new technological developments expanded the 'geometries of social interaction' and produced a number of 'perceived' harms in relation to the Internet, governments responded with increased control that may be creating additional harms instead of maximising the positive benefits.[230] The question at the moment is no longer whether the Internet can or should be regulated but how civil liberties are to be protected in an increasingly regulated Internet.[231]

The delegation of regulatory powers from the state to private actors, the increased legal liability of online intermediaries, the more investigatory powers given to law enforcement agencies, and the extensive use of architecture-based regulatory tools make evident the regulatory escalation,

---

[224] Gallagher, R. and Syal, R., 'Met police using surveillance system to monitor mobile phones', *The Guardian,* 30 October 2011, sec. UK News at <http://www.guardian.co.uk/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance>, accessed 28 December 2011.

[225] Regulation of Investigatory Powers Act (c.23) 2000 (England and Wales).

[226] Bamford, J., 'The Black Box', *Wired Magazine*, April (2012) at <http://www.wired.com> accessed 03 April 2012.

[227] Syal, R., Halliday, J., and Siddique, H., 'Theresa May defends email surveillance plans', *The Gardian,* 04 April 2012, sec. UK Police at <http://www.guardian.co.uk/uk/2012/apr/03/theresa-may-email-surveillance-plans>, accessed 04 April 2012.

[228] Williams, C., 'How Egypt shut down the internet', *The Telegraph,* 28 January 2011, sec. World News at <http://www.telegraph.co.uk/news/worldnews/africanandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html>, accessed 04 April 2012.

[229] Bambauer, D., 'Cybersieves', *Duke Law Journal,* 59(3) (2009), 377-446, p 445.

[230] McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 241.

[231] And hence the importance of this investigation. See for example Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006); Bambauer, D., 'Filtering in Oz: Australia's Foray into Internet Censorship', *Brooklyn Law School, Legal Studies Paper No. 125,* (2008); and Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009).

the potential for the violation of free speech and privacy protection, and the conflicts between private and public interests involving children protection, human rights protection and free speech associated with implementing such regulatory responses.

Examples of hybrid regulatory strategies in relation to online content were addressed above. This section will explore a number of negative consequences of hybrid regulation for free speech, privacy protection and democracy on the Internet found in the literature.

4.1 Unchecked private censorship, scope creep and lack of focus

One of the problems related to hybrid regulation of online content by private actors is the potential for unchecked private censorship.[232] For example, the UK self-regulatory body IWF manages a website blocklist that targets alleged child pornography since 2004, but this strategy raised concerns about private censorship particularly after the Wikipedia incident in December 2008, which showed the problematic adjudication of apparent illegality of online criminal content by private actors.[233] For Edwards, given the powers it '[…] possesses to exclude any kind of online content from the UK […],' the remit of the IWF should be reviewed to minimise the risk of unchecked private censorship.[234] McGuire also stresses that IWF's operation is a matter of concern because of the powers it has,[235] and Yar has also argued that the IWF has acted as police, judge and jury bypassing due process of law and unilaterally censoring online content.[236]

In a similar vein, Kreimer argues that regulation of online content by private actors is prone to scope creep, *i.e.* after regulatory schemes are implemented to block child pornography other controversial material can follow suit.[237] This situation has led some to argue that online blocking schemes should be established by legislation, not self-regulation, because this allegedly brings more transparency and minimise opaque censorship of private actors.[238]

Indeed, increased legal liability placed on online intermediaries and the ability of law enforcement agencies to implement online surveillance without judicial oversight have forced online intermediaries to implement regulatory measures of their own to avoid the risk of legal liability beyond what is usually required.[239] Online intermediaries have more incentives to

---

[232] De Hert, P. and Raab, C., 'Tools for Technology Regulation: Seeking Analytical Approaches', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008), p 274.

[233] See Chapter 7 about online child pornography regulation in the United Kingdom.

[234] Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 655 and 657.

[235] McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 281.

[236] Yar, M., 'The private policing of Internet crime', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 546-61, p 548-9.

[237] Kreimer, S. F., 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', *University of Pennsylvania Law Review,* 155(11) (2006), p 28.

[238] Edwards, L., Rauhofer, J., and Yar, M., 'Recent developments in UK cybercrime law', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 413-36, p 421.

[239] For a discussion of these issues see Newey, A., 'Freedom of expression: censorship in private hands', in Liberty (ed.), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (London: Pluto Press, 1999).

zealously accept government demands and avoid the risk of legal liability rather than protecting civil liberties online.

For Marsden, the 'safe harbour' principle created incentives to censor the reported content expeditiously without further scrutiny by the courts, because 'immediate compliance is self-serving, cheaper and easier' and 'ISPs will take the path of less resistance'.[240] Similarly, the threat of criminal prosecution in relation to alleged child pornography has forced major online intermediaries in Brazil to develop strategies of their own (for example automated filtering of child pornographic images via file hashing, human content analysis, and recording of users' log). None of these measures was established via legislation but implemented by private actors without any safeguard against potential abuse.[241]

Many Internet companies are prone to accept without discussion the censorship demands of their hosting states in order to operate there.[242] Zittrain and Palfrey report that many multinational Internet companies must comply with restrictions imposed by the countries where they operate and in so doing they commonly violate legal and ethical frameworks of their home state.[243] This has lead to calls for an international protective framework around online intermediaries and hardware manufacturers so they are not forced to comply with censorship demands nor do they provide censorship-related hardware, software and services to authoritarian regimes.[244]

Although, systems of notices and take down (NTD) in relation to controversial online content are prone to abuse. For example, Ahlert *et al.* assessed NTD procedures in regard to copyrights infringement in 2004 and showed that they were abused in the United Kingdom. They uploaded material already in the public domain in British online hosts and made a complaint to the relevant online intermediary about alleged copyright infringements. Generally, British ISPs took the perfectly legal content down 'almost immediately'[245] which seems to suggest that safeguards are needed to improve transparency and accountability of the UK NTD scheme for protection of copyrighted material.

---

[240] Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009), p 115 and 117.

[241] See Chapter 4 about online child pornography regulation in Brazil.

[242] Branigan, T., 'Facebook may 'block content' claim as speculation grows over entry into China', *Guardian News and Media Limited,* 20 April 2011 at <http://www.guardian.co.uk/technology/2011/apr/20/facebook-considers-censorship-claim-china>, accessed 21 April 2011. See also the Yahoo!'s compromise to China in Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006).

[243] Zittrain, J. and Palfrey, J., 'Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet', in Ronald Deibert, et al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), 103-22.

[244] See Zuckerman, E., 'Intermediary censorship', in Ronald J. Deibert, et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010); and also Noman, H. and York, J., 'West Censoring East: The Use of Western Technologies by Middle East Censors 2010-2011', (Toronto, Otawa and Stanford: Opennet Initiative, 2011) .

[245] Ahlert, C., Marsden, C., and Yung, C., 'How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation', (Oxford: Oxford Institute, 2004) at <http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf>, accessed 01 July 2010.

The NTD regime is an example of a 'fire-alarm' type of oversight, *i.e.* it is a less centralised, active and direct form of oversight that involves a number of procedures to encourage individual citizens to participate via a reporting mechanism. Nevertheless, this approach has been giving way to a 'police patrol' type of oversight, *i.e.* more centralised, active and direct mechanisms of content monitoring via online blocking, automated filtering and deep packet inspection technologies.[246] This change occurred not only in relation to child pornographic content but copyrights infringement and increase the chances of unchecked private censorship of online content.[247]

Another regulatory tool that facilitates unchecked private censorship is the implementation of online blocking schemes. They have been largely criticised for its potential for scope creep, lack of focus and limited effectiveness. They are only partially effective because often target websites, but there are a number of other Internet platforms and applications which are used to distribute child pornography (*e.g.* anonymised channels, P2P networks, email, and encrypted platforms). The website blocked can also have its domain name altered and move jurisdictions easily and rapidly, which renders the blocklist quickly outdated. Online blocking schemes are also prone to circumvention.[248] For example, Clayton pointed out in 2005 the possibility of circumventing the IWF blocklist of alleged child pornography URLs and also of determining what has been blocked, which could have been used by distributors of online child pornography to realise that they have been discovered.[249]

Stol *et. al* criticise the use of website blocking of alleged child pornographic content in the Netherlands and argue that it is not only ineffective but unlawful.[250] Similarly, McIntyre criticises the use of blocking systems within Europe because of their lack of legislative basis (violation of Article 10 of the EU Convention on Human Rights - ECHR[251]) and procedural safeguards (*i.e.* they are opaque and unaccountable).[252] Akdeniz also suggests that the operation of online blocking across Europe is likely to violate Article 10 of the ECHR.[253] Blocklists can

---

[246] See generally McCubbins, M. and Schwartz, T., 'Oversight Overlooked: Police Patrols versus Fire Alarms', *American Journal of Political Science,* 28(1) (1984), 165-79.

[247] See Edwards, L., 'Role and Responsibility of Internet Intermediaires in the Field of Copyright and Related Rights', (Geneve: WIPO, 2011) at <http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf>, accessed 28 December 2011.

[248] See generally EDRI, 'Internet Blocking Booklet', (Brussels: European Digital Rights, 2010) at <http://www.edri.org/files/blocking_booklet.pdf>, accessed 04 June 2010; Brown, I., 'Internet Censorship - Be Careful What You Ask for', in S. Kirca and L. Hanson (eds.), *Freedom and Prejudice: Approaches to Media and Culture* (Istanbul: Bahcesehir University Press, 2007); Callanan, C., et al., 'Internet blocking: balancing cybercrime responses in democratic societies', (Dublin: Open Society Institute, 2009) at <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf>, accessed 29 December 2011.

[249] Clayton, R., 'Failures in a Hybrid Content Blocking System', *Workshop on Privacy Enhancing Technologies* (Dubrovnik, Croatia, 2005) at <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf> Accessed 05 July 2010.

[250] Interestingly, they argue that the blocking system violates Article 8 (privacy), not Article 10 (freedom of expression), of the European Convention on Human Rights (ECHR). See Stol, W., et al., 'Governmental filtering of websites: The Dutch case', *Computer Law & Security Review,* 25 (2009), 251-62.

[251] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14. 1950 (04 Nov 1950) (Rome).

[252] McIntyre, T., 'Blocking child pornography on the Internet: European Union developments', *International Review of Law, Computers and Technology,* 24(3) (2010), 209-21.

[253] See Akdeniz, Y., 'To block or not to block: European approaches to content regulation, and implications for freedom of expression', *Computer Law & Security Review,* 26 (2010), 260-72, p 260.

also leak.[254] As a result, people can have access to compiled lists of child pornography websites hosted abroad and the relevant content provider may delete evidence after they find that their illegal website has been blocked, undermining future evidence collection by police forces. There are also fears that after blocking schemes are implemented, they are susceptible to scope creep.[255]

4.2 Lack of transparency, accountability, legitimacy, proper oversight and citizen involvement

Another problem of decentred and polycentric regulatory regimes is their lack of transparency, accountability, and legitimacy. When regulatory powers are transferred to private actors, there is the risk of opaque and unaccountable indirect content regulation.

For Lessig, indirect content regulation puts governments in a comfortable position because the political and technical burden of content regulation is transferred to private actors.

> Here the government is regulating indirectly by using the structures of real-space code to effect its ends, but this regulation, again, is not seen as regulation. Here the government gets an effect at no political cost. It gets the benefit of what would be an illegal and controversial regulation without even having to admit any regulation exists.[256]

> Indirection misdirects responsibility. When a government uses other structures of constraint to effect a constraint it could impose directly, it muddles the responsibility for that constraint and so undermines political accountability. If transparency is a value in constitutional government, indirection is the enemy. It confuses responsibility and hence confuses politics.[257]

For Lessig, '[…] we should worry about a regime that makes invisible regulation easier […]'[258] and therefore improve governmental oversight over content regulation performed by private actors. Similarly, Kreimer argues that regulation of online content by private actors is generally excessive, illegitimate and unaccountable; without adequate channels to correct distortions; without due process of law or judicial oversight; without guarantee of proportionality and not subject to review.[259]

Not only the lack of accountability of current regulatory policies has been a cause of concern, but poor citizen involvement in formulating and operating such measures is another issue that causes concern to policymakers. Generally, these policies are designed and implemented

---

[254] See Collin, J., 'Leaked Government blacklist confirms worst fears' *Electronic Frontiers Australia*; <http://www.efa.org.au/2009/03/19/leaked-government-blacklist-confirms-worst-fears/> accessed 09 August 2010.

[255] Bambauer, D., 'The Widening Gyre', *Information, Law, and the Law of Information* (2011) at <http://blogs.law.harvard.edu/infolaw/2011/06/20/the-widening-gyre/> Accessed 29 December 2011.

[256] Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 135.

[257] Ibid , p 133.

[258] Ibid , p 136.

[259] Kreimer, S. F., 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', *University of Pennsylvania Law Review,* 155(11) (2006), p 28.

without adequate input from civil rights and consumers' organised groups, and the public at large.

4.3 Difficulties in evaluation of hybrid regulation

Assessing how successful a policy has been in tackling online child pornography is also problematic, because evidence about the production, distribution and access to such content is difficult to obtain,[260] which makes any attempt to assess the effectiveness of regulatory intervention heavily problematic. Some indications can be obtained from international police operations, domestic criminal prosecution and from convicted offenders but such available evidence is too small in size to be representative, and online child pornography can be produced and assessed via a number of channels that remain unmonitored.

In addition, the concept of 'success' has to be constructed to mean not only less child pornographic material being produced and distributed, but also that fewer children are being abused, that investigation and surveillance are undertaken with due process and proper privacy protection, and that there are sufficient safeguards in place to protect free speech and secure that such policies are accountable, legitimate and transparent.

4.4 Crime displacement and unchecked investigatory powers

Regulatory interventions in decentred and polycentric regulatory environments may lead to unintended results because the actors involved are not only reactive but active; the behaviour of a single actor affects the others in unexpected ways.[261] The resilience and self-organising features of the Internet challenge regulatory intervention applied to controversial online material.[262] For example, the anonymised access via P2P networks and the availability of non-indexed online repositories make possible the displacement of online content related crimes to more resilient non-web environments.

Another implication of hybrid regulation is the unchecked investigatory powers given to law enforcement agencies in order to identify alleged offenders and collect criminal evidence, which may undermine civil liberties on the Internet, if there are no safeguards in place. For Grabosky, the protection of individual freedom has been undermined to increase the perceived security of the online environment.[263] As a result, a balance has to be struck between the right of privacy and the need of police surveillance to tackle online crime so as to avoid unchecked and

---

[260] Jenkins, P., 'Failure to launch: Why do some social issues fail to detonate moral panics?', *British Journal of Criminology,* 49 (2009), 35-47, p 38.

[261] Murray, A., *The regulation of cyberspace: control in the online environment* (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006), p 51-3.

[262] See Guadamuz, A., *Networks, Complexity and Internet Regulation: Scale-Free Law* (Cheltenham, UK: Edward Elgar, 2011).

[263] Grabosky, P., 'Security in the 21st Century', *Security Journal,* 20 (2007), 9-11.

excessive powers being assigned to law enforcement agencies under a cybercrime 'moral panic'.[264]

4.5 Excessive use of architecture-based regulatory tools

Another negative consequence of hybrid regulation of online content is the excessive use of architecture-based regulatory tools that raises not only fears of free speech violation but also a number of ethical issues. For example, Brownsword rejects utilitarianism as the prominent ethic to govern the way regulators control technology.[265] Similarly, Baldwin and Cave argue that questions involving rights and justice should not be answered only in terms of an utilitarian rationale,[266] and Sunstein argues that technological regulation that excludes the possibility of doing wrong may impede individuals from realising that they face a choice between right and wrong and therefore this denies them some practice of moral agency.[267] In a similar vein, Brownsword states that

> The most precious thing that an aspirant moral community can hand on to the next generation is an environment that is conducive to a moral way of life that hinges on agents trying to do the right thing, trying to respect the legitimate interests of fellow agents, and being held responsible for their actions.[268]

Indeed, architecture-base regulatory tools are criticised on different grounds. It has been argued elsewhere that they are prone to circumvention; technical failure by being either too narrow or too broad (false positive and false negative); it is developed in the shadow of public interest and legal rules; it overemphasises private interests; it is automatic and self-enforcing; and it may rob users of moral agency.[269] For McGuire, architecture based regulatory tools may be useful for legitimate policing but it is often used for no clear purpose.[270] This becomes more problematic because not only governments but private actors have policing functions in relation to online material.

4.6 Minimising the negative consequences of hybrid regulation: safeguards

---

[264] Thomas, D. and Loader, B., 'Introduction - Cybercrime: law enforcement, secutiry, and surveillance in the information age', in Douglas Thomas and Brian Loader (eds.), *Cybercrime: law enforcement, secutiry, and surveillance in the information age* (London: Routledge, 2000), 1-13, p 8.

[265] Brownsword, R., *Rights, regulation, and the technological revolution* (Oxford: OUP, 2008), p 77.

[266] Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999), p 77.

[267] Sunstein, C., *Republic.com* (Princeton and Oxford: Princeton University Press, 2001).

[268] Brownsword, R., *Rights, regulation, and the technological revolution* (Oxford: OUP, 2008), p 45; See also Brownsword, R., 'Neither East Nor West: Is Mid-West Best?', *SCRIPT-ed,* 15(3:1) (2006), p 21.

[269] Scott, C. and McIntyre, T., 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008), p 110-12; Roberts, H., Zuckerman, E., and Palfrey, J., '2007 Circumvention Landscape Report: Methods, Uses, and Tools', The Berkman Center for Internet & Society at Harvard University, 2009) at <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2007_Circumvention_Landscape.pdf>, accessed 04 June 2010; Yeung, K., 'Towards an Understanding of Regulation by Design', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008).

[270] McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 275.

The academic literature addressed so far indicates that there are a number of negative consequences of hybrid regulation. Nevertheless, the literature has also made a number of suggestions to minimise such negative consequences.

For example, Loader proposes basic principles to bring this dispersed network under democratic control which include individual and social groups involvement, human rights, and politics of allocation of police resources.[271] Similarly, building 'publicness' of the new configuration of public service providers via transparency mechanisms (for example increasing the quality of information, representation, choice and voice) and accountability channels in this fluid regulatory environment have also been proposed elsewhere.[272]

For Black, the regulatory responses in decentred regulatory environments should provide systems of extended accountability, enhanced democratic governance, and increased judicial review and parliamentary agency.[273] Similarly, the threat of uncontrolled private censorship of the online content has lead to calls for a more protective regulatory framework.[274] For Nunziato, free speech laws in the US have been more lenient in relation to online intermediaries (*i.e.* 'free speech conduits' engaged in transportation, communication and other public services related to online content) when compared to traditional conduits of content (*e.g.* newspaper and magazines) and this resulted in much of the operations of online intermediaries going unchecked by both the US government and courts. Nevertheless, he argues that such private actors should be considered as public organisations under free speech laws and be subject to closer governmental scrutiny and judicial oversight to minimise the risk of uncontrolled online content censorship.[275] Similarly, Stalla-Bourdillon argues that the increasingly regulatory powers of private actors on the Internet should be limited by a legal framework designed to enforce public principles.[276] Wu makes a similar point arguing that information industries 'can never be properly understood as normal industries' and 'perform a vital public function'. Therefore they should be subject to something more than just US antitrust laws, whose focus is on economic issues and neglects basic civil liberties' protection.[277]

---

[271] Loader, I., 'Plural Policing and Democratic Governance', *Social & Legal Studies,* 9(3) (2000), 323-45, p 326.

[272] Stirton, L. and Lodge, M., 'Transparency Mechanisms: Building Publicness into Public Services', *Journal of Law and Society,* 28(4) (2001), 471-89; and also Lodge, M. and Stirton, L., 'Accountability in the Regulatory State', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2010), 349-70.

[273] Black, J., 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Law Society Economy Legal Studies Working Paper No. 2/2008* (London: London School of Economics and Political Science, Law Department, 2008) at <http://www.lse.ac.uk/collections/law/>, accessed 03 April 2012, p 284.

[274] See Stalla-Bourdillon, S., 'Chilling ISPs... when private regulators act without adequate public framework...', *Computer Law & Security Review,* 26 (2010), 290-7; and also Perritt Jr., H. H., 'Towards a hybrid regulatory scheme for the Internet', *University of Chicago Legal Forum,* (2001), 215-332.

[275] See Nunziato, D., *Virtual freedom: net neutrality and free speech in the Internet age* (Stanford: Stanford University Press, 2009).

[276] Stalla-Bourdillon, S., 'Chilling ISPs... when private regulators act without adequate public framework...', *Computer Law & Security Review,* 26 (2010), 290-7.

[277] Wu, T., *The Master Switch: The Rise and Fall of Information Empires* (Digital Kindle edn.; London: Atlantic Books, 2010), p 304.

Laidlaw employs a similar argument in relation to search engines like Google arguing that it should be subject to more public oversight because of the public function they undertake as information gatekeepers.[278] There are not only financial concerns involved here (for example, placing sponsored companies at the top of the searches) but search engines have also been targeted by regulators (for example, employing content filtering of politically sensitive material and blocklists of websites allegedly hosting child pornography) without appropriate transparency and accountability channels. Moreover, there have been recommendations for user-generated content platforms to mitigate the negative effects of content removal and account deactivation taking into account human rights considerations.[279]

Others have called for an impact assessment of online content filtering schemes to identify and minimise abuses. For example, Edwards suggests a speech impact assessment based on five criteria, including: purpose of the scheme and audience restricted; judges; effectiveness; resources; and alternatives to inhibit the growth of unchecked censorship on the Internet.[280] Similarly, Bambauer presents a framework to assess the legitimacy of online filtering based on their openness, transparency, narrowness, and accountability in order to identify how regulators describe what they censor and why; whether they effectively block proscribed material and allow others; and the level of citizen involvement and participation.[281]

> To assess legitimacy, the framework asks four questions. First, is a country open about its Internet censorship, and why it restricts information? Second, is the state transparent about what material it filters and what it leaves untouched? Third, how narrow is filtering: how well does the content that is actually blocked - and not blocked - correspond to those criteria? Finally, to what degree are citizens and Internet users able to participate in decisionmaking about these restrictions, such that censors are accountable? Legitimate censorship is open; transparent about what is banned; effective, yet narrowly targeted; and responsive to the preferences of each state's citizens.[282]

Often private actors lack the democratic legitimacy to perform a public function of assessing and limiting access to controversial online content. This legitimacy derives in part from citizen involvement. There are different levels of citizen participation in designing and monitoring the operation of online content regulatory policies.[283] For Klang, the regulation of technology should be subjected to legitimate oversight by the public at large.[284] This may have been the

---

[278] Laidlaw, E., 'Private Power, Public Interest: An Examination of Search Engine Accountability', *International Journal of Law and Information Technology,* 17(1) (2008), 113-45.

[279] Newland, E., et al., 'Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users', (Cambridge, MA: The Berkman Center for Internet & Society and The Center for Democracy & Technology, 2011) at <http://cyber.law.harvard.edu/node/7080>, accessed 28 December 2011.

[280] See Edwards, L., 'The Internet is for Porn? Content Filtering and the New Censorship', (2009); and also Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 666.

[281] See Bambauer, D., 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering', *ExpressO,* at http://works.bepress.com/derek_bambauer/25 (2008); and also Bambauer, D., 'Cybersieves', *Duke Law Journal,* 59(3) (2009), 377-446.

[282] Bambauer, D., 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering', *ExpressO,* at http://works.bepress.com/derek_bambauer/25 (2008), p 7.

[283] See Bambauer, D., 'Cybersieves', *Duke Law Journal,* 59(3) (2009), 377-446, p 379.

[284] Klang, M., 'Disruptive Technology: effects of technology regulation on democracy', (Göteborg University, 2006), p 44.

case of the 2010 *Marco Civil* Bill in Brazil,[285] which aims to establish the general framework of a NTD regime and there has been substantial citizen involvement during its formulation. Nevertheless, there are no guarantees that these inputs will be kept during parliamentary debate expected to occur in the late 2012.

For Lessig, the regulation of online content via architecture-based tools, be it implemented by state or non-state actors, should be limited to the strictly necessary so regulators can achieve their aims with precision.[286] Indeed, architecture-based regulation of content should be crafted and implemented carefully to meet democratic controls and the rule of law.[287]

Bardach also argues that remedies to implementation problems should be taken into account in advance, in the policy-design and adoption stage, to overcome the perils of the 'implementation game', as a game of putting the administrative machine together to enforce the law and, of managing the different actors and institutions involved via persuasion and bargaining to achieve the regulatory aims pursued.[288]

In sum, regulation of controversial online content is heavily problematic and led to a range of hybrid regulatory strategies involving both state and private actors. These strategies may have a number of negative consequences to society and suggestions have been made to tackle them in order to achieve a balance between the conflictual interests at stake such as privacy protection vs accountability of users; children-friendliness of technology vs children protection; security vs creativity; and private vs public interests.[289] The next section will develop evaluative criteria to assess these negative consequences in the fieldwork in order to evaluate them in practice. This is important not only to adjust current policymaking but also to guide future initiatives.

5 Evaluative criteria to assess the negative consequences of hybrid regulation

This chapter has showed so far that regulation of controversial material available on the Internet is problematic and has been a concern for regulatory and governance scholarship.

First, regulation has been defined as a social phenomenon involving all forms of social control (whether intentionally or not) by different social actors in order to restrict or facilitate

---

[285] Marco Civil da Internet (2010). at <http://culturadigital.br/marcocivil/>, accessed 26 April 2011.

[286] Lessig, L., 'What Things Regulate Speech: CDA 2.0 vs. Filtering', *Jurimetrics,* 38 (Summer 1998 1998), 629-70, p 20-1; See also Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 120.

[287] Koops, B.-J., 'Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008), p 160; Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69; Scott, C. and McIntyre, T., 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008), p 111-12; Bambauer, D., 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering', *ExpressO,* at http://works.bepress.com/derek_bambauer/25 (2008).

[288] See Bardach, E., *The Implementation Game: What Happens After a Bill Becomes a Law* (Cambridge, MA: MIT Press, 1977), p 36-57 and 250.

[289] Grabosky, P. and Smith, R., *Crime in the Digital Age: controlling telecommunications and cyberspace illegalities* (New Brunswick-NJ and Sydney: Transaction Publishers and Federation Press, 1998), p 232-36.

behaviour, according to predefined rules. This provided flexibility to explore many aspects of online content regulation, taking into account the numerous actors and regulatory strategies used.

Second, the regulatory environment was described as decentred and polycentric, meaning that regulatory authority is diffused throughout society, there are multiple sites where regulation occurs, actors are autonomous entities interacting in complex ways, knowledge is fragmented, and more importantly, there is a blurring distinction between public and private regulatory action.

Third, the Internet was defined as a resilient and complex international communication network involving a number of applications and platforms, and as able to resist traditional regulatory intervention. Against this background, it has been argued that there are many regulable aspects of the Internet including infrastructure, protocols and technical standards, domain names, controversial content, and crime, and each one of these regulatory targets involve specific actors, challenges and strategies. Although regulation of such varied targets raises a number of relevant issues, there has been a substantial body of literature devoted to regulatory challenges posed by controversial content available on the Internet. This is the area where both state and private actors are struggling to develop new regulatory strategies across the world and they have been subject to a number of criticisms.

New communication technologies have challenged traditional regulatory intervention and, as a result, hybrid strategies were employed to face such challenges. The initial 'hands-off' rhetoric in relation to state involvement in the Internet no longer applies to regulation of criminal material available on the Internet. State-regulation has increased but has been unable to regulate alone. As such, state actors had to liaise with private actors (such as online intermediaries, software companies, Internet industry associations) to achieve its regulatory aims. This involved delegation of regulatory powers from the state to private actors and therefore a number of trade-offs were made, because both state and private actors had agendas of their own and pushed them forward that results in a number of negative consequences addressed above.

They were: (1) unchecked private censorship, scope creep, lack of focus, and excessive use of architecture-based regulatory tools; (2) increased unchecked and more invasive surveillance powers given to law enforcement authorities; (3) lack of transparency, accountability, legitimacy, proper oversight, and citizen involvement; and (4) issues around the inefficiency and ineffectiveness of regulatory intervention. Item (1) is related to free speech concerns, item (2) has to do with privacy protection, and items 3 and 4 are related to potential threats to democratic values and good regulation.

These are the evaluative criteria employed here to assess hybrid regulation of online content. Notably, these criteria are derived from academic literature and, as it is employed in the field, it

may incorporate not only other issues but also it may show that some variables are not so relevant in some jurisdictions as academics may think.

Do these criteria make sense in the fieldwork, and if so, in relation to which type of controversial content? Is there a particular type of online content that could serve as the best case study to evaluate such concerns? Are these concerns representative cross-nationally? Are there cross-national variations in relation to the regulatory approach employed? Are policies of online content regulation effective, efficient and ethical? Are regulators aware of such implications and are they including safeguards to minimise potential abuses? This research is expected to answer these questions and the evaluative criteria above is the starting point for such endeavour: the criteria are a tool to adjust current policymaking and guide future intervention.

Furthermore, it is a tool for designing a scheme of safeguards. The literature explored above indicates that a scheme of safeguards should be put in place to minimise the risk of free speech and privacy violations as well as to tackle the democratic deficit vis-à-vis the use of hybrid regulation. Suggestions include extending accountability, enhancing democratic governance, strengthening judicial and legislative oversight as well as citizen involvement, improving transparency, implementing impact assessment mechanisms, and following pre-stablished safeguards established before the implementation process. Although most people would agree that safeguards are necessary, not only the implementation of safeguards but of the regulatory model is more complex than it might seem at first. It involves political bargaining, conflicting agendas, cultural differences and financial interests. It also raises crucial issues such as the adjudication of apparent illegality of online content by private actors, success and failure of online content regulation, and the economics of regulation.

Assessment of current hybrid regulatory interventions of online content is an opportunity to explore these issues further and confront the literature findings with fieldwork evidence. But against which type of controversial content should these evaluative criteria be employed?

Although other controversial types of material available on the Internet are worth exploring, the problem of child pornography was chosen for a number of reasons. First, it has been used by governments worldwide to successfully justify the use of hybrid regulation in relation to online content. Second, it makes evident the resilient nature of the Internet to evade regulation. Third, it is in this area that regulatory measures have been pushed farther with little opposition and thus the negative implications for free speech, privacy protection and other democratic values can be assessed. Finally, child pornography has at the moment a relative international consensus about its criminal nature and this has pushed governments to cooperate at the international level; as a result, it makes a cross-national comparative approach less problematic.

The next part of this chapter will address the problem of online child pornography and the regulatory arrangements to limit access to such material, taking into account the typology of

regulatory models developed above. It will also justify the focus on child pornography and the choices of jurisdiction on which these evaluative criteria will be employed.

6 Child pornography on the Internet

The fight against online child pornography mobilised a number of governments around the world to erect a complex regulatory matrix involving both state and private actors, operating in different locations, at different degrees of evolution, under distinct legal cultures and jurisdictions, and with different amount of allocated budget. Generally, regulation of online child pornography is implemented with little opposition under the undebatable and successful argument of children protection and this is the reason why child pornography has been chosen. Because it shows the multitude of ways in which content regulation can be enforced on the Internet and the implications these strategies may have.

The development of modern anti-child pornography laws can be traced back to the late 1970s following the exposure of child sexual abuse as a social problem.[290] As a result, domestic anti-child pornography laws were created in a number of developed countries. This reaction was arguably effective in limiting the availability of child pornographic content within national borders until the mid-1990s.[291] Nevertheless, developments associated with the Internet and digital communication technologies have facilitated the proliferation of child pornography and so the enforcement of domestic anti-child pornography laws became largely ineffective. These developments include the digitisation of content, anonymised access, and the decentralised and multi-jurisdictional architecture of the Internet which rendered the choice of jurisdiction and the acts of policing state agencies heavily problematic.

This problematic law enforcement led to changes in three areas. First, domestic anti-child pornography laws escalated in some jurisdictions. New conducts and types of content associated with child pornography were criminalised in addition to the establishment of harsher penalties. Another response came at the international level to tackle the multi-jurisdictional nature of the Internet and the disparities in domestic laws such as the 2000 UN Optional Protocol[292] and the 2001 CoE's Cybercrime Convention.[293] Nonetheless, the enforcement of these international instruments fell short of disparities in domestic laws, technological know-how and slow ratification of international treaties.[294] Second, Internet industry self-regulation was also

---

[290] See Section 7 below.

[291] See generally Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003); O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007); and Jenkins, P., *Beyond Tolerance: Child Pornography on the Internet* (New York: New York University Press, 2001).

[292] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

[293] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[294] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 207 and 223.

employed via Internet industry CoCs and voluntary filtering schemes by online intermediaries. These strategies however were unable to tackle the problem of child pornography available on the Internet. Third, hybrid regulation was taken onboard via closer partnership between state and non-state regulatory actors, increased liability of online intermediaries, more investigatory and surveillance powers given to law enforcement authorities, and the extensive use of architecture-based regulatory technologies. Before these regulatory models are explored, the next section will introduce the problem of online child pornography.

The definition of child pornographic content was subject to international variations and proved to be controversial. Nevertheless, this investigation will employ the definitions established by the 2000 UN Optional Protocol and the 2001 CoE's Cybercrime Convention, because they addressed the key conceptual aspects of the problem and were generally accepted internationally. Both provisions defined a child as a person under the age of 18, in line with Article 1 of the 1989 UN Convention on the Rights of the Child.[295]

The 2000 UN Optional Protocol defined child pornography in Article 2(c):

> Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.[296]

The 2001 Council of Europe Cybercrime Convention defined child pornography in Article 9(2):

> […] the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct.[297]

Lawmakers across the world faced a number of challenges to define child pornographic content on the Internet.[298] The age of a child, the involvement of real children or of a totally virtual child, and the different ways that child pornographic content can be represented were heavily controversial and subject to national variations. First, defining the legal age of a child proved to be problematic. Although many jurisdictions ratified the age limit of 18 established in Article 1 of the 1989 UN Convention on the Rights of the Child, some countries consider the age of 16 as the age of sexual consent and this creates domestic legal inconsistencies. For example, two

---

[295] UN Convention on the Rights of the Child. Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989. Entry into force 2 September 1990, in accordance with article 49. 1989 (United Nations).

[296] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

[297] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[298] Gillespie, A., 'Defining Child Pornography: Challenges for the Law', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010; and also O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 66.

children aged 16 can perform consensual sexual activity legally but are prohibited from taking photographs of the act, because such visual depiction is defined as child pornographic content. In addition, it is difficult to identify whether the person depicted in the image is a child or not, particularly those persons near the age limit. Generally the rule of 'appears to be a child' is employed at the discretion of law enforcement agencies and is not subject to any objective guidance.[299] Second, the production of child pornography may involve a real or an entirely computer-generated child.[300] Another problem is whether the material where adults pose and dress as children is also to be considered child pornography.[301] Third, the legal definitions of child pornography may take into account the type of media (for example a photograph, altered photograph, entirely computer-generated photograph, drawings, tracings, cartoon imagery, annotated photographs, video and audio recordings, and written material) and the level of seriousness involved.[302] As a result, the law has permanently changed to address the latest technological developments and the demands of specific social groups.[303]

Finally, the activities associated with online child pornography can be divided into three areas: the production (for example, taking or making), distribution (*e.g.* publishing or selling) and access (for example, downloading, viewing, possessing or collecting). Generally domestic anti-child pornography laws and other regulatory strategies target these activities. Nevertheless, such categories are not watertight and alleged offenders may perform not only one but two or all three conducts simultaneously, because distinctions amongst the producer, distributor and viewer of child pornography became blurred after the Internet. For example, gaining access to online child pornographic content, such as viewing and downloading, may result in a making or distribution offence if the material is saved locally by the website browser or is stored in a P2P shared folder of a home computer, respectively.

7 The driving forces pushing domestic state regulation of online child pornography forward

Domestic anti-child pornography laws widened their scope in a number of jurisdictions to address conducts and types of content associated with child pornographic content after the arrival of the Internet. This escalation of domestic laws occurred jurisdictions such as Australia, Brazil and the United Kingdom[304] and was a result of enforcement challenges posed by the

---

[299] Gillespie, A., 'Defining Child Pornography: Challenges for the Law', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010.

[300] See the discussion about pseudo-photographs and prohibited images of children in Section 7.2 below.

[301] Some jurisdictions outlawed images that conveys the impression that the person portrayed is a child. See Criminal Justice and Public Order Act (c.33) 1994 (England and Wales) and Coroners and Justice Act (c.18) 2009 (England and Wales).

[302] There are also taxonomic efforts to assess the seriousness of the child pornographic content and this has been used to guide sentencing decisions on child pornography-related trials. See for example p 112 of the Sexual Offences Act 2003: Definitive Guideline (2007). Sentencing Guidelines Council, at <http://sentencingcouncil.judiciary.gov.uk/docs/web_SexualOffencesAct_2003.pdf> accessed 10 July 2011.

[303] Also, fuelling allegations of scope creep in regards to regulatory policies, as it will be discussed later.

[304] The anti-child pornography laws and regulations applied in these jurisdictions will be addressed in Chapter 4.

Internet, but there were also other driving forces behind this regulatory escalation that deserve further explanation. These include the media-made fear of crime, commercial private interests, use of child pornography as a 'soft-spot' to increase regulation in other areas, symbolic politics, and the legitimate interest of child protection.

The next subsections will explore such regulatory rationales and a number of driving forces behind the escalation of anti-child pornography laws both before and after the Internet. This discussion is important because it makes evident why these laws and regulations overcame the online censorship debate and were implemented much easier than other online content related laws and regulations (for example, in relation to copyrights infringement, adult pornography and privacy protection).

7.1 The harms before the Internet

Provisions against child pornography implemented after the late 1970s were based on a number of regulatory rationales. The protection of real children from direct harm was the key rationale supporting anti-child pornography laws at first. It was believed that direct harm would have to be imposed against the child involved in the production of child pornography. This argument was straightforward because if the material depicted the sexual abuse of a real child, the harm was self-evident.[305] This rationale led to the criminal provisions enacted during the late 1970s regulating the production and distribution, irrespective of commercial intent, and the possession with a view to distribution (*i.e.* qualified possession). It was not until the late 1980s and the early 1990s that other rationales were added to the mix via the criminalisation of the mere possession of child pornography in England and Wales, and United States, respectively.[306]

The criminalisation of mere possession was supported by a different argument because this act alone did not involve a direct harm being inflicted against a child nor did it involve further distribution. It was argued that mere possession of child pornography should be criminalised because it: (1) provides a market and makes the demand evident; (2) perpetuates the image and memory of the abuse over time; (3) may cause further sexual offences and promote harmful attitudes towards children; (4) may be used to seduce other children; (5) may normalise sexual interest in children; and (6) threatens society's shared sense of morality.[307] In addition, there are claims to consider child pornography not a crime of sexual abuse but of sexual exploitation irrespective of commercial gains so as to emphasise the fact that the abuse is prolonged over

---

[305] Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009), p 104.

[306] The mere possession of child pornographic content was only criminalised in Brazil in 2008. See Chapter 4.

[307] See Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003), p 24-5; O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 68-75; Krone, T., 'Combating Online Child Pornography in Australia', in Max Taylor and Ethel Quayle (eds.), *Viewing child pornography on the Internet* (Dorset: Russel House Publishing, 2005); Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009), p 105-7; Clough, J., 'Now you see it, now you don't: Digital images and the meaning of 'possession'', *Criminal Law Forum,* 19 (2008), 205-39; Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009), p 111-20.

time even though the image is merely possessed by the alleged offender.[308] These rationales make clear that the harm continues after the material is produced; it is prolonged over time via mere possession. The criminalisation of mere possession was also for policing reasons because it arguably facilitated the arrest of alleged producers and distributors of child pornography. These successful arrests may be however a result of other factors such as motivation of police forces, more public awareness about the problem, and media influence.

7.2 The harms after the Internet

The next step was the criminalisation of the making, distribution and mere possession of pseudo-photographs and the use of computers during the mid-1990s.[309] Pseudo-photographs were photographic depiction of non-real children (for example, computer-generated, morphed, juxtaposed and collages). Another rationale is employed here. It is argued that although pseudo-photographs did not involve a direct harm towards a real child for its production, they could be undistinguishable from child pornographic photographs that involved a real child. As such, the pseudo-photographs could be used to: (1) groom and seduce other children; (2) normalise the deviant sexual behaviour of paedophiles and escalate towards further sexual abuse of children; (3) restrict prosecutors in their ability to obtain convictions, because otherwise persecutors would have to prove that real children were involved; and (4) facilitate paedophile interaction.[310] The criminalisation of pseudo-photographs accepted that the harm not necessarily always derived from the direct sexual assault of a real child. Although no real child was involved, there was harm being caused against all children as a universal concept.[311] The provisions criminalising pseudo-photographs were enacted in the US[312] but were later struck down by the Supreme Court on the grounds of free speech protection.[313] This placed the burden on US prosecutors to prove that the material charged depicted real children. Although this burden was expected to limit successful criminal convictions in the US, Akdeniz reports that there were successful prosecutions in this regard.[314] Later in the US, such material was

---

[308] O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 78; Quayle, E., Loof, L., and Palmer, T., 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the III World Congress against Sexual Exploitation of Children and Adolescents', (Bangkok: ECPAT International, 2008) at <http://www.childcentre.info/public/Thematic_Paper_ICTPsy_ENG.pdf>, accessed 09 June 2010, p 17-22.

[309] In the US, the use of computers in the distribution of child pornography was outlawed in the Child Protection and Obscenity Enforcement Act 1988 (Pub. L. No. 100-690, 102 Stat. 4486) (USA).

[310] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 22-3; Gillespie, A., 'Defining Child Pornography: Challenges for the Law', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010.

[311] Oswell, D., 'When Images Matter: Internet Child Pornography, Forms of Observation and an Ethics of the Virtual', *Information, Communication and Society,* 9(2) (2006), 244-65.

[312] See the Child Pornography Prevention Act 1996 (United States, Pub. L. No. 104-208, 110 Stat. 3009) (USA).

[313] See *Ashcroft v Free Speech Coalition*, 535 US 234 (2002).

[314] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008); See also Wolak, J., Mitchell, K., and Finkelhor, D., 'Child Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study', *National Center for Missing and Exploited Children*, 2005) at <http://www.missingkids.com/en_US/publications/NC144.pdf>, accessed 07 June 2010, p 23.

criminalised but only in relation to production and distribution, not mere possession, which was still regarded as obscene child pornography.[315]

Non-photographic child pornography material, such as cartoon and drawings, was criminalised in England and Wales in 2009 under a similar rationale. The relevant consultation process acknowledged that although there was no strong evidence to support a causal relationship between these images and further sexual abuse of children, '[…] it is felt by the police and children's welfare organisations that possession and circulation of these images serves to legitimise and reinforce highly inappropriate views about children.'[316]

One common ground for criminalisation of mere possession of both photographs and pseudo-photographs was the alleged causal relationship between them and further sexual assault committed against a child. It was believed that viewing could escalate into actual sexual abuse of a child. This relationship is challenged by the academic literature, because it lacked substantial empirical proof of causality.[317] In addition, Taylor and Quayle report that not all offenders involved with child pornography sexually assault children nor are all pictures a sexual assault in progress.[318] Indeed, the people involved in the proliferation of child pornographic content are not only interested in financial reward but have non-commercial motivations (for example, grooming children, entertainment, sexual gratification, blackmail, and sense of belonging to a community of like-minded people).[319]

It is evident that the scope of the law broadened and escalated to include new perceived harms derived from latest technological developments. The mere possession of child pornography in England and Wales was a criminal offence not only in relation to photographs and pseudo-photographs but non-photographic content such as tracings, drawings and other cartoon imagery. Similarly, any sexually explicit material involving adults conveying the impression of being a child could be considered child pornography.

---

[315] See Section 304 of the PROTECT Our Children Act 2008 (Pub.L. 110−401, 122 Stat. 4229) (enacted 13 October 2008) (USA).

[316] See 'Consultation on Possession of Non-Photographic Visual Depictions of Child Sexual Abuse', Home Office, 2007) at <http://scotland.gov.uk/Resource/Doc/1099/0048474.pdf>, accessed 12 July 2010, p 1.

[317] Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009) p 123; Gillespie, A., 'Tackling Child Pornography: The Approach in England and Wales', in Max Taylor and Ethel Quayle (eds.), *Viewing child pornography on the Internet* (Dorset: Russel House Publishing, 2005), p 11; Carr, A., 'The social dimension of the online trade of child sexual exploitation material', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010, p 2.

[318] Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003), p 4 and 5.

[319] Child pornography may be also used to increase social status and recognition in paedophilia networks, replace unsatisfactory relationships and fulfil the pleasure of collecting. See Carr, A., 'The social dimension of the online trade of child sexual exploitation material', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010, p 5; and also Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003), p 8-22.; Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009), p 118; Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003), p 8-22.

Against this background, anonymised P2P, encryption, widespread unregulated mobile access, virtual reality games and human-machine sexual interaction are perceived as new venues for regulation and will eventually be the target of future anti-child pornography laws. Similarly, the availability of human-machine interaction devices,[320] virtual reality sex games[321] and sexting[322] produced new perceived harms to children and new opportunities for criminalisation. The convergence amongst artificial intelligence, robotics and biomedical engineering provided new avenues for the proliferation of harms associated with child pornographic content. This makes evident the vicious circle of escalating criminal laws to cope with technological developments that not only displaces crime but has chilling effects to free speech and privacy protection of Internet users.[323]

7.3 Other driving forces

The regulatory rationales described above were supported by an arguably legitimate interest in protecting children against sexual abuse in the online environment. The technological advances led to new opportunities for crime commission and the law has adapted accordingly to tackle such crimes.[324] Nevertheless, there were other driving forces pushing the state regulation of child pornography on the Internet: the media-made fear of crime, commercial private interests, use of child pornography as a 'soft-spot' to increase regulation in other areas, and symbolic politics. These issues will be explored below.

In *Folk Devils and Moral Panics*, Cohen addresses the demonisation of certain social groups and issues, the allocation of blame, and the following exaggerated media representation that ignites social control responses.[325] For him, these responses are shaped not by real evidence but, to a greater extent, by the perceived threat of a particular issue. Generally this seems to explain governmental reaction in relation to the criminal content available online. For example, Wykes and Harcus argue that social control of online terror has been based on a perceived threat mediated by media discourses and disconnected from the realities of crime, and this perceived threat often informs and misleads policymaking.[326] Similarly, Jewkes and Yar argue that societal

---

[320] See the research undertaken by Professor Kevin Warwick about human-machine interaction and cyborgs at <http://www.kevinwarwick.com/>, accessed 11 August 2010.

[321] See Woods, J., 'Avatars and Second Life adultery: A tale of online cheating and real-world heartbreak', *Telegraph,* 2008 at <http://www.telegraph.co.uk/technology/3457828/Avatars-and-Second-Life-adultery-A-tale-of-online-cheating-and-real-world-heartbreak.html>, accessed 11 August 2010; Waters, D., 'Can Second Life regulate virtual sex?', *BBC News,* 2009 at <http://www.bbc.co.uk/blogs/technology/2009/04/can_second_life_regulate_virtu.html>, accessed 11 August 2010.

[322] Ahmed, M., 'Police warn over rise of teenage 'sexting' trend', *The Times,* 05 August 2009 at <http://technology.timesonline.co.uk/tol/news/tech_and_web/article6738532.ece>, accessed 14 May 2011.

[323] Would the display of child pornographic content hosted in a neuro-surgical implanted device and screened in an artificial retina be liable to criminal prosecution? Would the sexual intercourse with a child robot to be criminalised in the future? These questions show how anti-child pornography laws can escalate further and, particularly, how regulatory policies can be even more invasive to current standards of free speech and privacy protection.

[324] Grabosky, P., *Electronic Crime* (Master Series in Criminology; Upper Saddle River, NJ: Pearson Prentice Hall, 2007), p 5.

[325] Cohen, S., *Folk devils and moral panics: the creation of the Mods and Rockers* (3rd edn.; London: Routledge, 2002).

[326] Wykes, M. and Harcus, D., 'Cyber-terror: construction, criminalisation and control', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 214-27, p 216 and 225.

responses to online crime have been largely mediated and constructed via many domains of representation.[327] For Wall, the perceptions of cybercrime have been 'shaped by the cultural origins of cybercrime in social science fiction' whilst 'the practical reality is quite different.'[328] As a result, a growing culture of fear about cybercrime[329] has shaped the regulatory responses amidst little evidence about the regulatory target; indeed, there is little knowledge about the real dimension of online child pornography, because the occurrence of cybercrime often goes unreported to authorities,[330] global crime statistics are problematic,[331] and this is an underground criminal activity. These are reasons why assessing regulatory success and effectiveness in relation to online child pornography regulatory policymaking is fraught with difficulties.

Similarly, this tendency to respond quickly to an immediate or anticipated crisis with potential for political consequences and the difficulties in regulating complex issues have been demonstrated in another regulatory arena; the regulation of dangerous dogs. Although substantially different in nature, both the problem of child pornography and dangerous dogs share some similarities which are relevant to the regulatory analysis (*e.g.* unthinking reflex legislative response to media agenda, apparent consensus about the threat posed to children, regulation more problematic than what appears to be at first sight, and legislation that is difficult to enforce).[332] These examples make evident how institutions shape their responses differently in a process of 'selective adaptation' from outside pressures.[333] As such, not only the media influence but the institutional response and institutional capabilities played a role here.

Nevertheless, such responses are not the only factors driving anti-child pornography regulation. A number of 'moral entrepreneurs' used this exaggerated perceived threat to their advantage pushing their own agendas forward.[334] For example, legislators, non-governmental organisations, businesses, and regulators embarked on moral crusades to increase political

---

[327] Jewkes, Y. and Yar, M., 'Introduction: the Internet, cybercrime and the challenges of the twenty-first century', Ibid, 1-8, p 5.

[328] Wall, D., 'Criminalising cyberspace: the rise of the Internet as a 'crime problem'', Ibid, 88-103, p 100.

[329] See Wall, D., 'Cybercrime and the Culture of Fear: social science fiction and the production of knowledge about cybercrime', *Information, Communication and Society,* 11(6) (2008), 861-84.

[330] Grabosky, P. and Smith, R., *Crime in the Digital Age: controlling telecommunications and cyberspace illegalities* (New Brunswick-NJ and Sydney: Transaction Publishers and Federation Press, 1998), p 215; Jewkes, Y., 'Public policing and Internet crime', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: WIllan Publishing, 2010), 525-45, p 527; Wall, D., *Cybercrime: the transformation of crime in the information age* (Cambridge: Polity Press, 2007).

[331] Maguire, M., 'Crime data and statistics', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (4th edn.; Oxford: OUP, 2007).

[332] See generally Hood, C., 'Assessing the Dangerous Dogs Act: when does a regulatory law fail?', *Public Law,* Summer (2000), 282-305; and Lodge, M. and Hood, C., 'Pavlovian Policy Responses to Media Feeding Frenzies? Dangerous Dogs Regulation in Comparative Perspective', *Journal of Contingencies and Crisis Management,* 10(1) (2002), 1-13. See also the government mandatory plan to micro-chip dangerous dogs in the England and Wales at Adetunji, J., 'Dog microchips expected to be made compulsory', *The Guardian,* 21 April 2012, sec. World News at <http://www.guardian.co.uk/world/2012/apr/21/dog-microchips-compulsory?newsfeed=true>, accessed 05 May 2012.

[333] Lodge, M. and Hood, C., 'Pavlovian Policy Responses to Media Feeding Frenzies? Dangerous Dogs Regulation in Comparative Perspective', *Journal of Contingencies and Crisis Management,* 10(1) (2002), 1-13, p 3.

[334] See ch 7 and 8 in Becker, H. S., *Outsiders: Studies in the Sociology of Deviance* (New York, NY.: The Free Press, 1966).

capital, achieve governmental funding, obtain commercial revenues, and accumulate more authority, respectively. In addition, after their crusade was finished, new rules were created and the relevant machinery of enforcement was put into place, they acted to secure their institutional survival. As such, they often searched for other alarming issues, widened the relevant bureaucracy and regulatory powers, justified their authoritative position, and acted to win the respect of the regulatees. The actors responsible for the actual enforcement lived a permanent dialogical dilemma of showing that, whilst their work was necessary, worthwhile, and effective, the threat still existed, whether it was moving to new venues or being transformed somehow.[335] Their work was never completely finished and the problem was permanently put into the political agenda to secure their institutional survival.

The little opposition to anti-child pornography laws and regulations explains why this regulatory enterprise found fewer obstacles to implementation in comparison to other problematic online content. Generally regulation of online content involves conflicting principles such as free speech vs censorship and fighting terrorism vs privacy protection,[336] and it is followed by strong opposition by anti-censorship groups. Nevertheless, it seems that under the protection of children from sexual abuse rationales, anti-child pornography laws overcame both free speech and privacy protection concerns and found little obstacles so far to escalate across the world. In addition, people who opposed these laws risked being seen as collusive with paedophiles.[337] The limited debate during lawmaking facilitated the passing of these laws without greater public scrutiny.

7.4 Final remarks

From the 1970s onwards, there were a number of rationales and driving forces pushing domestic state regulation of online child pornography forward faster than those in relation to other problematic online content. This led to an escalation of anti-child pornography laws targeting a number of conducts and types of content as well as establishing harsher penalties associated with child pornography on the Internet. As argued by O'Donnell, the domestic state regulation of child pornography has produced since the late 1970s a 'tsunami of laws and promises' in some jurisdictions.[338]

Both commercial and non-commercial production and distribution of child pornography were outlawed during the late 1970s and the early 1980s. Mere possession was criminalised in the late 1980s in England and Wales. The use of computers in the production and distribution of child pornography was outlawed around the mid-1990s which led to the criminalisation of

---

[335] Ibid , p 157.

[336] Grabosky, P. and Smith, R., *Crime in the Digital Age: controlling telecommunications and cyberspace illegalities* (New Brunswick-NJ and Sydney: Transaction Publishers and Federation Press, 1998), p 122.

[337] See in Chapter 4 the case of Internet entrepreneurs in the UK who were demonised by tabloid newspapers because they oppose the regulatory stance taken by the police and the government in 1996.

[338] O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 222.

pseudo-photographs in England and Wales. The age of a child was raised from the age of 16 to 18 in most jurisdictions.[339] The courts in England and Wales blurred the distinctions between possession and distribution, downloading and making, printing and making, and in 2009 non-photographic child pornography (for example cartoon pornography) was criminalised. As of until 2010, any image (photographic, pseudo-photographic or non-photographic) depicting children (real or computer-generated) or adults (conveying the impression of a child) in sexual activity was outlawed in England and Wales.

There was a strong international call to criminalise written material, child erotica (meaning child nudes without any sexual activity involved) and cartoon imagery.[340] Indeed, anti-child pornography laws were increasing in most jurisdictions across the world. Nevertheless, this regulatory response via domestic criminal laws and the courts (domestic state regulation) was only partially successful in limiting access to online child pornography, because of the multi-jurisdictional and resilient nature of the Internet. Following Hood, laws and the courts do not enforce the rule on their own and therefore making rules is something completely different from enforcing them; it involves difficult choices about enforcement options (for example, modifying the rule, persuasion, pursuing and punishing violators, or making it difficult to break the rule), enforcement levels (how much to enforce?), and enforcement actors (public or private?).[341]

The next section will explore some reasons why enforcement of anti-child pornographic laws is problematic on the Internet and will employ the typology of regulatory models explored above in Section 1.2.

8 Regulatory models for online child pornography

> Just when suppression of the child pornography trade seemed within sight as national legislatures finally began to take seriously the harms caused by magazines and videos, the Internet arrived on the scene.[342]
>
> In the past, obtaining child pornography was difficult […] but now circumstances have changed […] this is because of the Internet.[343]

8.1 State and multi-state regulation

---

[339] In 1984 in the United States, and in 2003 in England and Wales.

[340] Quayle, E., Loof, L., and Palmer, T., 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the III World Congress against Sexual Exploitation of Children and Adolescents', (Bangkok: ECPAT International, 2008) at <http://www.childcentre.info/public/Thematic_Paper_ICTPsy_ENG.pdf>, accessed 09 June 2010.

[341] Hood, C., *Administrative Analysis: an introduction to rules, enforcement and organizations* (Brighton, Sussex: Wheatsheaf Books Limited, 1986), p 48. See also Bardach, E., *The Implementation Game: What Happens After a Bill Becomes a Law* (Cambridge, MA: MIT Press, 1977).

[342] O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 28.

[343] Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003), p 9.

Although domestic anti-child pornography laws escalated in many jurisdictions with the advent of the Internet, child pornographic content was produced across the world, sexual offenders were able to groom children in wider geographical basis, photographs and videos were digitally manipulated and uploaded onto the Internet with ease, and child pornographic material was distributed and accessed on the Internet via different platforms and applications.[344] Once uploaded onto the Internet, child pornography could be accessed virtually anywhere in the world, be it via hypertext applications, social networking systems (SNS), real-time instant messaging systems, closed paedophilia online groups or anonymised and encrypted channels. Domestic state regulation alone is unable to effectively limit access to online child pornography.

The reasons why domestic state regulation has been challenged include the digitisation of content, anonymised access and multi-jurisdictional nature of the Internet.

First, digitisation of content facilitated the production, distribution and collection of child pornographic material, particularly derived from print material freely available in the past. In addition, the alleged offender does not have to go to a photography store to have the film developed, can avoid using the mail services to access and distribute such material, and have a number of computer graphics software to manipulate original images or create new material.

Second, anonymised access has challenged the policing of content, identification of alleged offenders and collection of criminal evidence. In addition, there are more actors involved in the transmission of child pornography than only the sender and receiver. A number of online intermediaries are responsible for receiving, hosting and passing on packets of data (for example Internet service, content and host providers, social networking and real-time messaging systems)[345] and this diversity of actors makes the policing of child pornographic content more complex.

Third, the Internet is a transnational communication medium and therefore subject to regulation by numerous sovereign states. It connects people worldwide in a number of different jurisdictions subject to different child pornography laws and content-related regulatory schemes and this renders the choice of jurisdiction and the enforcement of jurisdictional powers heavily problematic when applied to Internet transactions. For example, although there is a rough consensus about the criminal nature of child pornographic content across the world, domestic anti-child pornography laws of each jurisdiction may define the age of a child as well as the type of content, conducts and penalties associated with child pornography differently. Nevertheless, taking into account that content made available on the Internet is generally

---

[344] See generally Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008); and also Quayle, E., Loof, L., and Palmer, T., 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the III World Congress against Sexual Exploitation of Children and Adolescents', (Bangkok: ECPAT International, 2008) at <http://www.childcentre.info/public/Thematic_Paper_ICTPsy_ENG.pdf>, accessed 09 June 2010.

[345] Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88; See also Reed, C., *Internet Law: Text and Materials. Second edition.* (Cambridge: Cambridge University Press, 2004).

accessed in all jurisdictions, and that domestic laws cannot be enforced in a foreign jurisdiction without a bilateral agreement or international convention, harmonisation of criminal laws is necessary for the regulation of child pornography at the international level. Otherwise, country A with harsher anti-child pornography criminal laws is unable to enforce its laws limiting access to such material within its jurisdiction, if a more tolerant country B, outside the jurisdiction of A, is a producer or host of child pornographic content as defined in A.

Another problem is the complex cross-national law enforcement and cooperation between domestic police forces. Differences in relation to domestic procedural criminal laws, budget, expertise and priority given to fighting online child pornography amongst police forces across the world make law enforcement heavily problematic. Finally, the multi-jurisdictional nature of the Internet facilitates the access to and grooming of children in wider geographical areas and in real-time. Before the Internet, sexual offenders generally would have to access real children in the vicinity or travel to other countries.[346] Nevertheless, the Internet provides access to children located virtually anywhere in the world, and such feature expanded opportunities for sexual abuse against children and production of child pornographic material.[347]

The multi-jurisdictional challenges faced by domestic state regulation led governments to employ multi-state regulatory strategies to harmonise anti-child pornography laws and law enforcement at the international level. Domestic state regulation had limited success in limiting access to child pornographic content largely because of the multi-jurisdictional nature of the Internet. This led some governments to employ multi-state regulatory responses to improve the cross-national functionality of national legal systems.[348] These responses included the international harmonisation of anti-child pornography substantive and procedural criminal laws.

There are a number of cross-national variations in relation to domestic anti-child pornography laws. For example, the 2008 International Center for Missing and Exploited Children reports that of the 187 Interpol members only 29 have ‘sufficient’ legislation to tackle online child pornography, and suggests that countries should increase efforts towards the harmonisation of anti-child pornography laws at the international level to avoid safe havens for offenders.[349] Similarly, Akdeniz argues that seeking international harmonisation of laws is crucial to address the problem of child pornographic content available on the Internet.[350]

---

[346] O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 36.

[347] See Wall, D., *Cyberspace crime* (Aldershot: Ashgate Dartmouth, 2003).

[348] Williams, K., 'Transnational developments in Internet law', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 466-91, p 467.

[349] ICMEC, 'Child Pornography: Model Legislation & Global Review ', International Centre for Missing & Exploited Children, 2008) at <http://www.icmec.org/en_X1/English__5th_Edition_.pdf>, accessed 08 June 2010.

[350] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 164.

The 1989 UN Convention[351] and the 2000 UN Optional Protocol[352] provided the legal framework of children's rights and defined what online child pornography is. The 1999 UN Child Labour Convention[353] established in Article 3(b) that the use of a child for the production of pornography or pornographic performances is one of the worst forms of child 'labour.' The UN published a number of reports to push anti-child pornography policymaking worldwide.[354] Another example of international lawmaking is the 2001 CoE's Cybercrime Convention[355] which established a number of substantive and procedural anti-child pornography criminal laws to harmonise legislation, facilitate investigation and improve cooperation within Europe and beyond. Expanding extradition capabilities is another example of multi-state regulation designed to target alleged offenders. Many countries passed domestic laws to facilitate the extradition of nationals committing child pornography related offences in other countries, where such laws are inexistent as well as domestic laws to punish nationals returning from these countries. The 2011 EU Directive established in Article 5(3) that EU member states shall take the necessary measures to punish the intentional access to child pornography available on the Internet.[356]

Nevertheless, multi-state regulation has a number of limitations to stop access to child pornographic content on the Internet. These international treaties are not directly binding, countries reserve the right not to apply some provisions, and the ratification process is slow and politically problematic.[357] For example, the implementation of the 2001 CoE's Cybercrime Convention by non-European states was limited because some countries had concerns about the Eurocentric nature of the treaty and they demanded the establishment of another agreement based on wider global participation.[358] Similarly, the UK signed the 2001 CoE's Cybercrime Convention on 23 November 2001 but ratified it only on 25 May 2011, because of issues relating to some procedural provisions.[359]

---

[351] UN Convention on the Rights of the Child. Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989. Entry into force 2 September 1990, in accordance with article 49. 1989 (United Nations).

[352] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

[353] Worst Forms of Child Labour Convention 1999 (International Labour Organization (ILO) in 1999 as ILO Convention No 182) (ILO).

[354] See for example Petit, J., 'Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the sale of children, child prostitution and child pornography. E/CN.4/2005/78, 23 December 2004.', (New York: United Nations, 2004) at <http://www.unhcr.org/refworld/category,REFERENCE,UNCHR,,,42d66e480,0.html>, accessed 30 June 2010.

[355] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[356] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union).

[357] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 207 and 223; McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 265.

[358] See UN, 'Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, 12-19 April 2010)', at <http://www.unodc.org/unodc/en/crime-congress/crime-congresses.html>, accessed 04 December 2011.

[359] See Murray, A., *Information Technology Law: the law and society* (Oxford: OUP, 2010), p 406.

International law enforcement is another key strategy to limit access to child pornography available online, because international anti-child pornography laws would be largely ineffective if law enforcement agencies did not cooperate internationally to enforce them. For Grabosky and Smith, communication and collaboration amongst police forces, creation of specialised units, improved training funding and staffing are essential tasks to tackle online crimes.[360] As such, there were advances in the area of cross-national policing, harmonisation of investigatory and prosecutorial protocols for reaching offenders overseas. A number of law enforcement agencies and specialised police forces operated cross-nationally to fight child pornography on the Internet, such as the G8 Virtual Globe Task Force,[361] Interpol[362] and the 24/7 protocol established by the 2001 CoE's Cybercrime Convention. In addition, there were a number of arguably successful international police operations (for example, Operations Wonderland, Landslide, Ore, and Starburst). Nevertheless, international law enforcement was not without problems. Generally domestic police forces lacked the proper financial resources and technical expertise, the political will to prioritise the protection of children over property-related online crimes, and the ability to cooperate internationally.[363] The permanent rotation of police personnel, the conflicts over the ownership of the investigation by different police forces and the under-reporting of online crime were reasons for unsuccessful Internet policing.[364]

Domestic anti-child pornography laws were already in place before the advent of the Internet and digital communication technologies. Nevertheless, such technological developments challenged the enforcement of domestic laws in a number of ways and this led to an escalation of both state and multi-state regulation. Alongside this escalation process, self-regulatory strategies were employed by private actors, particularly the Internet industry, to limit the availability of child pornographic content on the Internet. This is the topic of the next section.

8.2 Self-regulation

In the early days of the Internet, self-regulation and spontaneous ordering have been advocated by some authors as the proper regulatory approach to tackle controversial content available online.[365] The self-regulation school considers the Internet a free environment, a place unresponsive to state regulation, a separate jurisdiction, a control-averse and anarchic space only subject to laws of its own. As a result, the Internet industry, online communities and users are believed to be in a better position to regulate controversial online material by themselves without any regulatory intervention from the state.

---

[360] Grabosky, P. and Smith, R., *Crime in the Digital Age: controlling telecommunications and cyberspace illegalities* (New Brunswick-NJ and Sydney: Transaction Publishers and Federation Press, 1998), p 216-18.

[361] 'Virtual Globe Taskforce', at <http://www.virtualglobaltaskforce.com/>, accessed 09 August 2010.

[362] INTERPOL, 'Interpol', at <http://www.interpol.int/>, accessed 09 August 2010.

[363] Carr, J. and Hilton, Z., 'Combating child abuse images on the internet – international perspectives. [Unpublished]', (2010) .

[364] Jewkes, Y. and Andrews, C., 'Internet Child Pornography: international responses', in Yvonne Jewkes (ed.), *Crime Online* (Devon: Willan Publishing, 2007), 60-80, p 72-5; See also Wall, D., *Cyberspace crime* (Aldershot: Ashgate Dartmouth, 2003).

[365] See Section 3.1 above about self-regulation.

In a number of regulatory issues, private actors are regarded as holding more technical expertise and flexibility than state agencies to address the regulatory problem and this position is also advocated by the online self-regulation school. For Akdeniz, self-regulatory strategies are commonly regarded as cost-effective and tailor-made, and therefore able to avoid blunt censorship laws.[366] Indeed, self-regulation strategies against online child pornographic content have been implemented in the UK to avoid the burden of domestic laws regulating the operation of online intermediaries.[367] In addition, self-regulation has been employed as a regulatory response not only in relation to content 'harmful to minors' (*e.g.* use of voluntary online content filtering, rating systems and public awareness programmes), but in regard to online child pornography (for example via Internet industry self-regulation and the creation of Internet hotlines) as a complement of domestic criminal law.[368] The self-regulatory instruments available to limit access to child pornographic content on the Internet may include private agreements and terms of service (ToS) regulated by contract law, Internet industry codes of conduct (CoCs), online community-based decisions and parental monitoring.

Online intermediaries such as Internet service, content and host providers, online content filtering manufacturers, and online payment systems may belong to an Internet industry association. There are a number of such associations across the world and they are generally expected to protect and represent online intermediaries' interest nationally and regionally (for example, Internet Service Providers Association - ISPA UK, EURO ISPA, the Australian Internet Industry Association - IIA, and the Brazilian ABRANET).[369] These associations may establish CoCs to regulate the behaviour of its members and indicate the best practice in the industry.[370] For example, the ISPA UK CoP[371] was adopted in 1999 and established the minimal general requirements and best practices that their members should follow as well as the type of sanctions they are subject to, setting the grounds for the work developed by the Internet Watch Foundation.[372] Similarly, the Australian IIA established a code of conduct of its own that complement the Australian censorship laws.[373] Generally these CoCs contain provisions about the availability, removal and notification of controversial content including child pornography.

---

[366] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 247.

[367] See Chapter 7 about online child pornography regulation in the United Kingdom.

[368] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (1999).

[369] ISPA, 'Internet Service Providers' Association UK', at <http://www.ispa.org.uk/home/>, accessed 29June 2010; EUROISPA, 'European Association of Internet Service Providers', at <http://www.euroispa.org/>, accessed 29 June 2010; IIA, 'Internet Industry Association: policy, advocacy and representation for Australian business', at <http://www.iia.net.au/>, accessed 22 August 2011; ABRANET, 'Associação Brasileira de Internet', at <http://www.abranet.org.br/>, accessed 30 August 2010.

[370] Also known as Codes of Practice.

[371] ISPA, 'ISPA Code of Practice', at <http://www.ispa.org.uk/>, accessed 29 June 2010.

[372] IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

[373] IIA, 'Codes for Industry Co-Regulation in Areas of Internet and Mobile Content (Pursuant to the Requirements of the Broadcasting Services Act 1992). May 2005 (includes provisions affecting mobile services). Version 10.4. As Registered by the Australian Broadcasting Authority.', (Internet Industry Association, 2005) at <http://www.iia.net.au> Accessed 26 September 2011.

Nevertheless, although these private actors established self-regulatory provisions to limit access to child pornography, these measures were only enforceable towards a limited number of voluntary members, because membership was generally voluntary. In addition, the regulatory provisions established via CoCs may vary in practice, and there was only a limited range of sanctions available.[374] Industry associations have tended to be lenient when applying sanctions against their own members.

The ToSs of a company and the private agreements regulated by contract law were employed to regulate the controversial content available online. Generally violations may lead to interruption of the service, cancellation of accounts, civil compensation or criminal prosecution. For example, if one user was found to be uploading, hosting or exchanging child pornography, its account may be closed, the alleged criminal material removed, the evidence preserved, and the relevant law enforcement agency notified. Nevertheless, enforcement of ToSs has had only a limited, if any, impact on stoping people accessing child pornography on the Internet. Closing an account does not stop the user from creating another account or using the service of another company operating within the same country or abroad. Enforcing private agreements was also problematic because users might have provided false information about themselves and accessed the service via anonymised channels.

Another self-regulatory strategy employed against child pornography is the activity of online 'vigilantes and militias.'[375] These self-appointed groups often took the 'law into their own hands' and tried to disrupt the child pornography activities online. Private and grassroots groups (for example the Anti-Pornography League, Condemned, Cyberangels, Pedowatch and Ethical Hackers against Paedophilia) have targeted online child pornography since the mid-1990s.[376] Although online vigilantism by self-appointed communities may have some advantages over formal law enforcement, such as employing specialised expertise without being subject to formal legal constraints, law enforcement via the state is arguably more legitimate, transparent and accountable.[377] Indeed, online vigilantism has a number of limitations that includes the violation of the law, deletion of criminal evidence, function creep, and perhaps pathological motives.[378]

---

[374] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 248.

[375] Jenkins, P., *Beyond Tolerance: Child Pornography on the Internet* (New York: New York University Press, 2001), p 165.

[376] See Pedowatch, 'Pedowatch.Org', at <http://www.aboutus.org/PedoWatch.org>, accessed 29 June 2010; Cyberangels, 'Cyberangels', at <http://www.cyberangels.org/about.php>, accessed 29 June 2010; ACPO, 'AntiChildPorn.Org', at <http://www.antichildporn.org/overview.html>, accessed 29 June 2010; APL, 'The Anti-Pornography League', at <http://www.angelfire.com/art/antipornography/>, accessed 29 June 2010.

[377] Grabosky, P., *Electronic Crime* (Master Series in Criminology; Upper Saddle River, NJ: Pearson Prentice Hall, 2007), p 98.

[378] Jenkins, P., *Beyond Tolerance: Child Pornography on the Internet* (New York: New York University Press, 2001), p 182; Wall, D., 'Policing and the Regulation of the Internet', *Criminal Law Review. December Special Edition: Crime, Criminal Justice and the Internet,* (1998), p 84; McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007), p 285.

The use of state, multi-state, and self-regulation strategies to limit access to child pornography on the Internet has been explored so far. The hybrid regulation of child pornography on the Internet is the topic of next section.

8.3 Hybrid regulation

> This is too big a task for the police alone. The active cooperation of ISPs, businesses and other institutions, as well as individual users, is essential if there is to be any prospect of success.[379]

> […] the governance of Internet child pornography requires a collective and 'multi-pronged response to a multifaceted problem' in which both public and private bodies are involved at various levels.[380]

> In relation to the internet we need a shared culture of responsibility with families, industry, government and others in the public and third sectors all playing their part […].[381]

Hybrid regulation was explored generally in Section 3.3 above. It involves regulation by both state and private regulatory actors, increased legal liability and control placed on online intermediaries, and increased capabilities of systems of social control via more investigatory powers given to law enforcement agencies and the use of architecture-based regulatory tools.[382] These features will be explored below in relation to online child pornography regulation.

8.3.1 Online content regulation via private actors

Generally regulation of controversial online content via online intermediaries is increasing[383] and this is also the case in relation to child pornography. Under the threat of arrests and regulatory legislation, Internet service and content providers in the UK have set up an Internet industry organisation to receive reports from the public, notify relevant online intermediaries and police forces, and manage a blocklist of URLs associated with alleged child pornographic content available on the Internet. A Parliamentary Investigation Committee (CPI) forced the

---

[379] O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007), p 174.

[380] Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008), p 2 (quotation marks in the original).

[381] Byron, T., 'Safer Children in a Digital World: The Report of the Byron Review', 2008) at <http://www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf>, accessed 30 June 2010, p 2.

[382] This hybrid approach is also called multi-layered approach or co-regulation. See Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008); Byron, T., 'Safer Children in a Digital World: The Report of the Byron Review', 2008) at <http://www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf>, accessed 30 June 2010; 'Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States (Executive Summary)', (Cambridge, MA: The Berkman Center for Internet & Society at Harvard University, 2008) at <http://cyber.law.harvard.edu/pubrelease/isttf/>, accessed 07 June 2010; Cave, J., Marsden, C., and Simmons, S., 'Options for and Effectiveness of Internet Self- and Co-Regulation. Summary prepared for the European Commission', (Cambridge: RAND Europe, 2008) at <http://www.rand.org/pubs/technical_reports/2008/RAND_TR566.pdf>, accessed 04 June 2010.

[383] See Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88; Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009).

major Brazilian ISPs to establish standardised procedures to record online logs of Internet users in order to identify alleged offenders. Online payment systems were also targeted. The Financial Coalition against Child Pornography on the Internet[384] was created in 2006 to tackle commercial websites allegedly selling access to child pornography (*e.g.* blocking the payment and unregistering the relevant websites). Domain names' registers were asked to revoke domain names of websites allegedly involved with child pornography. There were growing domestic legislation to establish criminal liability of online intermediaries for the content they host or distribute, and to establish mandatory recording of users' identification and online logs. In addition, governments passed domestic laws to increase surveillance powers of law enforcement agencies investigating child pornography related offences. These laws facilitated the use of surveillance equipment, collection of evidence, identification of users, and cooperation between relevant police forces and online intermediaries. The increased use of cloud-computing and distant digital storage facilitated the regulation of content by private actors, because user-generated content is under the supervision of an easily regulated node of the network.

8.3.2 Internet hotlines

Hybrid regulation was also implemented in the EU via the EU Safer Internet Programme, the face of the European policymaking in relation to harmful and illegal online content. Generally child pornography was tackled via the creation of national Internet hotlines and the International Association of Internet Hotlines (INHOPE) Forum,[385] and legal liability of online intermediaries. The EU involvement with online regulation started in 1996. Under the motto 'what is illegal offline remains illegal online,' the 1996 Green Paper[386] and the 1996 Communication[387] established the distinction between illegal (*e.g.* child pornography, racial hatred and terrorism) and harmful (*i.e.* material that is harmful to minors, for example legal adult pornography, political opinions, religious beliefs or any other material that might offend the values and feelings of other persons) online content. The 1996 Communication recommended the use of self-regulatory measures (*e.g.* empowerment of parental supervision via voluntary filtering and rating systems) to tackle harmful content, whereas it suggested the enforcement of domestic laws (*i.e.* domestic state regulation), co-operation between member states (*i.e.* multi-state regulation), the legal liability of online intermediaries, and the creation of reporting mechanisms (*e.g.* Internet hotlines) to limit the availability of child pornography on the Internet.

---

[384] FCACP, 'Financial Coalition Against Child Pornography', at <http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703>, accessed 09 June 2010.

[385] INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010.

[386] Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services. Brussels, 16.10.1996, COM(96) 483 final. (1996).

[387] Illegal and Harmful Content on the Internet. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Brussels, 16.10.1996, COM (96) 487 final. (1996). at <http://aei.pitt.edu/5895/01/001527_1.pdf> accessed 12 July 2010.

The EU Safer Internet Programme can be divided into four stages: (1) Safer Internet Action Plan - SIAP (1999-2002); (2) Safer Internet Action Plan - SIAP (2003-2004); (3) Safer Internet Plus Programme (2005-2008); and the (4) Safer Internet Programme - SIP (2009-2013).

The 1999 SIAP (1999-2002)[388] covered a period of four years with a budget of €25 million (euros) and promoted the use of Internet industry self-regulation (*e.g.* codes of conduct) and content monitoring schemes (*e.g.* Internet hotlines) to limit access to child pornography in addition to the use of domestic state regulation. The 1999 SIAP Evaluation[389] reported unsatisfactory uptake of filtering and rating systems for harmful content, poor involvement of the Internet industry, the need for addressing the role of new technologies and engaging with foreign actors, but also the successful creation and networking of Internet hotlines in all member states, except for Portugal and Luxembourg.

The 2003 SIAP (2003-2004)[390] covered a period of two years with a budget of €13,3 million (euros). It addressed the protection of children in relation to the use of new technologies (for example mobile broadband content, online games, P2P networks, and real-time messaging systems), it fostered the involvement of the Internet industry and international cooperation. The 2003 SIAP Evaluation[391] reported little improvement in relation to uptake of filtering or harmful content, but it emphasised the success of national Internet hotlines tackling child pornography.

The following 2005 Safer Internet Plus Programme (2005-2008)[392] established four lines of action: (1) fighting against illegal content; (2) tackling unwanted and harmful content; (3) promoting a safer environment; and (4) awareness raising. It continued to support the use of voluntary filtering at the user-level to tackle harmful content but started to encourage the use of blocking systems to limit access to child pornography at the 2006 Safer Internet Forum and funded the CIRCAMP Project in 2007.

---

[388] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. (1999).

[389] 'The Evaluation of the Safer Internet Action Plan 1999-2002. Executive Summary.', (Luxembourg: European Commission, 2003) ; See also 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions concerning the evaluation of the Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors. Brussels, 03.11.2003. COM(2003) 653 final.', 2003) .

[390] Decision No. 1151/2003/EC of the European Parliament and of the Council, of 16 June 2003, amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. (2003).

[391] 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Final evaluation of the implementation of the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Brussels, 06.11.2006, COM(2006) 663 final.', 2006) .

[392] Decision No. 854/2005/EC of the European Parliament and of the Council, of 11 May 2005, establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies. (2005).

Finally, the 2009 Safer Internet Programme (2009-2013)[393] has a budget of €55 million (euros) and addresses the threats posed to children by the so-called web 2.0 (*e.g.* social networking systems, user-generated content etc.). It also targeted the problem of cyberbullying and grooming. It has four lines of action: (1) ensuring public awareness; (2) fighting against illegal content and 'harmful conduct' online; (3) promoting a safer Internet environment; and (4) establishing a knowledge base. Most of its allocated budged (48%) was for public awareness and only 34% was for tackling illegal and harmful content. The term harmful content was replaced by harmful conduct (for example cyberbullying and grooming) which may be a result of the unsuccessful use of online content filtering and rating systems at the user-level to tackle harmful content. The 2009 SIP also unified the work performed by the Internet hotline, help-line and awareness about children safety online into a single institution.

Overall EU policymaking encouraged domestic state regulation, promoted public awareness, and supported the work of Internet hotlines to limit access to child pornographic content across Europe. The creation of hotlines to report the availability of child pornography and other controversial online content started in the mid-1990s. For example, the British IWF[394] was created in 1996 and was followed by similar organisations across Europe.[395] There has been a European network of hotlines since 1999.[396] The idea of one network of Internet hotlines was suggested by the UK NGO Childnet International in 1997. Later, the initiative was funded via the DAPHNE Programme and established as a Dutch company in November 1999 and called the INHOPE Forum. INHOPE was created to provide support to Internet hotlines in Europe and beyond, encourage the exchange of expertise and technical reports, and also inform policymakers. It was designed to provide Internet hotlines with a fast channel to remove alleged child pornographic material hosted overseas where there was another affiliate member in operation.

8.3.3 Criminal liability of online intermediaries

Domestic state regulation was employed to regulate online intermediaries and establish their legal liability in relation to child pornographic material. This was the case not only in domestic jurisdictions such as Australia[397] and Brazil,[398] but across jurisdictions such as the EU. For

---

[393] Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a muitiannual Community programme on protecting children using the Internet and other communication technologies. (2008). Strasbourg at <http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm> .

[394] See IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 21 March 2010.

[395] See INHOPE's webpage for a list of Internet hotlines operating in Europe. INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010.

[396] The INHOPE Association started in 1999 with 08 members, but it reported 38 members in 2010. See Ibid.

[397] Broadcasting Services Amendment (Online Services) Act 1999 (Cth Australia).

[398] See Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil).

example, the 2000 EU Directive on Electronic Commerce established the legal liability of online intermediaries located in Europe for the content they hosted or distributed.[399]

For Edwards, the European ISPs were in a difficult position during the late 1990s, because of potential legal liability of the content they transmitted and hosted. Against this background they demanded exemption from strict legal liability based on three main arguments: the lack of effective legal and actual control over the content; that they were mere intermediaries; and for economic survival. This set the context where the legal framework for the legal liability of online intermediaries in Europe was established in 2000.[400]

The 2000 EU Directive defined online intermediaries as information society service providers but also call them intermediary service providers. As such, online intermediaries included a wide range of private actors such as Internet service, content and host providers, weblogs, search tools, social networking systems, and backbone providers. The 2000 EU Directive established the safe harbour regime, meaning that online intermediaries are exempt from legal liability so long as they cooperate when asked to do so, and the NTD approach in relation to criminal content.

When one online intermediary operated as a (1) 'mere conduit' of content, they were basically exempted from all liability. Nevertheless, if it operated as a (2) 'content host':[401] (a) it was exempt from civil liability if it had no 'actual knowledge' of the illegal activity and was not 'aware of facts and circumstances from which the illegal activity or information was apparent'; and (b) it was exempt from criminal liability if it had no actual knowledge. Generally they were not required to actively seek this knowledge via proactive monitoring of content but would become liable if they did not act expeditiously to remove the content reported after notification. Nevertheless, Walden has stressed that the increased production of user-generated content and the availability of filtering systems may push online intermediaries to exercise more editorial control over the online content to avoid the risk of litigation.[402]

The context where online intermediaries operated changed and it became more difficult to demand exemption from legal liability as it was the case around the late 1990s. Indeed, there are cheaper technologies of online content control, the cost of surveillance is decreasing and the implementation of these regulatory technologies did not undermine the economic survival of online intermediaries after all.[403]

---

[399] EU Directive on Electronic Commerce 2000 (DIRECTIVE 2000/31/EC, 08 June 2000).

[400] Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88, p 58.

[401] Storing and hosting content more than transiently. See articles 14(1)A and 14(1)B of the EU Directive on Electronic Commerce 2000 (DIRECTIVE 2000/31/EC, 08 June 2000).

[402] See Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62, p 458.

[403] See *e.g.* Edwards, L., 'Role and Responsibility of Internet Intermediaires in the Field of Copyright and Related Rights', (Geneve: WIPO, 2011) at <http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf>, accessed 28 December 2011.

8.3.4 Architecture-based regulatory tools

A number of architecture-based regulatory tools were employed to limit access to child pornography on the Internet. These included content filtering and blocking systems, tethered appliances, and the use of surveillance equipment for interception and analysis of data trafficking.

The problematic removal of child pornographic content hosted overseas challenged the effectiveness of state, multi-state and self-regulation. Although there was state regulation in place to remove alleged child pornographic material hosted within the jurisdiction, the relevant content was also hosted overseas and therefore still accessible from within the jurisdiction. This led to the implementation of content blocking systems to limit access to child pornography hosted overseas. Blocking systems were employed in a number of countries and applied to different online applications (for example, websites, e-mail, spam, newsgroups, peer-to-peer networks, search engines and Internet messaging).[404]

For Quayle *et al*., although online blocking is not the definitive solution to stop people sexually abusing children, '[…] at least this initiative contributes to an overall solution.'[405] Similarly, the IWF argues that although the removal at the source is the most effective way to tackle the availability of child pornographic content hosted overseas, they '[…] consider blocking to be a short-term disruption tactic which can help protect users from stumbling across these images, whilst processes to have them removed are instigated […]'.[406]

The use of website blocking against alleged child pornographic websites has been employed by the IWF since 2004 and became law within the EU in 2011. The mandatory blocking of overseas websites hosting alleged child pornography was never included within the EU policymaking, but in a change of policy the 2009 EC Proposal for a Council Framework Decision established in Article 18, the use of website blocking to stop access to child pornography.[407] After the entry into force of the Lisbon Treaty, this was replaced with the 2010 Proposal for a Directive[408] and the original 2009 text was slightly altered so as to remove any

---

[404] Callanan, C., et al., 'Internet blocking: balancing cybercrime responses in democratic societies', (Dublin: Open Society Institute, 2009) at <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf>, accessed 29 December 2011; Eneman, M., 'A Critical Study of ISP Filtering of Child Pornography' *European Conference on Information Systems. Paper 209* (2006); <http://is2.lse.ac.uk/asp/aspecis/20060154.pdf> accessed 29 December 2011.

[405] Quayle, E., Loof, L., and Palmer, T., 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the III World Congress against Sexual Exploitation of Children and Adolescents', (Bangkok: ECPAT International, 2008) at <http://www.childcentre.info/public/Thematic_Paper_ICTPsy_ENG.pdf>, accessed 09 June 2010, p 99.

[406] IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 21 March 2010.

[407] Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA. 2009 (Brussels).

[408] 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 (COM(2010)94 final), 29 March 2010 (Brussels).

reference to police and judicial authorities undertaking blocking of Internet pages.[409] The 2010 Proposal was enacted in December 2011 and established in Article 25(1) and (2) that EU member states shall take necessary measures to obtain removal of child pornographic webpages hosted outside of their territory and may take measures to block access to webpages containing or disseminating child pornography towards Internet users within their territory.[410]

Generally the EU established that the use of online content blocking strategies was at the discretion of each member state and generally not encouraged explicitly. Nevertheless, the EU seems to have adopted a more prescriptive role in this regard and the use of blocking systems to limit access to online child pornography has increased in the EU since 2006. For McIntyre, the 2003 SIAP Evaluation,[411] the increased number of overseas illegal websites reported, the existence of blocking systems already operating in a number of member states and the alignment of domestic anti-child pornography laws were reasons for this change in EU policymaking.[412]

Indeed, website blocking carried out in the United Kingdom[413] and Norway provided the empirical evidence for other trials across Europe. European police-led initiatives funded by the EU like CIRCAMP[414] also implemented website blocking systems as a preventive strategy. The CIRCAMP (COSPOL Internet Related Child Abuse Material Project) is a police initiative from COSPOL[415] funded under the 2005 Safer Internet Plus Programme that employed the 'child abuse anti-distribution filter' to block access to child pornographic content hosted in overseas websites. These initiatives showed the increasing acceptance of website blocking mechanisms to limit access to child pornographic content in Europe.

More recently, the policies of NTD for material hosted domestically and of website blocking for overseas websites became legally required in all 27 member states of the EU. The 2011 EU Directive on child abuse, child sexual exploitation and child pornography mentioned earlier

---

[409] For McIntyre, this is to avoid legislation being enacted and thus facilitates the use of self-regulatory blocking practices. See McIntyre, T., 'Blocking child pornography on the Internet: European Union developments', *International Review of Law, Computers and Technology,* 24(3) (2010), 209-21, p 217-8.

[410] See Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union).

[411] 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Final evaluation of the implementation of the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Brussels, 06.11.2006, COM(2006) 663 final.', 2006) .

[412] See McIntyre, T., 'Blocking child pornography on the Internet: European Union developments', *International Review of Law, Computers and Technology,* 24(3) (2010), 209-21.

[413] From 1996 to 2002, the British IWF operated under the notice and take down scheme. In 2002, a controversial ban on USENET Newsgroups was implemented. In June 2004, they put into operation the BT Cleanfeed to block access to URLs allegedly hosting child pornographic content. See Chapter 7 about online child pornography regulation in the United Kingdom.

[414] See CIRCAMP, 'Cospol Internet Related Child Abusive Material Project', at <http://circamp.eu>, accessed 30 June 2010.

[415] COSPOL is an European law enforcement network created in 2004 that amongst other things aims to improve the law enforcement cooperation in the EU against the commercial sexual exploitation of children. See EUROPOL, 'CIRCAMP - COSPOL Internet Related Child Abusive Material Project', at <http://www.europol.europa.eu/index.asp?page=InternetRelatedChildAbusiveMaterialProject>, accessed 05 August 2010.

established a uniform law in relation to limiting access to and blocking websites with alleged child pornographic content across Europe. Article 5(3) about the offences concerning child pornography established that ' […] knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year […].' According to Article 25(1) and (2):

> 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 […].[416]

There were a number of safeguards in Article 25(2) in relation to the implementation of the website blocking schemes by the EU member states. For Carr, the 2011 EU Directive raised a number of issues around the role Internet hotlines and particularly the INHOPE in Europe in relation to NTD (domestically) and website blocking (overseas) of child pornographic material.[417]

In Australia, there has been a website blocking voluntary scheme at the ISP-level to limit access to child pornography in operation since July 2011.[418] In the US, there was an unsuccessful legislative attempt in the State of Pennsylvania to require ISPs to block access to websites allegedly hosting child pornography,[419] but this was achieved in the State of New York via agreements negotiated between the attorney general and major ISPs (for example Vernon, Sprint and Time Warner Cable) to prohibit access to newsgroups allegedly hosting child pornography related content.[420]

In addition to website blocking, hardware and software were employed to monitor and analyse the traffic on the Internet in relation to controversial content including child pornography. For example, Carnivore was a system designed by the US Federal Bureau of Investigation to monitor e-mails and electronic communications in the US. It changed its name to DCS1000 and was abandoned in 2001 in favour of a commercial piece of software.[421] More importantly, the National Security Agency (NSA) developed a surveillance scheme involving a massive

---

[416] See Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union).

[417] Carr, J., 'Hotlines and INHOPE: time to take stock?', *Desiderata* (2012) at <http://johnc1912.wordpress.com/2012/03/02/hotlines-and-inhope-time-to-take-stock-2/> Accessed 22 March 2012.

[418] See Chapter 4 about the regulation of online child pornography in Australia.

[419] See 'Summary and Highlights of the Philadelphia Federal District Court's Decision: CDT v. Pappert, Case No. 03-5051 (E.D. Pa. Sept. 10 2004)', (Washington, DC: Center for Democracy and Technology, 2004) at <http://www.cdt.org/speech/pennwebblock/20040915highlights.pdf>, accessed 11 April 2011.

[420] These major ISPs were 'asked' to sign Codes of Conduct. See 'Attorney General Cuomo takes legal action against social networking site that ignores proliferation of child pornography', (New York, NY: Office of the Attorney General, 2008) at <http://www.ag.ny.gov/media_center/2010/june10b_10.html> Accessed 11 April 2011; Kravets, D., 'Communications Decency Act Tipping Under Cuomo Kid-Porn Accord', *Wired,* 2008, sec. Threat Level at <http://www.wired.com/threatlevel/2008/06/analysis-commun/>, accessed 28 December 2011.

[421] See <http://en.wikipedia.org/wiki/Carnivore_(software)>, accessed 11 August 2010.

datacenter able to intercept, store and analyse online communications from around the world.[422] The EU Project MAPAP targeted the exchange of child pornographic content via P2P networks and received funding under the EU Safer Internet Action Plan. Another example of architecture based regulatory strategy is the so-called Deep Packet Inspection (DPI). This technique accessed not only the header, but the content of the data being distributed and it was used in a wide range of areas for surveillance and censorship purposes. Software for automated analysis of images were created and used by online intermediaries to prevent users uploading alleged child pornographic content to their networks.[423]

In England and Wales, the 2000 RIPA[424] established a number of provisions to facilitate the collection of evidence and surveillance on the Internet. A warrant could be issued by the executive (not the judiciary) and the RIPA also demanded that the ISPs maintained real-time interception capabilities to facilitate monitoring. In addition, it is argued elsewhere that its strict provisions about encryption and access to encrypted information may have violated the presumption of innocence, undermined the privilege from self-incrimination, and inverted the burden of proof.[425] The UK government announced plans to expand the existing surveillance powers of law enforcement authorities.[426]

Regulation of online child pornography was performed not only via online intermediaries, but at the user-level via tethered digital devices such as mobile phones and tablets.[427] The internal configuration of these devices may be altered and prompted from afar and subject to instantaneous revision: this made surveillance and content control much easier to perform.[428]

For example, the US company Apple had the intention to keep its products porn-free[429] and enforced strict regulatory rules against pornography on the applications developed for its tethered devices.[430] This was known as the Apple's walled garden. These devices could be unlocked with the special software but this was considered a breach of the terms of use and may have voided the warranty.[431] It is also worth pointing out that such special software is developed

---

[422] Bamford, J., 'The Black Box', *Wired Magazine*, April (2012) at <http://www.wired.com> accessed 03 April 2012.

[423] Carr, J., 'Microsoft attacks online child pornography', *Desiderata* (2011) at <http://johnc1912.wordpress.com/2011/07/05/microsoft-attacks-online-child-pornography-3/> Accessed 28 December 2011.

[424] Regulation of Investigatory Powers Act (c.23) 2000 (England and Wales).

[425] Edwards, L., Rauhofer, J., and Yar, M., 'Recent developments in UK cybercrime law', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 413-36, p 424 and 427.

[426] Syal, R., Halliday, J., and Siddique, H., 'Theresa May defends email surveillance plans', *The Gardian,* 04 April 2012, sec. UK Police at <http://www.guardian.co.uk/uk/2012/apr/03/theresa-may-email-surveillance-plans>, accessed 04 April 2012.

[427] The issue of regulation via tethered appliances was discussed above in Section 3.3.

[428] Zittrain, J., 'Perfect Enforcement on Tomorrow's Internet', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008), p 132.

[429] Arthur, C., 'I want the iPad porn-free, says Apple's Steve Jobs: Apps for the new iPad have had to self-censor ', *The Guardian,* Tuesday 25 May 2010 2010 .

[430] See APPLE, 'Registered Apple Developer Agreement', (2010) .

[431] Halliday, J., 'JailbreakMe released for Apple devices', *Guardian Technology Blog* (2010) at <http://www.guardian.co.uk/technology/blog/2010/aug/02/jailbreakme-released-apple-devices-legal> Accessed 12 August 2010.

by hacker communities and are hard to find and use. In some cases, breaking digital locks was against the law even if no copyright infringement was committed.[432] Similarly, some governments like United Arab Emirates, India, Saudi Arabia and China threatened to ban Blackberry mobile phones applications, because these devices allegedly used the manufacture's own encrypted network to transmit data and were therefore able to circumvent state regulation.[433]

9 Employing evaluative criteria for assessing hybrid regulation of online child pornography in Australia, Brazil and the United Kingdom

The second part of this chapter presented the problem of child pornography on the Internet and explored relevant regulatory measures in the area taking into account the typology of regulatory models developed in Section 1.2: self-regulation; state and multi-state regulation; and hybrid regulation. In addition, it showed how the digitisation of content, anonymised access, and multi-jurisdictional nature of the Internet challenged the enforcement of laws and regulations against online child pornography. This led to updates and expansion of anti-child pornography laws across the world and also to a number of hybrid regulatory measures involving both state and private actors.

These measures include increased investigatory and surveillance powers of law enforcement authorities, more liability imposed on the online intermediaries, financing of initiatives, *e.g.* creation of Internet hotlines and implementation of filtering strategies, use of architecture-based regulatory strategies, and international cooperation of policing. The rationales driving this regulatory expansion are not only motivated by economic reasons but also by human rights concerns. Such rationales include: (i) the amplified dimension of perceived harms; (ii) the new venues where child abuse can be performed whether against a real or a fictitious child; and (iii) institutional agendas geared by symbolic politics (*i.e.* something has to be done about it whether it is effective or not), moral entrepreneurs, media-made criminality, prospects of financial gains and survival (for example, by Internet hotlines, politicians, and software and hardware companies), and also a legitimate interest to protect children against abuse. Indeed, these agendas were successful to justify the expansion of anti-child pornography laws and regulations for the online environment.

Many critics have argued that regulation of child pornography should focus on the primary abuse of children and international cooperation. As such, less emphasis should be put on the circulation of online material, because it is costly, ineffective and it deflects attention from more important issues. This chapter showed however that such 'hands-off' rhetoric in relation to

---

[432] See Digital Millennium Copyright Act 1988 (17 USC § 512 (g)) (USA).

[433] Generally see Zittrain, J., 'BlackBerry-22', *The Future of the Internet and How to Stop It* (2010) at <http://futureoftheinternet.org/blackberry-22> Accessed 12 August 2010.

state involvement in the Internet has been defeated: the regulation of child pornography available online is increasing.

Yet, this regulatory escalation raises a number of questions. Do these hybrid regulatory policies designed to limit access to child pornographic material available on the Internet represent a threat to free speech, privacy and other democratic values? Do these concerns hold cross-nationally? Are there any safeguards in place? Is hybrid regulation employed in similar ways across different jurisdictions? Are these strategies converging towards a single universal model? What are the mechanics and administrative constraints of these policies? Who is bearing the financial costs to implement these regulatory measures? Are these policies efficient and effective? In order to address these questions, this research will employ the evaluative criteria designed above against current regulatory policies in Australia, Brazil and the United Kingdom.

It seems that most concerns highlighted in the literature hold true but many others are not substantiated by evidence. For example, it may be the case that the actual regulatory mechanisms put in place are far less threatening to free speech and privacy than trumpeted by the literature. The actual implementation of anti-child pornography regulations may be only symbolic politics in the sense that online child pornography is not a top regulatory priority in daily police routines when compared to the regulation of property and financial related online crimes. In addition, although regulatory measures, for example notices of take down and blocking of websites have been considered 'successful' strategies, these have only little effect in limiting access to child pornographic content available online, because people are able to exchange such content via non-web channels and platforms. In other words, these policies may be displacing crime to more resilient channels.[434]

In addition, Section 6 onwards shows the relevance that the control of online child pornography has for the regulation, governance and criminology literature. This is a problem that concerns a number of researches in these areas, and makes evident the need to articulate ideas and concepts from each field in order to develop policies that not only work in practice but protects free speech and privacy. Many of these ideas and concepts were covered here to explain the phenomenon of online child pornography regulation from different perspectives, and will be referenced in the following chapters.

Against this background, Chapter 4 will explore in detail the laws and regulations for limiting access to online child pornographic material in Australia, Brazil and the United Kingdom, and Chapter 5 will apply the evaluative criteria described above so as to produce a report on each jurisdiction for each criteria. These jurisdictions were chosen because, although they have

[434] There is evidence to suggest that child pornography is exchanged via P2P networks. See for example Latapy, M., 'Measurement and Analysis of P2P Activity Against Paedophile Content', at <http://antipaedo.lip6.fr/>, accessed 14 March 2012.

reasonably similar anti-child pornography laws, they have crucially different approaches to the constitutional framework, scope and mechanics of anti-online child pornography regulations.[435]

The next chapter will explore methodological and ethical issues involved in this investigation before the case study material is addressed in Chapter 4.

[435] The reasons for the choice of jurisdictions will be explored in detail in Chapter 3.

CHAPTER 3: METHODOLOGY

1 Introduction

Chapter 2 explored the academic literature about regulation and the problematic enforcement of regulatory measures to control controversial material available on the Internet. It classified regulatory interventions into three categories according to relevant regulatory actors involved: (1) self-regulation; (2) state and multi-state regulation; and (3) hybrid regulation. Chapter 2 also highlighted the negative consequences of hybrid regulation and developed evaluative criteria to assess such consequences. Subsequently, it explained the problem of child pornography and addressed the self-, state and multi-state, and hybrid regulatory initiatives to limit access to child pornographic material available on the Internet.

This research employs the evaluative criteria developed in Chapter 2 against current regulatory models limiting access to child pornographic material on the Internet in three different jurisdictions to evaluate the implications of hybrid regulation for free speech, privacy and democracy in the online environment. The problem of child pornography was chosen because, in this area, regulatory measures have advanced faster and relatively unopposed in comparison to the regulation of other types of controversial material. For example, in Brazil, although the cybercrime and online intermediaries' regulation bills were under parliamentary discussion, a number of agreements, pro-active content monitoring performed by private actors and specific legislation placing criminal liability on online intermediaries, only in relation to child pornographic content, are already in place. In the United Kingdom, although only recently courts required ISPs to block access to URLs allegedly violating intellectual property rights,[436] URL blocking of alleged child pornographic content has been in operation since 2004. In Australia, blocking of alleged child pornography websites has already been employed voluntarily at the ISP-level, whereas the regulation of other violent material available online was pursued via user-level voluntary filtering.

This investigation analysed comparatively the Australian, Brazilian and the UK regulatory models and it was based on documentary evidence and unstructured interviews employed under a multiple-case study strategy. Australia, Brazil and the United Kingdom were chosen as case studies because they had generally similar anti-child-pornography laws, both domestically and in terms of their commitments under international treaties, they were considered democratic countries subject to democratic controls of content, and access to data was relatively unproblematic in these jurisdictions. This provided a common ground for comparison.

[436] Halliday, J., 'British ISPs will block The Pirate Bay within weeks', *The Guardian,* 30 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/30/british-isps-block-pirate-bay>, accessed 01 May 2012.

Of course, this common ground for comparison is open to debate. Australia, Brazil and the United Kingdom[437] have different legal systems in relation to the application of criminal laws, different degrees of autonomy amongst levels of government (*e.g.* federal, state and territories), and varied powers given to law enforcement agencies. However, they share a substantial number of similar anti-online child pornography criminal provisions in terms of criminal conducts, types of content and sentencing. They also share the will to regulate child pornographic material available on the Internet. More importantly, they were chosen as case studies because despite so different constitutional frameworks and varied regulatory scope and mechanics, they all settled on similar approaches and rationales to child pornography regulation. This provided an opportunity to explore different aspects and variations of hybrid regulation, and also to address its broader implications for free speech, privacy and democracy on the Internet.[438]

This study is important for at least three key reasons. These include: (1) policymaking; (2) legal, criminological and regulatory scholarship; (3) and new case study evidence of how regulation works in practice.

First, the analysis developed here is expected to help reform current policymaking in relation to access to online child pornography, a field that is growing in importance across the world.[439] It also identifies a range of potential threats from anti-online child pornography regulation, developed cross-national evaluative model and a scheme of safeguards, and explores the regulatory costs involved. These have further practical utility as a guide for policymaking in relation to regulation designed to limit access to child pornographic material available online. The academic literature about Internet regulation was explored and tested out against the evidence from case studies, including the potential implications of hybrid regulation, the use of decentred and polycentric theories of regulation, the assessment of apparent illegality of online material by private actors, the cross-national similarities and differences of regulatory and institutional arrangements, and the problematic implementation of such measures.

Second, it has implications for criminological scholarship, particularly in the field of comparative criminology and social control, because it addresses responses to crime that depend on international mutual efforts and occur within a decentred regulatory framework.[440] It deals with crime and social control in a modern society where the governance of security and order

---

[437] The legislation analysed was of England and Wales.

[438] The reasons for choosing Australia, Brazil and the United Kingdom will be discussed in detail in Section 5 below.

[439] See *e.g.* Articles 5(3) and 25 of the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union) that requires all EU member states to criminalise the knowingly access to online child pornography and, more importantly, to take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territories.

[440] See Chapters 2 and 3 for a discussion about the multi-jurisdictional challenges posed by the Internet.

has been rapidly and radically transformed.[441] It addresses the evolution of anti-online child pornography laws, the resilient nature of the Internet and displacement of cybercrime, and the regulatory rationales used to criminalise a number of conducts and material associated with child pornography. Furthermore, it shows the enforcement of existing frameworks to be problematic (for example, in relation to criminal content regulation) because of the resilient and multi-jurisdictional nature of the Internet and it suggests that more flexible regulatory approaches and robust safeguards have the potential to resolve something of these issues.

Third, this research explores the evolution of anti-child pornography laws and regulations in Brazil, where little academic information is available. It shows that not only regulation of online content based on agreements are problematic for free speech, privacy protection and good regulation but it also provides a starting point for further research in the field.

Although most regulatory policies addressed in detail here (NTD and website blocking) target child pornographic material available on the world wide web (WWW), this investigation does not restrict its scope to web-based child pornographic material. Instead, it takes into account that other means of distribution and access exist such as anonymised P2P, FTP, real-time chat systems, and darknet. This choice was made to: (1) explore other avenues of regulatory intervention (particularly within the remit of law enforcement authorities) that had a deterrent effect in limiting access to online child pornography; and (2) show how access to child pornography was displaced to less regulated online environments once NTD and website blocking policies were in place.

The problem of child pornography available on the Internet involves not only the production but the distribution of, and the access to, child pornographic material. Each activity involves a number of features and is subject to multiple regulatory responses. The production and distribution of child pornography on the Internet are addressed only peripherally in this investigation because they are not the focus of this research; this study focuses on the regulatory measures designed to limit access to child pornography available on the Internet.

Although the focus is on regulations to limit access to online child pornography, this study also explores laws against child pornography *per se*, the criminal liability of intermediaries and surveillance powers of law enforcement authorities, and court cases in each jurisdiction in order to present the overall environment where these regulations operate. As such, it covers not only laws and regulations that directly aim to limit access to child pornography available online (for example, prohibition of knowingly access, and the use of NTD and blocking strategies) but those which indirectly inhibit or have a deterrent effect in such conduct (*e.g.* the prohibition of mere possession, production and distribution of child pornography, the facilitation of surveillance powers of law enforcement authorities, and the increased criminal liability of

[441] See *e.g.* Loader, I. and Sparks, R., 'Contemporary Landscapes of Crime, Order, and Control: governance, risk, and globalization', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (4rd edn.; Oxford: OUP, 2007), 78-101; Also see Braithwaite, J., 'The New Regulatory State and the Transformation of Criminology', *The British Journal of Criminology* 40 (2000), 222-38.

online intermediaries). Notably, the study of lawmaking, police operations, criminal prosecution, sentencing, convicted offenders and victims in relation to online child pornography offences are outside the scope of this research.

This chapter will explore the methodological and ethical issues choices made to conduct this investigation. First, the documentary analysis and the unstructured interviewing scheme will be addressed within the scope of a multiple-case study strategy. Subsequently, a few issues in relation to cross-national research and the professional involvement of this author with the research topic will be discussed.

2 Documentary analysis

For Atkinson and Coffey, if people need to understand organisations they cannot ignore documents, because institutions are deeply dependent on paperwork.[442] Indeed, documents are relevant to understand how both state and private actors regulate to limit access to child pornography available on the Internet. This is the reason why documents were the main research evidence of this study, and the documentary analysis was employed as a method of research on its own right rather than playing a secondary role.[443]

Generally, the documentary analysis employed here aimed to provide a detailed account of regulatory measures in place to limit access to online child pornography in all three chosen jurisdictions. It was expected to: (i) describe and explain the legal and regulatory frameworks in operation; (ii) highlight key similarities and differences amongst regulatory models; (iii) identify the implications of hybrid regulation for democratic legitimacy, transparency and accountability; (iv) inform the following unstructured interviewing scheme;[444] and (v) to validate the findings derived from interviews.[445]

Different types of documents were collected and analysed during this investigation. They were divided into three categories: (1) conventional legal sources (for example parliamentary bills, explanatory memorandums, statutes, cases and agreements); (2) institutional documents derived from state and private sources (*e.g.* public and private administrative documents and reports); and (3) academic literature. Mass-media outputs (*e.g.* newspaper and magazine articles,

---

[442] Atkinson, P. and Coffey, A., 'Analysing Documentary Realities', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 45-62.

[443] See Prior, L., 'Following Foucault's Footsteps: text and context in qualitative research', Ibid, 63-77; Atkinson, P. and Coffey, A., 'Analysing Documentary Realities', Ibid, 45-62.

[444] Some authors emphasise the role of documentary analysis in pre-interview preparation to refine questions and put answers into context as the interview progresses. See Moyser, G., 'Non-Standardized Interviewing in Elite Research', in Robert G. Burgess (ed.), *Studies in Qualitative Methodology: conducting qualitative research* (1; London: Jai Press, 1988), 109-36; Becker, H. S. and Geer, B., 'Participant Observation: The Analysis of Qualitative Data', in Robert G. Burgess (ed.), *Field Research: a sourcebook and field manual* (London: Unwin Hyman, 1982), 239-50; Mason, J., 'Qualitative Interviewing: asking, listening and interpreting', in Tim May (ed.), *Qualitative Research in Action* (London: Sage Publications, 2002), 225-41.

[445] Yin, R. K., *Case Study Research: Design and Methods* (4th edn.; Los Angeles: Sage, 2009).

television programmes, blogs and radio broadcasts) were considered but only as indicators of other documentary sources.[446]

Documentary collection and analysis followed a coding scheme designed to organise the documentary data according to relevant research questions and objectives.[447] Against this background, the coding scheme divided the documents collected into two categories: (1) documents related to anti-child pornography laws, and also legislation in relation to legal liability of online intermediaries and investigatory powers of law enforcement agencies; and (2) documents related to the overall online content regulatory framework. The size, scope and period of documentary sample varied according to the phenomenon's occurrence in each jurisdiction. For example, documents related to legal framework were dated 1990 to 2010 (Australia), 1990 to 2010 (Brazil) and 1978 to 2010 (United Kingdom); and documents related to regulatory framework were dated 1990 to 2010 (Australia), 1999 to 2010 (Brazil) and 1990 to 2010 (United Kingdom). Again, this coding system was in line with the enactment of domestic anti-child pornography laws and initial operation of regulatory measures in each jurisdiction.

Generally access to most documents was unproblematic, because they were publicly available online. Conventional legal documents were publicly available online in all three jurisdictions. Institutional documents were generally found online but more restricted documents were only available upon request. Academic literature was easily found in Australia and the UK when compared to Brazil, where only a few academic studies and reports were available.

Documentary analysis in legal research is associated with doctrinal research methods.[448] This approach to legal research is based on the assumption that law is a product of rules derived from cases and statutes which are applied by an impartial judge in order to resolve a dispute. As a result, analysis of legal problems is limited to the interpretation of cases and statutes, assuming an artificial separation between law and society. Some critics argue that although the doctrinal legal approach is able to provide a normative evaluation of law and its regulations, it fails to address the 'why' questions, institutional agendas, power struggles and the politics of regulation in relation to the phenomenon investigated.[449]

In contrast to doctrinal studies of law, socio-legal approaches to legal research incorporate the social context into legal analysis. According to these approaches, law and regulations are not only mere extensions of statutes, cases, and governmental documents but are social products shaped by different actors, and influenced by variables such as power struggles, ideological

---

[446] This was for two main reasons: media outputs would require a distinct method of content analysis; and media operators, albeit important actors for online child pornography regulation, were not within the scope of this investigation.

[447] See Appendix 4 for the coding schedule of the documentary analysis.

[448] See generally Aarnio, A., *Essays on the Doctrinal Study of Law* (London: Springer, 2011).

[449] See *e.g.* Fox, M. and Bell, C., *Learning Legal Skills* (3rd edn.; London: Blackstone Press Ltd., 1999), p 9; and also Banakar, R. and Travers, M., 'Law, Sociology and Method', in R. Banakar and M. Travers (eds.), *Theory and Method in Socio-Legal Research* (Oxford: Hart, 2005).

conflicts, gender, class and race. In short, the socio-legal analysis of law takes on board different voices left unheard by the doctrinal approach and may supplement it accordingly.

The documentary analysis (or doctrinal approach) has limitations. First, documentary evidence may reflect or disguise the institutional agendas where they are produced. They are not transparent windows of the world but create a particular version of reality that represents potential rather than actual meaning.[450] For Scott, they should be analysed as social constructs, as part of their social context of production, distribution and consumption, and interpreted according to their authenticity, credibility, representativeness and meaning.[451]

For example, civil rights organisations emphasise the drawbacks of regulation for the protection of civil liberties online; state regulators focus on the need of regulation to protect children, arrest offenders and maintain order; online content filtering manufacturers overemphasise the advantages of their products; and online intermediaries might advocate a 'hands-off government' approach to the Internet on privacy and free speech grounds, but in reality they are only reluctant to implement regulatory measures to avoid any additional operational expenses on their side. Generally each organisation produces documentary evidence that emphasises certain aspects that pushes their agendas forward, whereas issues that are against their interests are either underemphasised or suppressed entirely.

In addition, documents may provide contradictory information, and it is commonly the case that the law found in documents, *i.e.* the 'law in books', differs from the actual phenomenon under investigation, *i.e.* the 'law in action.' In other words, documents about legal and regulatory frameworks may provide information substantially different from the actual daily operation of institutions responsible for implementing these regulations in practice. Furthermore, access to a few relevant institutional documents could only be granted after email conversations or interviews, when participants get to know the researcher and develop a sense of trustworthiness. For example, in Brazil many relevant documents and other contextual issues were only acknowledged after interviews were conducted.

These issues became clear after data was collected and the analysis began. The documentary evidence was only able to answer certain questions (for example the scope and structure of relevant law and regulations, the detailed practical information about how the regulatory scheme works, the potential negative implications of regulatory measures) and only peripherally could answer other questions such as the reasons why certain regulatory measures were preferred, and the agenda of institutional actors. In sum, there are wider social questions that documents, or the doctrinal approach, may be unable to answer. As a result, it is important to establish the research

---

[450] Watson, R., 'Ethnomethodology and Textual Analysis', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 80-97; Bauer, M. W., 'Analytic Approaches for Text, Image and Sound', in Martin W. Bauer and George Gaskell (eds.), *Qualitative Researching with Text, Image and Sound: a practical handbook* (London: Sage Publications, 2000), 131-51.

[451] For a discussion about these criteria see Scott, J., *A matter of record: documentary sources in social research* (Cambridge: Polity, 1990).

question in advance bearing in mind the limits of documentary analysis, and if necessary, include other research methods such as questionnaires, interviews or participant observation, to achieve what the research aims.

This investigation was only peripherally interested in conflictual institutional agendas, whether within or outside the organisation, political power struggles, or other issues around gender, race and ideological conflicts. Although these were interesting research topics on their own right and were briefly discussed in this study, this investigation was designed to address the regulation of access to online child pornography to evaluate the implications of hybrid regulation for free speech, privacy and democracy in the online environment. And, in this regard, the documentary evidence fulfilled its role.

In order to tackle some limitations of documentary analysis, this investigation employed a validation scheme, and this will be explored below.

3 Validation scheme for the documentary analysis: an expert consultation exercise

The documentary analysis explored and explained each regulatory model in detail, including anti-child pornography criminal laws, relevant legislation about regulation of online intermediaries and investigatory powers of law enforcement authorities as well as online content regulations, historical context, key actors, regulatory mechanics and scope, which constitute the case study material found in Chapter 4. Again, the documentary analysis explored relevant official documents from each jurisdiction, including conventional legal sources and institutional documents. A number of academic articles and media articles were also included, and the coding strategy was designed to identify the legal and regulatory frameworks from each jurisdiction.

After draft chapters were finished, a validation exercise was conducted. The validation scheme was based on an expert consultation exercise and aimed to: (1) resolve any contradictions found in the documentary analysis; (2) explain some policymaking decisions not found in documents; (3) obtain more documents and follow other relevant leads; (4) correct errors and omissions; and (5) minimise the cultural misunderstandings derived from a cross-national investigation.

Potential participants were chosen from a range of different backgrounds such as academia, civil service and non-governmental, and were specialists in the topic capable of validating the documentary evidence collected. The participation process followed ethical guidelines established by the Research Ethics Committee of the University of Sheffield, and the potential participants were invited and approached via email, telephone or both.[452] According to these guidelines, (i) participants were able to choose to be identified or not; (ii) responses were to be

[452] See Appendix 2 for a copy of the invitation letter.

kept confidential, unless permission was given; (iii) a consent form was provided to inform participants about the research and their participation. During the invitation process, all relevant information (*i.e.* explanatory statement, consent forms, and confidentiality agreement) were provided to potential participants. Eighteen people were approached this way. Six participants agreed to provide feedback on each relevant draft chapter: two experts from Australia; one from Brazil; and three from the United Kingdom. Subsequently, each draft chapter (all in English) was submitted for feedback via email to the expert according to his/her jurisdiction.

The invitations were sent around late November 2011 and five written feedbacks were received by February 2012. After the feedback was received, it was briefly discussed with the participant via email, whenever necessary. In addition, follow-up interviews were conducted with the Brazilian expert. These interviews were unstructured so as to include the participant's understanding of the problem and be flexible enough to reveal issues neglected in the documentary analysis. This research method will be discussed further in Section 4 below.

Eighteen people were invited to participate in this research but only six took part in the consultation exercise. Ten people agreed to participate initially, but four of them did not reply after the relevant information was sent, and they gave no reasons for this. Some respondents were concerned about the confidentiality agreement and made clear that the contribution would be of their own and not of the institution they were associated with, perhaps to avoid any potential conflict of interest. In other situations, social skills were needed to build up trust and convince participants to accept the invitation.

After this feedback was received and analysed, a number of changes were made in each case study chapter. Of course, all changes were made according to my own judgment and based on previous documentary analysis. Feedback received was in written text format (five altogether), except in the Brazilian case, where the participant provided feedback via unstructured interviews.

Most changes in the Australian case study were about omissions, minor errors and misunderstandings of Australian legislation, particularly, because of complex constitutional arrangements asserting powers to the Commonwealth, States and Territories in terms of criminal laws and content regulation. A few historical events were added to the revised version, and a number of websites and official documents were recommended for reading. A number of important details were added in relation to most recent ISP-level voluntary website blocking scheme. In addition, there were invitations for further reading and thinking in a few occasions when the expert disagreed with my point of view.

The Brazilian case study underwent a substantial change in content. Perhaps, this was because there were only a few academic works available about child pornography regulation in Brazil, and accounts about key discussions and decisions on the topic were not publicly easily available. In addition, the Brazilian expert was able to provide long and detailed feedback on the

draft chapter. Many omissions, errors and misunderstandings were found; a number of gaps in the historical development of regulatory measures were filled; the expert invited me to do more reading and thinking about my prior point of view whenever s/he disagreed; and a number of documents and websites were recommended for reading. Perhaps because of the substantial amount of information unintentionally neglected during the documentary analysis, most considerations made by the expert were taken into account, but again, these changes were made after consulting documents in order to validate the feedback given.

The feedback given by the Brazilian expert was given under an unstructured approach and conducted via the software Skype; these interviews amount to about 10 hours of conversation. The structure of the Brazilian case study chapter remained generally the same after the validation, but it was enriched with more information and initial criticisms had softened in some parts; this is because the information gathered during the validation process changed the understanding of a few particular issues. A number of issues neglected during the documentary analysis were taken onboard. For example, the reluctance of online intermediaries to implement regulatory measures because of operational costs and political struggles occurring behind the scenes were information not available on documents. On a few occasions, the expert criticised my point of view but this was largely because of the institutional agenda s/he pursued. Whenever any change was made to the original draft chapter, this was either based on new documents initially neglected, or on a new reading of a document already read during the documentary analysis.

The feedback about the United Kingdom case study was relatively less extensive when compared to the other two case studies, perhaps because of the wide range of academic work already available on the subject. The responses were generally punctual and in relation to minor errors and omissions, particularly, about legislation, interpretation of key court decisions and actual operation of the regulatory scheme. Few important documents were suggested for further reading, particularly a recently enacted piece of legislation. There were however invitations to rethink my views on the controversial Wikipedia incident, to soften the criticism on the URL blocking scheme managed by the IWF and to put other criticisms under a wider perspective. In fact, this was more like an invitation for discussion rather than a straightforward request to change my point of view about these issues.

Overall, the expert consultation exercise was able to (i) correct minor mistakes, errors and omissions of draft chapters; (ii) include other relevant documents in the analysis; (iii) either support or soften the criticisms made in the draft chapters; and (iv) minimise potential misunderstandings derived from cultural differences and language misinterpretations.[453] The consultation exercise can be compared to a peer review prior to a publication on a journal: improvements are made to draft papers without interfering substantially on the author's point of view and the gist of argument advanced. After the consultation process was finished, one can

[453] For a discussion about problems of cross-national research, see Section 5 below.

safely say that the reviewed chapters are valid accounts about how online child pornography regulation was addressed in each jurisdiction.

This consultation process was a relatively easy, fast and cheap method to validate the documentary evidence. Of course, it depended on the generosity of experts, who contributed with their time and intellectual effort towards the research. Another advantage is that it can be conducted at a distance, whether via e-mail or Internet telephony, and thus reach people in other jurisdictions. In addition, it is a chance to test out the issues highlighted in the academic literature and the researcher's own perspectives on a particular subject. It is an opportunity to include other issues and concerns omitted in the literature but which are important to take on board.

Nevertheless, this sort of validation exercise is not recommended when institutional immersion is necessary, *e.g.* when the research question demands methods such as participant observation over a period of time. The researcher must critically approach the recommendations made by experts, and understand in advance the potential agendas they may be pursuing. More importantly, the experts' considerations must always be contrasted with the documentary evidence available.

Finally, the validation scheme opened a window of opportunity for experts to impose their visions and agendas onto the research. In addition to a number of errors and misunderstandings being promptly corrected, and new references being included, in a few cases the participants disagreed with the tone or approach taken to a particular problem and tended to push their own agenda and understanding. Although these interventions were often thought-provoking and improved the analysis, they were taken with care and explored further via email discussions and documentary analysis.

4 Unstructured interviewing scheme

The documentary analysis was sufficient to describe and explain the legal and regulatory frameworks as well as the regulatory mechanisms operating in each jurisdiction. This technique was able to answer the research questions of this investigation. Nevertheless, the draft chapter about Brazil was initially considered rather unsatisfactory because of too few documents collected. This was the reason why unstructured interviews were conducted.[454] These interviews aimed to: (1) explain further issues from the expert's feedback; (2) explore decisionmaking processes relevant to the research question; and (3) explore in more depth the experts's own understanding of the problem.

[454] Unstructured interviews are more time demanding and costly when compared to other interviewing techniques, but the small size of the sample used in this investigation made this possible under the resources available.

The academic literature stresses that although there are a number of ways to collect information from participants such as questionnaires and structured interviews,[455] unstructured interviews are more appropriate to observe respondent's workplace environment, perceive things like body language and clarify inconsistent information immediately, instead of assuming that the respondent's reality would fit a prior theoretical scheme.[456] Accordingly interviewees are expected to construct rather than reveal something; they act as collaborative partners in the process of knowledge construction instead of being considered vessels of answers.[457] Interviewees and interviewer are expected to actively interact so as to weaken the dominant role of the latter and the degree of procedural reactivity. As such, the interview was guided not by a rigid list of questions, but by the draft chapter about the Brazilian case study and the coding scheme found in Appendix 4; the expert was also free to follow other issues. The interview, albeit flexible and unstructured, was controlled.[458]

The unstructured interviews employed for this research involved only the Brazilian expert (who took part in the validation scheme. They were qualitative-oriented, based on the Brazilian draft chapter and coding schedule, and conducted only in relation to the Brazilian case study, because the draft chapter was considered only partially satisfactory, and therefore a substantial number of extra readings and amendments were necessary.

These interviews were conducted via the Internet telephony software Skype and digitally recorded after the participant gave informed consent.[459] They were then transcribed and the audio destroyed. Personal identifiers were not collected from the interviewee. A coding system was used to avoid using the interviewee's name within the transcribed text and as filenames. The audio digital record was encrypted and stored in a password protected personal computer. Later, the digital audio was transcribed and then destroyed. The transcribed data (digital text) was printed and kept in a locked cabinet. In sum, (i) the participant was able to choose to be identified or not; (ii) responses were kept confidential; (iii) audio recordings were destroyed after transcription; (iv) a consent form was provided before the interview in order to inform the participant about the research and his/her participation.

---

[455] See a range of research methods available in Bryman, A., *Social Research Methods* (3rd edn.; Oxford: OUP, 2008).

[456] Gerson, K. and Horowitz, R., 'Observation and Interviewing', in Tim May (ed.), *Qualitative Research in Action* (London: Sage Publications, 2002), 199-224; Mason, J., 'Qualitative Interviewing: asking, listening and interpreting', Ibid, 225-41.

[457] Atkinson, P. and Silverman, D., 'Kundera's Immortality: The Interview Society and the Invention of the Self', *Qualitative Inquiry,* 3(3) (1997), 303-25; Holstein, J. A. and Gubrium, J. F., *The active interview* (Qualitative research methods; Thousand Oaks, Calif. ; London: Sage, 1995).

[458] Becker, H. S. and Geer, B., 'Participant Observation: The Analysis of Qualitative Data', in Robert G. Burgess (ed.), *Field Research: a sourcebook and field manual* (London: Unwin Hyman, 1982), 239-50; Wilson, M., 'Asking Questions', in Victor Jupp and Roger Sapsford (eds.), *Data Collection and Analysis* (London: Sage Publications, 1996), 94-120; Holstein, J. A. and Gubrium, J. F., 'Active Interviewing', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 113-29.

[459] Prior informed consent was required from all participants in accordance with the University of Sheffield postgraduate research ethics guidelines. See Appendix 3 for a copy of the participant consent form.

Interviews were analysed in the light of prior documentary analysis and served to improve the Brazilian case study chapter. It made evident that a number of issues and new avenues for research may arise during the conversation, and that the researcher can easily lose track of the research question being pursued if unstructured interviews are not controlled. Indeed, a number of issues, such as insider information and 'behind the scenes' political conflicts, albeit interesting in their own right, were outside the scope of the investigation and only peripherally mentioned in the case study. Other issues, however, were relevant and thus explored in more detail. All amendments made to the Brazilian case study chapter were not only based on experts' feedback but also validated by the existing and the new documents collected. This served to enrich the case study with more than one perspective and led to a few amendments whenever this author agreed with them. Of course, the resulting final chapter is all this author's own responsibility.

Bryman highlights a number of limitations associated with unstructured interviews, such as problematic access to participants, language barriers and misunderstandings, and personal reactivity (*i.e.* the effects of the researcher's interaction upon respondents' responses).[460] Nevertheless, the small sample size of this investigation contributed to keeping the interviewing scheme under control.

5 Multiple-case study strategy

Both the documentary analysis and unstructured interviews were employed under a multiple-case study strategy. For Yin, this strategy embeds research design, data collection techniques and data analysis, and it is recommended whenever it is necessary to provide an in-depth description of, or explain how a contemporary social phenomenon, over which the researcher has little control, works.[461] Indeed, such a strategy was employed here to explore and understand a complex social phenomenon (the regulations to limit access to online child pornography) taking into account the policies implemented in three different jurisdictions. This aimed to illuminate the question of how regulatory policies operated and also to explore a few contextual issues involved.[462] As such, the unities of analysis are regulations to limit access to online child pornography in Australia, Brazil and the United Kingdom: each jurisdiction is a case study to explore the implications of hybrid regulation.

A multiple-case study strategy was preferred here because inferences from a single-case study were likely to be unreliable, a single-case study would offer limited scope for generalisations from the empirical evidence[463] and, particularly, because of the cross-national nature of online child pornography regulation.[464] Furthermore, a multiple-case study strategy offered the

[460] Bryman, A., *Social Research Methods* (3rd edn.; Oxford: OUP, 2008).

[461] Yin, R. K., *Case Study Research: Design and Methods* (4th edn.; Los Angeles: Sage, 2009).

[462] For Yin, this is another advantage of employing a case study strategy: exploring the contextual issues associated with the phenomenon under scrutiny. See Ibid .

[463] See Ibid .

[464] See Chapter 2 about the multi-jurisdictional challenges posed by the Internet.

opportunity to develop comparative evaluative criteria to assess the implications of hybrid regulation. This strategy facilitates the inclusion of other jurisdictions in order to test out inferences already produced. More importantly, a multiple-case study strategy was needed to identify as many implications of hybrid regulation as possible in order to guide policymaking, and to explore the multi-jurisdictional regulatory challenges posed by the Internet.

Australia, Brazil and the United Kingdom were chosen as case studies because they had generally similar anti-child-pornography laws, both domestically and in terms of their commitments under international treaties, they were considered democratic countries subject to democratic controls of content, and access to data was relatively unproblematic in these jurisdictions. This provided a common ground for comparison. More importantly, they were chosen as case studies because despite very different constitutional frameworks and varied regulatory scope and mechanics, they all settled on similar approaches and rationales to child pornography regulation. This provided an opportunity to explore different aspects and variations of hybrid regulation, and also to address its broader implications for free speech, privacy and democracy on the Internet. They were also representative samples in relation to the models of regulation described in Chapter 2.[465]

This follows the comparative logic of a 'most similar systems design' (*i.e.* choosing countries as similar as possible in relation to relevant features) which will produce intersystemic similarities (the controlled variables - such as similar anti-child pornography laws) and intersystemic differences (the explanatory variables that are theoretically relevant and may be used in explaining such differences - for example, regulatory policies implemented in each jurisdiction).[466] This research intends, to a certain extent, to explain the divergence of hybrid regulation in place in these jurisdictions *vis-à-vis* the similar anti-child pornography laws they adopted.

In addition, language and easy access to documents and participants were important in selecting these jurisdictions. These choices were based on a brief literature search about the topic, but were also exploratory in nature to some extent. Other jurisdictions were potential candidates (for example the US, Russia and China) but the limited resources available, and the more difficult access to data were substantial obstacles; they were discharged as a result.

Although anti-child pornography legislation and interpretations varied significantly in England and Wales, Northern Ireland and Scotland, 'United Kingdom' was used as a case study. This was because the research focused on the work of the Internet Watch Foundation, whose operation is UK wide.

5.1 The difficulties of a cross-national study

---

[465] See generally Berg-Schlosser, D. and De Meur, G., 'Comparative Research Design: Case and Variable Selection', in Rihoux Benoît and Charles Regin (eds.), *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques* (London: Sage, 2009) about the reasons to select a case to study.

[466] Przeworski, A. and Teune, H., *The Logic of Comparative Social Inquiry* (London: Wiley-Interscience, 1970).

For Nelken, there are three approaches to comparative criminology. The behavioural science approach that aims to 'transcend cultural diversity in order to achieve genuine scientific statements.' The interpretative approach that intends to 'show how the meaning of crime and criminal justice is embedded within cultural contexts.' Finally, the comparativist approach that aims to 'classify and learn from the rules, ideals and practices from other jurisdictions.'[467] The comparativist approach is the one taken here. This investigation was neither intended to explain the regulatory differences in terms of cultural and institutional dissimilarities, nor to exclude cultural diversity from the analysis. Instead, this investigation was designed to improve current policymaking by learning from other jurisdictions' experiences.

The cross-national approach to research was relevant not only for this investigation but also for other areas within the field of criminology. This is largely because of the increased importance of transnational crimes and the academic search for understanding and reforming of current policymaking.[468] There are however a number of difficulties associated with the conduction of cross-national studies on both practical and theoretical grounds.[469] The core dilemmas are in relation to the notion of culture. Who and what is going to speak for the culture studied (documents, people, institutions)? Is culture just another variable to be taken on board or the overall context where the social phenomenon occurs? Should culture be approached as a monolithic or as a multidimensional concept?[470]

The notion of local culture has therefore a significant role in cross-national comparative criminology. This investigation made a number of assumptions in this regard however to provide grounds for comparison. It assumed that child pornographic content was similarly disapproved, that law and regulation were straightforward concepts, and that free speech, privacy protection and democratic values were similarly perceived in all three jurisdictions. Nevertheless, child pornography may not be objectionable at the same level, laws and regulations in Brazil follow the civil law tradition, and free speech, privacy protection and democratic values may not be similarly perceived in Australia, Brazil and the United Kingdom.

In addition to the problematic notion of culture, there are issues in relation to 'equivalence of measurement'. Is there any assurance that cross-national researchers are comparing 'like with like'? How can they be sure that similar questions have similar meanings in different cultural contexts? Bottomley and Pease argue that different countries define and measure crime in different ways: crime statistics therefore are products of human interaction in dissimilar cultural settings.[471] Similarly, Vagg argues that the process of collecting, processing and disseminating

---

[467] Nelken, D., 'Comparing Criminal Justice', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (3rd edn.; Oxford: OUP, 2007), 139-57.

[468] Ibid.

[469] For a number of these challenges, see Karstedt, S., 'Comparing cultures, comparing crime: Challenges, prospects and problems for a global criminology', *Crime, Law and Social Change,* 36(3) (2001), 285-308.

[470] See generally Nelken, D., 'Whom can you trust? The Future of Comparative Criminology', in David Nelken (ed.), *The Futures of Criminology* (London: Sage Publications, 1994), 220-43.

[471] Bottomley, K. and Pease, K., *Crime and Punishment: interpreting data* (Buckingham: Open University Press, 1986).

crime-related evidence is influenced by cultural contexts.[472] Of course, the cross-national comparison conducted here had to use approximations to provide grounds for comparison and analysis, and to assume that similar questions had similar meanings in all jurisdictions studied.

Researcher reflexivity raises a number of questions. What are the taken-for-granted assumptions and how does the researcher's cultural background influence research findings? Is it more appropriate to be a native or a foreign researcher when the subject addressed is under a cross-cultural perspective? What is the role played by language barriers?

These questions are far from resolved, but there should be a sense of pragmatism in this regard. Indeed, there is little consensus about how to conduct a cross-national research because different strategies involve both benefits and drawbacks. For Nelken, the best choice for approaching a cross-national investigation is to match what the study is purported to achieve with the methodology employed for such endeavour.[473] Similarly, Smelser points out that these problems may be mitigated if the comparative dimension achieves what the research aims.[474]

It may be the case that conducting a successful cross-national research has more to do with employing research methods that are adequate to the nature of the research questions and aims, rather than being overwhelmed by the orthodoxy of extreme relativism; a touch of responsible pragmatism is necessary to overcome the paralysis of excessive relativism.[475]

6 Personal involvement

The sections above discussed methodological issues associated with this investigation and explained a number of choices made. This section will explore the professional involvement of this author with the research topic.

I was an undergraduate in Computer Science in 1998 when a number of legal issues related to the Internet called my attention. During that time, academics started to address a number of implications that the Internet had on issues such as domain names' disputes, protection of privacy, regulation of online pornography, incitement to racial hatred, protection of intellectual property, jurisdiction, and law enforcement. The criminological aspects of cyberspace and the study of cybercrime led this author to apply for a degree in Law to explore these issues further.

---

[472] Vagg, J., 'Context and Linkage: Reflections on Comparative Research and Internationalism in Criminology', *British Journal of Criminology,* 33(4) (1993), 541-54.

[473] For Nelken, it is necessary to be critical about the methodology employed and its inherent limitations. See Nelken, D., 'Whom can you trust? The Future of Comparative Criminology', in David Nelken (ed.), *The Futures of Criminology* (London: Sage Publications, 1994), 220-43, p 225.

[474] Smelser, N. J., 'The Methodology of Comparative Analysis', in Donald P. and Osherson Warwick, Samuel (ed.), *Comparative Research Methods* (Englewood Cliffs, N.J.: Prentice-Hall, 1973), 3-41.

[475] See Ruggiero, V. and et al., 'Towards a European Criminological Community', in Ruggiero and et al. (eds.), *The New European Criminology: Crime and Social Order in Europe* (London: Routledge, 1998), 1-15; and also Leavitt, G. C., 'Relativism and Cross-Cultural Criminology: A Critical Analysis', *Journal of Research in Crime and Delinquency,* 27(1) (1990), 5-29.

In 2001, I was invited to work part-time coordinating an experimental Internet hotline project at CEDECA-BA,[476] and worked there until the mid-2002, when I was accepted for a Master of Arts in International Criminology at the University of Sheffield in September of 2002, after successfully obtaining a scholarship from the British government (the Chevening Scholarships Programme). Along this period, I conducted a comparative investigation between the pilot-Internet hotline created in CEDECA-BA and the British hotline Internet Watch Foundation. The masters' dissertation addressed the operation of both Internet hotlines and provided a cross-national comparative analysis.[477]

Later in 2004, I started my career in the civil service in the State of Bahia in Brazil. The formulation and assessment of public policies were amongst my responsibilities. I was interested in how the Brazilian government was tackling the proliferation of online child pornography in the country. As a result, I proposed an investigation to map the operation of different public and private actors tackling the availability of child pornographic material on the Internet in Brazil. The research addressed not only the role of Brazilian Internet hotlines, but the Internet industry, Parliament and police authorities. It was conducted from September 2004 to November 2005 and adopted a qualitative approach: questionnaires and unstructured interviews were applied. Eight police authority representatives (Federal and State Police); six association of internet service providers; 13 Internet hotlines; and 39 legislative bills (under appreciation by the Brazilian National Congress) were included in this study.[478]

It was against this background that this doctoral research came to life. The decision to focus on regulatory initiatives limiting access to child pornography on the Internet was a result of my past experience in academia, civil society (*i.e.* children protection non-governmental organisation) and the public sector. Perhaps, losing my wife and friend Samantha Reis, who also worked in the field as a child psychologist, in a tragic accident in 2006, or perhaps, being a single father of a young boy aged 3 at the start of this investigation also played a role in choosing this research topic. This author believes however that these two events, instead of crystallising any radicalism in his views or in the analysis developed here, helped him in keeping the faith, motivation and academic criticism during the most difficult of times, particularly when this investigation seemed to be going nowhere.

A personal interjection: despite the formal layout of this thesis and the critical approach towards the subject, which may suggest that I am insensitive towards human suffering or, perhaps to some, that I am sympathetic to the claims of paedophiles, I do believe child sexual abuse is an

---

[476] The *Centro de Defesa da Criança e do Adolescente da Bahia* is a non-governmental organisation located in Brazil that provided legal and psychological assistance to children victims of sexual abuse. During the time this author worked there, he attended a number of international conferences about the problem of child pornography available on the Internet.

[477] See Reis, F., 'Internet Hotlines Fighting Online Child Pornography: a comparative study between Brazil and England.', (The University Of Sheffield, 2003), at <http://www.fabiorei.com> accessed 07 June 2010.

[478] Oliveira, T. and Reis, F., *Pornografia Infantil na Internet: o enfrentamento no Brasil (unpublished)* (Salvador-BA, Brasil: CEDECA-BA, 2006) 104p.

outrageous aggression; I do feel angry and upset at such revolting violence; I do feel compassionate towards those who are recovering from the trauma.

Notably, this investigation did not involve any child victim of sexual abuse nor any convicted sexual offender. Similarly, no illegal website was visited nor was any child pornographic material viewed under any circumstance.

This reduced considerably the ethical issues around the research topic. Nevertheless, although this research focused only on regulatory responses to online child pornography, there are a number of ethical issues involved. This investigation owns ethical responsibilities towards the sponsors, respondents and the silenced victims of sexual abuse. First, I had to be extremely concerned with my claims not to be collusive with paedophiles' arguments. Second, I had to be sensitive to sponsorship standpoints and expectations.[479] Third, I added to the proliferation of discourses around children sexual abuse. I could absolutely not be exempted from any of these ethical dilemmas.

Although I was a civil servant and this doctoral project was partially funded by the Government of the State of Bahia, in Brazil, this investigation was subject to no influence from the government. I was absolutely free to conduct the research without any political pressure that could influence the final result; there was neither any fear from retaliation nor threat of any sort in this regard. On the contrary, being a civil servant made me aware of how things work inside the government in practice, and facilitated access to people and documents. My prior experience at a non-governmental organisation and involvement with children rights' activists also facilitated access to relevant people and documents. Generally, rather than providing a partial account about the research topic, this condition contributed to enrich this research.

7 Final comments

This chapter addressed methodological and ethical issues associated with this study. The documentary analysis and unstructured interviewing scheme employed under a multiple-case study strategy were discussed. In addition, difficulties of conducting cross-national investigation and the professional involvement of this author were addressed. The next chapter explores the laws and regulations in place to limit access to child pornography on the Internet in Australia, Brazil and the United Kingdom, respectively.

[479] This investigation was partially sponsored by the Government of the State of Bahia (Brazil). All other expenses were paid for by my personal means.

CHAPTER 4: CURRENT MODELS FOR REGULATING ACCESS TO CHILD PORNOGRAPHY: AUSTRALIA, BRAZIL AND THE UNITED KINGDOM

This chapter explores in detail the laws and regulations to limit access to online child pornographic content in Australia, Brazil and the United Kingdom. It is an overview of the substantive law and regulatory framework in place in these jurisdictions based on the documentary evidence available.

1 Australia

The online regulatory scheme established in 1999 extended the existing regulation of television broadcasting to the online environment and relied on a substantial number of statutes, administrative regulations and industry self-regulation to limit access to illegal material available on the Internet, and also to online material deemed unsuitable for children and young people. In fact, the Australian scheme targeted not only illegal material, *e.g.* child pornography but content considered inappropriate to minors such as adult pornography. The federal government is the central regulatory actor but online intermediaries (*e.g.* ISPs, content service and hosting service providers) play a significant role via Industry Codes of Practice (CoP).

Child pornographic material hosted in Australia was targeted via notices of take down[480] sent by the federal regulator ACMA to relevant Internet content service or hosting service providers. Overseas child pornographic websites were targeted via a voluntary user-level filtering scheme employed since 2000. Nevertheless, another voluntary filtering scheme, employed at the ISP-level, was launched by the Internet Industry Association in July 2011 to block access to overseas child pornographic websites by the means of a partnership with the Australian Federal Police and Interpol. Furthermore, the federal government has been trying since 2007 to implement a nationwide mandatory filtering scheme at the ISP-level, via legislation, to target not only child pornographic content but other types of material included in the federal regulator's blocklist.

Section 1.1 explores the historical context of online content regulation in Australia particularly in relation to child pornographic material. Section 1.2 addresses Commonwealth, State and Territory criminal laws tackling the production, distribution and possession of online child pornography. Subsequently, Section 1.3 provides a detailed account of the Commonwealth online content regulatory laws and regulations to limit access to online child pornography, be it hosted in Australia or overseas. Although this research focuses on regulation to stop accessing child pornography on the Internet, the case study material addressed the wider scope of the

[480] Generally, notices of take down are the requests sent by the relevant authority to hosting services or content service providers informing that either illegal or inappropriate content was found to be hosted in their servers. After being notified, the online intermediary may be liable if it does not act expeditiously to remove access to such content.

Australian regulatory regime so as to place the research question into the overall regulatory context.

1.1 Historical context[481]

The debate about online content regulation in Australia started in the mid-1990s following the report of the Bulletin Board System (BBS) Task-force in 1994.[482] Later in June 1996, the Australian Broadcasting Authority (ABA)[483] published a report[484] about online content regulation suggesting a self-regulatory approach via Internet industry Codes of Practice (CoP), monitored by ABA, to regulate the content available on the Internet. Subsequently, in February 1997, a Senate Select Committee launched an inquiry and issued a report in late June 1997. The majority report recommended criminal offences for online publication or distribution of various types of material including material unsuitable for minors (*i.e.* material lawful to publish or distribute offline), while the minority report (by opposition parties' Committee members) opposed this and various other recommendations.[485] On 15 July 1997, a proposal for a regulatory framework[486] formulated by the Ministry of Communications and the Arts, and the Attorney General, was issued for public consultation. The Minister for Communications contended, in an associated media release, that the proposal was '[…] consistent with […] the recommendations, released last June, of the ABA's major study of on-line content regulation.'[487] On 15 December 1997, Commonwealth, State and Territory Attorneys-General issued a media release '[…] reaffirm[*ing*] that criminal sanctions should apply to people who place offensive or illegal material on the Internet […]' and that ISPs would be subject to a new criminal offence '[…] of knowingly, though passively, allowing another person to commit an offence.'[488] For Griffith, the debate that followed made evident the conflict between self-regulation and a more

---

[481] For an overview about online content regulation in Australia, see EFA, 'History of Internet Regulatory Proposals/ Activity in Australia', (updated January 2000) at <http://www.efa.org.au/Issues/Censor/censhistory.html>, accessed 19 September.

[482] 'BBS Task-force Report', (Australia, 1994) at <http://web.archive.org/web/20020906144005/http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&pathid=/pubs/bulletin_board/report.htm>, accessed 05 March 2012.

[483] The ABA was the federal regulator at that time, but it has now been replaced by the ACMA. See ACMA, 'Australian Communications and Media Authority - The ACMA is a statutory authority within the federal government portfolio of Broadband, Communications and the Digital Economy', at <http://www.acma.gov.au>, accessed 28 March 2010.

[484] ABA, 'Investigation into the Content of On-line Services', (Australia: Australian Broadcasting Authority, 1996) at <http://web.archive.org/web/20060827020412/http://www.acma.gov.au/acmainterwr/aba/about/recruitment/olsfinal.pdf>, accessed 05 March 2012.

[485] 'Report of the 'Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies', (Australia, 1997) at <http://www.aph.gov.au/senate/committee/comstand_ctte/online3/index.htm>, accessed 05 March 2012.

[486] 'Principles for a Regulatory Framework for On-line Services in the Broadcasting Services Act 1992', (Australia: Ministry for Communications and the Arts and the Attorney-General, 1997) at <http://web.archive.org/web/20000226172048/http://www.dcita.gov.au/nsapi-text/?MIval=dca_dispdoc&pathid=/policy/framework.html>, accessed 05 March 2012.

[487] 'Minister's media release', (1997) at <http://web.archive.org/web/20031124104143/http://www.dcita.gov.au/Article/0,,0_1-2_1-4_10366,00.html> Accessed 05 March 2012.

[488] 'A-Gs' media release', (Australia, 1997) at <http://web.archive.org/web/20070608032701/http://www.ag.gov.au/www/attorneygeneralHome.nsf/Alldocs/086E324FF9AA0947CA256B53000F1B19?OpenDocument> Accessed 05 March 2012.

'stringent criminal' stance in relation to online content regulation and this led to a co-regulatory compromise.[489]

In April 1999, the Commonwealth Government introduced a Bill into Parliament,[490] which came into effect in January 2000 and amended the Broadcasting Services Act (BSA) 1992.[491] The 1999 amendment[492] aimed to extend the current content regulatory framework applied in relation to television broadcasting to the Internet. This regulatory approach was subject to substantial criticism[493] particularly after a similar statute was struck down by the US Supreme Court in 1997.[494]

Amongst other things, the Australian legislation established a voluntary content filtering scheme that was arguably unable to block access to content hosted overseas, be it illegal or harmful. As a result, the Australian Institute published a survey in 2003 showing how easily children could access inappropriate material online and this raised public calls for an ISP-level mandatory content filtering. The Australian Labor Party opposed a mandatory filtering scheme but this approach changed in 2007 when such policy was included in the political programme as part of the election campaign. It was also in 2007 that a new piece of legislation[495] amended the existing online content regulatory laws to cope with new technological developments (*e.g.* streaming and live content services). The 2007 amendments were introduced by the Howard Coalition Government and were passed before the 2007 election with a commencement date of 01 Jan 2008.

Although the government was the key online content regulator in Australia, the Internet industry was involved by developing and complying with Codes of Practice (CoP). In fact, a number of CoPs were produced, registered and reviewed over time and they generally guided Australian online intermediaries to comply with the relevant regulatory legislation so as to avoid the risk of legal liability. Domestic laws not only established the regulatory regime of online content in relation to the Internet industry but it also tackled the production and distribution of, and the access to child pornography on the Internet by ordinary members of the public. As a result, a number of anti-child pornography criminal laws were amended at the Commonwealth, State and Territory levels. Generally the Commonwealth criminal laws were applied in relation to inter-

---

[489] Griffith, G., 'Censorship in Australia: Regulating the Internet and other recent developments', NSW Parliamentary Library Research Service, 2002) at <http://www.parliament.nsw.gov.au>, accessed 25 September 2011, p 23.

[490] 'Minister's media release announcing the introduction of the 1999 Bill', (Australia, 1999) at <http://web.archive.org/web/20020821095852/http://www.dcita.gov.au/Article/0,,0_1-2_1-4_13762,00.html > Accessed 05 March 2012.

[491] Broadcasting Services Act 1992 (Cth Australia).

[492] Broadcasting Services Amendment (Online Services) Act 1999 (Cth Australia).

[493] See particularly the work developed by the Australian non-profit organisation (i) EFA, 'Electronic Frontiers Australia', at <http://www.efa.org.au/>, accessed 22 August 2011; and also Graham's personal website (ii) Graham, I., 'Libertus.net: about censorship and freedom of expression, in Australia and elsewhere', at <http://libertus.net/>, accessed 22 August 2011.

[494] See Chapter 3 about US governmental attempts to regulate online material considered inappropriate to minors.

[495] Communications Legislation Amendment (Content Services) Act 2007 (Cth Australia).

state offences (*e.g.* online intermediaries and intentional access), and the relevant State and Territory criminal laws were applied in relation to intra-state offences (*e.g.* mere possession).

Nevertheless, the constitutional position on this was not that straightforward. The Commonwealth did not have general power to regulate in relation to inter-state matters, and the States and Territories were not limited to regulating in relation to intra-state matters. Which level of government could regulate what, depended on provisions from the Australian Constitution, which limited the Commonwealth's powers to regulate to specific matters stated in the Constitution, and also depended on how the Australian High Court had interpreted those specific powers in the Constitution in cases challenging or disputing the constitutionality of a particular piece of legislation.

The Commonwealth did not have a constitutional head of power enabling them to enact criminal offences applicable to the conduct of ordinary members of the public, in relation to activity that did not involve use of a carriage service (except in circumstances, *e.g.* damage to Commonwealth owned property). That was the reason why laws concerning offline child pornographic material (possession, production and offline distribution, which were either a part of, or contributed to the child pornography online industry) were laws of States and Territories, because only they had constitutional power to regulate in that regard.[496] As a result, these different jurisdictional levels defined child pornography, the age of a child, the relevant offences, defences and penalties differently. Australia ratified the 2000 UN Optional Protocol[497] on 08 January 2007 but it was not a signatory of the 2001 CoE's Cybercrime Convention.[498]

Child pornographic content hosted overseas has been targeted since 2000 via a voluntary filtering scheme at the user-level, following the 1999 and 2007 amendments of the 1992 Act.[499] Nevertheless, another voluntary filtering regime at the ISP-level was launched by the Internet Industry Association in July 2011. This scheme blocked access to overseas website domains (not particular URLs) allegedly containing child pornographic material, it was based on a blocklist created and maintained by Interpol and it was voluntarily employed by a few Australian ISPs. The Commonwealth government has been trying to implement a mandatory ISP-level filtering scheme via legislation since 2007, which was expected to target not only child pornography but other material.

1.2 Legislation

---

[496] See the 'Chapter 6 of the Joint Parliamentary Committee report on their inquiry into the Cybercrime Legislation Amendment Bill 2011', (Australia, 2011) at <http://www.aph.gov.au/house/committee/jscc/cybercrime_bill/report/chapter6.pdf>, accessed 05 March 2012 for more information about the constitutional situation.

[497] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

[498] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[499] Broadcasting Services Act 1992 (Cth Australia).

Australia was a federal country comprised of one federal entity (*i.e.* the Commonwealth),[500] six States (*i.e.* New South Wales, Victoria, Queensland, South Australia, Western Australia and Tasmania) and two Territories (*i.e.* the Australian Capital Territory and the Northern Territory) and they all had jurisdiction in relation to anti-child pornography criminal laws. Generally the Commonwealth had criminal jurisdiction over inter-state offences, whereas Australian States and Territories had criminal jurisdiction over intra-state offences but this was not so straightforward as discussed above. As a result, anti-child pornography criminal laws applied in each jurisdiction differed not only in relation to the definition of child pornography and age of a child, but also in relation to types of child pornographic content, criminal conducts, defences and relevant penalties. It has been argued that these jurisdictional discrepancies created a number of difficulties to law enforcement agencies,[501] but others believe that these differences showed 'relatively coherence' in practice.[502]

Australia regulated both online content and online intermediaries via legislation, in addition to self-regulatory guidelines developed by the Internet industry. The online content regulatory framework in relation to online intermediaries is explored in Section 1.3 below. This section, however, addresses Australian anti-child pornography criminal laws, particularly the provisions that attempted to limit access to child pornographic content available on the Internet (for example possession and intentional access by individuals) as well as legislation that had a deterrent effect on online access (for example regulation of investigatory powers of law enforcement bodies), and also the relevant international treaties ratified by Australia.

1.2.1 State-regulation:[503] anti-child pornography criminal laws

Generally anti-child pornography criminal laws tackling production and distribution of, and access to online child pornography have at least five elements: (i) the definition of online child pornography (*i.e.* what child pornography is and the age of a child); (ii) the types of child pornographic content (*i.e.* photographs, pseudo-photographs, cartoons, text, audio); (iii) the criminal conducts (*i.e.* production, distribution and access); (iv) the legal defences (*i.e.* exemption from criminal liability); and (v) the relevant penalties.[504] The Commonwealth, States and Territories criminal laws addressed each one of these elements differently.

> […] state and territory legislation dealing with internet content continues to vary enormously. For example, Operation Auxin, a national investigation of those buying child pornography via the internet, resulted in arrests and charges being laid across Australia. Due to the continuing lack of uniformity across jurisdictions, those arrested were charged

---

[500] The words 'Commonwealth' and 'federal' will be used hereinafter interchangeably to mean the federal entity of the Australian government.

[501] See Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52.

[502] Griffith, G. and Simon, K., 'Child Pornography Law', New South Wales Parliament, 2008) at <http:// www.parliament.nsw.gov.au/prod/parlment/publications/>, accessed 12 July 2010, p 73.

[503] See the definition of state regulation developed in Chapter 2. This definition is not to be confused with the legislation enacted by the Australian States.

[504] See Section 1 in Chapter 3 about the problem of online child pornography.

> under state and territory laws, which included a variety of offences, defences, and penalties depending on whereabouts a person was charged. Thus even those in possession of the same content, in the same format, of the same quantity, and from the same source are still subject in Australia to hugely varying laws.[505]

This subsection presents an overview of Australian anti-child pornography criminal laws at the Commonwealth (within its constitutional remit to regulate broadcasting services); and States and Territories levels. Although the five elements abovementioned are generally covered in relation to each jurisdictional level, the focus here is placed on criminal provisions relevant to limit access to child pornographic material available on the Internet.

1.2.1.1 Commonwealth anti-child pornography criminal laws

Criminal offences under the Commonwealth jurisdiction were established by the Criminal Code Act 1995[506] as amended by the Telecommunications Offences and Other Measures Act 2004;[507] these amendments came into effect from March 2005.[508] Online child pornography provisions were found in Division 273 (offences involving child pornography material or child abuse material outside Australia) and Division 474 (telecommunications offences) of the Criminal Code Act 1995 as amended. Carriage (also carrier) service provider had the same meaning as in the Telecommunications Act 1997 (*i.e.* a service for carrying communications by means of guided and/or unguided electromagnetic energy).[509] In addition, Internet content host and Internet service provider had the same meaning as in Schedule 5 of the 1992 Act as amended.

The amended Criminal Code Act 1995 defined what child pornography was, the age of a child, types of child pornographic content, criminal conducts, legal defences and relevant penalties at the Commonwealth level and were in relation to offences committed via the use of a carriage service. Child pornographic material was defined in Section 473.1 of the amended 1995 Act as material that:

> (1) depicts a person, or a representation of a person, who is, or appears to be, under 18 years of age and who: (i) is engaged in, or appears to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or (ii) is in the presence of a person who is engaged in, or appears to be engaged in, a sexual pose or sexual activity; or
>
> (2) the dominant characteristic of which is the depiction, for a sexual purpose, of: (i) a sexual organ or the anal region of a person who is, or appears to be, under 18 years of age; or (ii) a representation of such a sexual organ or anal region; or (iii) the breasts, or a representation of the breasts, of a female person who is, or appears to be, under 18 years of age; or

---

[505] Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 345.

[506] Criminal Code Act 1995 (Cth Australia).

[507] Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth Australia).

[508] The Customs Act 1901 (Cth Australia) targets the importation and exportation of child pornographic content in relation to *e.g.* print publications, DVDs, video tapes and content stored on physical goods such as computer disks and laptops. It does not target the importation or exportation of digital data by means of telecom networks.

[509] Telecommunications Act 1997 (Cth Australia).

(3) describes a person who is, or is implied to be, under 18 years of age and who: (i) is engaged in, or is implied to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or (ii) is in the presence of a person who is engaged in, or is implied to be engaged in, a sexual pose or sexual activity; or

(4) describes: (i) a sexual organ or the anal region of a person who is, or is implied to be, under 18 years of age; or (ii) the breasts of a female person who is, or is implied to be, under 18 years of age.

Child pornographic content covered thus both visual and textual materials under the Commonwealth criminal law.[510] Provisions in relation to child pornography were found in the Division 474 about telecommunications offences of the amended 1995 Act, and relied on Section 51(v) of the Commonwealth of Australia Constitution about the broadcasting power of the Commonwealth to legislate in this regard.[511] Its Subdivision D targeted offences related to using a carriage service for child pornography material, and its Subdivision E addressed offences related to the obligations of Internet service providers and Internet content hosts in relation to this. The amended 1995 Act distinguished between child pornographic content and child abuse material (*i.e.* material depicting a person under 18 as a victim of torture, cruelty or physical abuse), and criminalised online grooming (*i.e.* to procure or groom under-aged persons).

The amended 1995 Act criminalised in Section 474.19 to access (*i.e.* to access or solicit) or distribute (*i.e.* to cause material to be transmitted to him/herself, transmit, make available, publish, distribute, advertise or promote) child pornography material using a carriage service. In addition, Section 474.20 made it an offence to possess (*i.e.* to possess or control), distribute (*i.e.* to produce or supply) or access (*i.e.* to obtain) child pornography material with the intention that the material be used using a carriage service. Note that the offences above were in relation to the use of a carriage service and that was the reason why they are under the Commonwealth jurisdiction. In addition, Section 474.21 established a number or defences in relation to child pornographic material (*e.g.* if the conduct is of public benefit, if the person was conducting his/her duties as law enforcement officer, or if the person engaged in the conduct in good faith). Online content filter companies were exempt from criminal liability in relation to online child pornographic content according to Section 474.21(4)(b).

There were provisions in relation to child pornography offences committed outside Australia by Australian nationals or residents; these provisions were found in Section 273.5. They made a criminal offence to produce, distribute or possess child pornographic material outside Australia and attached a penalty of 15 years imprisonment. These were to prevent Australian nationals or residents going overseas to engage in such criminal activities aiming to evade criminal prosecution in Australia.

---

[510] Griffith, G. and Simon, K., 'Child Pornography Law', New South Wales Parliament, 2008) at <http://www.parliament.nsw.gov.au/prod/parlment/publications/>, accessed 12 July 2010, p 24.

[511] Commonweatlh of Australia Constitution Act 2003 as amended (Australia).

1.2.1.2 Australian States and Territories anti-child pornography criminal laws

Commonwealth criminal laws in relation to online child pornography covered offences committed via carriage services and they were explored above. The reach of both State and Territory criminal laws was much broader[512] and therefore most offences related to offline child pornographic content (*e.g.* production and possession of child pornography for commercial or non-commercial purposes) were under their criminal jurisdiction.

Australian States and Territories established their own substantive criminal law and had different provisions about what child pornography was, the age of a child, types of child pornographic content, criminal conducts and relevant penalties. For example, child pornographic content could be defined as child pornography, child exploitation material or child abuse material depending on the jurisdiction.[513] The mere possession offence was subject to varying penalties depending on the State or Territory where the offence was committed, despite the fact that intentional access to child pornography via a carriage service was punished uniformly under Commonwealth criminal law.[514] In addition, the States and Territories anti-child pornography laws covered not only photographs and pseudo-photographs but drawings, cartoons, written texts and spoken words.

Similarly, in some jurisdictions the age of a child in relation to child pornographic content was of a person under 16 (*e.g.* New South Wales, Queensland, South Australia and Western Australia), whereas in other jurisdictions the age of a child was of a person under 18, which was in line with the 2000 UN Optional Protocol.[515] The age of 16 was the age of consent in most States and Territories. In a number of them, where the age in relation to child pornographic material was 18 years, the situation existed where 16 and 17 year olds were lawfully permitted to engage in sexual activity but if they took a photograph of themselves (whether or not sexually explicit), they could be convicted of a criminal offence and put on a sex offenders' register.

It was unclear whether these differences had any relevant implications, for example 'forum shopping,' but it may be the case that such legal uniformity led to complications in terms of nation-wide or international police operations and varying levels of deterrence to potential offenders. In addition, the sense of fairness may an issue here because the same offence may be subject to different definitions and penalties depending where the offence was committed in Australia. Yet, in terms of the regulation of access to child pornographic content it seemed

---

512 Griffith, G. and Simon, K., 'Child Pornography Law', New South Wales Parliament, 2008) at <http://www.parliament.nsw.gov.au/prod/parlment/publications/>, accessed 12 July 2010, p 73.

513 For a description of the States and Territories anti-child pornography criminal laws, see Gillespie, A., *Child Pornography: law and policy* (Oxon: Routledge, 2011), p 82-97 and also p 202-217.

514 Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 351.

515 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

unlikely that offenders would move around Australian States and Territories in order to avoid higher punishment if caught.

1.2.1.3 Law enforcement investigatory powers

Regulation of law enforcement investigatory powers, particularly in relation to online content criminal offences, addressed the collection of criminal evidence, the identification of alleged offenders and the cooperation of online intermediaries with the law enforcement bodies for purposes of criminal investigation. Although these provisions did not target individuals directly, but rather indirectly via online intermediaries, it is important to address them here because they may have a deterrent effect in limiting access to child pornography available on the Internet. In Australia, the legal framework for the interception of communication at the Commonwealth level was established by the Interception and Access Act 1979[516] and the Telecommunications Act 1997,[517] both amended by the Interception and Access Amendment Act 2007;[518] and the Surveillance Devices Act 2004.[519]

The Interception and Access Act 1979 made it an offence for a person to intercept a communication passing over a telecommunication service or to access stored communications without a relevant warrant. It regulated the issuing of warrants and established an oversight scheme to protect against unlawful interceptions. The Surveillance Devices Act 2004 regulated the use of surveillance devices such as. computer-based surveillance, listening devices, optical and tracking devices.[520] These two Acts were within the portfolio responsibilities of the Commonwealth Attorney-General and it applied to carriage service providers, which included Internet access service providers, according to Section 87.[521]

Section 313 of the amended 1997 Act established that service providers were required to do their best to prevent their networks being used for the commission of offences and to help the Australian police forces enforcing the criminal law. As a result, it has been advocated by the Internet Industry Association as the legal basis for the voluntary ISP-level filtering scheme targeting overseas child pornographic website domains in 2011. Nevertheless, this claim is debatable and is discussed later in this chapter.

Part 13 of the amended 1997 Act imposed an obligation on carriage service providers to protect the privacy and confidentiality of communications and information about the affairs and personal particulars of persons, except when an exemption specified in Part 13 was applicable.

---

[516] Telecommunications (Interception and Access) Act 1979 (Cth Australia) as amended.

[517] Telecommunications Act 1997 (Cth Australia) as amended.

[518] Telecommunications (Interception and Access) Amendment Act 2007 (Cth Australia).

[519] Surveillance Devices Act 2004 (Cth Australia).

[520] See the Attorney-General's Department website for an overview about the telecommunications interception and surveillance legislation in Australia. 'Attorney-General's Department - Australian Government', at <http://www.ag.gov.au/>, accessed 19 September.

[521] Section 87 defines carriage service providers as a supplier of listed carriage service (*i.e.* a service for carrying communications by means of guided and/or unguided electromagnetic energy) to the public.

Exemptions included the disclosure of information to law enforcement agencies under the conditions and circumstances specified in the amended 1997 Act. It set out several means by which law enforcement agencies were authorised to obtain information from carriage service providers such as: (i) interception warrants (*e.g.* to listen to or require recording of the content of real time communications); (ii) stored communications warrants (for example, to access or obtain copies of the content of stored communications such as email messages stored on an ISP's server); (iii) 'authorised requests'[522] to obtain information about a particular customer (*e.g.* name and address of a person who was using a particular IP address at a particular time); and (iv) to obtain information about (excluding the content or substance of) a communication such as source, path, and destination.

A number of police operations took place in Australia. The Australian Federal Police and State police forces launched Operation Auxin in 2004 and were able to arrest and charge 191 Australians in relation to child pornography offences. Following the 2004 amendments,[523] Operation Centurion was launched in June 2008, via cooperation with Interpol, and resulted in 136 people arrested in Australia for accessing child pornography available on the Internet.[524] There was a memoranda of understanding negotiated between the Australian Communications and Media Authority (ACMA) and Australian police forces regulating the notification and investigation of child pornographic content hosted in Australia (thus involving the Australian content service providers and hosting service providers). This memoranda established the roles and responsibilities of both governmental bodies in this regard in addition to knowledge sharing and training events.[525]

1.2.2 Multi-state regulation: the international treaties

Australia had anti-child pornography laws not only domestically but it was a signatory of the 2000 UN Optional Protocol.[526] This multi-state regulatory instrument established a definition of child pornography in Article 2 and suggested that signatories should criminalise a number of conducts in relation to child pornographic content (such as production, distribution and possession). It also established a number of provisions to protect children against sexual exploitation. Australia signed the 2000 UN Optional Protocol on 18 December 2001 and ratified

---

[522] Authorised requests are not permitted to be used to obtain information about the content or substance of a communication; a warrant is required for disclosure of content of communications.

[523] Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth Australia).

[524] See 'Proposed Reforms to Commonwealth Child Sex-Related Offences', (Attorney-General's Department, Australian Government, 2009) at <http://www.ag.gov.au> Accessed 25 September 2011, p 55; and also 'AFP successfully combats child sex exploitation', *Platypus Magazine*, (2009) at <http://www.afp.gov.au/~/media/afp/pdf/1/11-child-protection.ashx> accessed 07 March 2012.

[525] See ACMA, 'ACMA hotline – Frequently asked questions: 25. What is the relationship between the ACMA and law enforcement?', (updated 02 September 2011) at <http://www.acma.gov.au/WEB/STANDARD/pc=PC_310147#25>.

[526] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

it on 08 January 2007. The 2001 CoE's Cybercrime Convention[527] established a number of provisions in relation to substantive and procedural criminal law to facilitate international police cooperation mainly within Europe, but Australia was not a signatory of this international instrument.

1.3 Regulatory policies

The preceding section explored the Australian anti-child pornography criminal laws, particularly those designed to limit access to child pornographic content available on the Internet in relation to individuals who produce, distribute or access child pornography. Against this background, this section addresses the online content regulatory model established by Commonwealth legislation in partnership with the Internet industry to target child pornographic content available on the Internet whether hosted in Australia or overseas. Although the anti-child pornography criminal laws discussed above were established at different jurisdictional levels (*i.e.* by the Commonwealth, States and Territories), the Australian content regulation scheme was established by Commonwealth legislation and enforced, to a large extent, uniformly across the country. The reason for this was because the Commonwealth of Australia Constitution limited Commonwealth powers to enact laws in this regard.

The regulation of online material in Australia targeted a number of issues: (i) it addressed both material considered inappropriate to minors and illegal material such as child pornography; (ii) although the Internet industry played a role via self-regulatory practices, the framework was centred in the government regulator and involved substantial regulatory bureaucracy (*i.e.* legislation and administrative regulation); (iii) there was a federal statutory regulator forcing online intermediaries to remove the relevant content hosted in Australia; (iv) the relevant content hosted overseas was addressed via a voluntary filtering scheme at the user-level, but there was a voluntary ISP-level scheme in operation since 2011 supported by the IIA, and the government has been trying since 2007 to implement a mandatory ISP-level filtering system via legislation based on its own blocklist.

Although this case study was about child pornography, this section explores the overall online content regulatory scheme because it was within this framework that the access to online child pornography has been targeted in Australia.

1.3.1 Online content regulation in Australia: the Commonwealth legislation

The regulation of content involving television broadcasting in Australia was established by the Broadcasting Services Act 1992,[528] until 01 January 2000, when amendments established by the Services Act 1999[529] commenced. The basis of such amendments was a government decision

---

[527] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[528] Broadcasting Services Act 1992 (Cth Australia).

[529] Broadcasting Services Amendment (Online Services) Act 1999 (Cth Australia).

that online content should be regulated like content transmitted by television subscription broadcasting and narrowcasting services, not like offline material such as print publications, films and videos.[530] As a result, the 1999 Act extended the laws applied to traditional media towards the content available online taking into account the classification system as applied to the television broadcasting industry.[531] The regulatory scheme was amended again by the Content Services Act 2007[532] so as to cover new technological developments, *e.g.* online live streaming and linking services available in Australia. All these regulatory developments are explored below.

1.3.1.1 The amendments in 1999

In April 1999, the Commonwealth Government introduced a Bill into Parliament,[533] which came into effect in January 2000 and amended the Broadcasting Services Act (BSA) 1992.[534] The 1999 amendments came into force via the Online Services Act 1999[535] and aimed generally to extend the current content regulatory framework applied in relation to television broadcasting to the Internet and established a co-regulatory approach toward the content available online. The 1999 Act aimed to: (i) implement a complaint mechanism; (ii) implement a take-down notice scheme in relation to online content defined as 'prohibited content' which includes material that is lawfully available to adults in offline videos and print publications; and (iii) restrict access to other types of content unsuitable for children and young people.

Generally the 1999 amendments established a complaint-based mechanism operated by a federal statutory regulator (*i.e.* the Australian Broadcasting Authority - ABA), placed a few regulatory responsibilities on the Australian Internet industry by the means of Internet industry Codes of Practice (CoP) and industry standards, and established a number of public awareness policies. Bodies and associations representing the Australian Internet industry were implicitly compelled to develop CoPs and ABA had a reserve power to impose an industry standard, if no CoP was developed, or if the CoP was judged deficient. These CoPs were to be registered by the ABA before coming into force.

The ABA was made responsible for the operation of the complaints hotline in relation to prohibited or potential prohibited content available on the Internet, for the international liaisons and for ensuing the compliance of Australian online intermediaries with the relevant legislative

---

[530] See the explanatory memorandum at 'Broadcasting Services Amendment (Online Services) Bill 1999: Explanatory Memorandum', The Parliament of the Commonwealth of Australia: The Senate, 1999) at <http://www.comlaw.gov.au/Details/C2004B00465/Explanatory%20Memorandum/Text>, accessed 05 March 2012.

[531] See Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 338. See also Alston, R., 'The Government's Regulatory Framework for Internet Content', *University of New South Wales Law Journal,* 23(1) (2000), 192-97.

[532] Communications Legislation Amendment (Content Services) Act 2007 (Cth Australia).

[533] The original bill required the Australian ISPs to block access to prohibited content available on overseas websites using ISP-level filtering, but this provision was later removed from the bill because of wide criticism and was replaced by a user-level voluntary filtering scheme. See Graham, I., 'The Net Censorship Dilemma: Liberty or Tyranny', (updated 06 June 2009) at <http://libertus.net/liberty/>, accessed 01 September 2011.

[534] Broadcasting Services Act 1992 (Cth Australia).

[535] Broadcasting Services Amendment (Online Services) Act 1999 (Cth Australia).

provisions. The definition of prohibited content covered RC (Refused Classification) and X18+ rated content as well as the R18+ rated content not subject to a Restricted Access System (RAS). Generally, ABA was responsible for investigating and assessing these complaints made by members of the public and, if applicable, for issuing interim or final take-down notices to the relevant Australian Internet content host so the material could be removed. If the prohibited or potential prohibited content was hosted overseas, an Australian police force was contacted (if the content was of serious nature, *e.g.* child pornography) and content filter vendors were notified, so ISPs could deal with the issue according to the relevant CoP or industry standard provisions (*i.e.* the ISPs would inform its customers about the availability of such filters).

1.3.1.2 The amendments in 2007

Online content regulatory legislation was amended again in 2007 by the Content Services Act 2007.[536] This not only amended Schedule 5 but included Schedule 7 in the already amended BSA 1992. Generally the 2007 amendments extended the categories of prohibited and potential prohibited content (*i.e.* including the RC and X18+ rated content as well as the R18+ and MA15+ rated content[537] not subject to a Restricted Access System (RAS);[538] for the relevant prohibited content hosted in Australia, it established the take-down, service-cessation and the link-deletion notices in relation to a hosting, live content and links service, respectively; it established the concept of an 'Australian connection' so as to cover content hosted in Australia and content provided from Australia, as in the case of a live content service; and it established the requirements for future industry CoPs and standards in relation to content service and hosting service providers.

In addition, the 2007 amendments altered the existing prohibited category to include the commercial MA15+ rated content not subject to a Restricted Access System; and the overseas-hosted content that was or 'could be' classified R18+ (enabling the ACMA - which replaced the Commonwealth regulator ABA - to add such content to its blocklist). This gave ACMA a new power to issue 'interim' take-down notices in relation to Australian-hosted suspected R18+ rated content, on the basis of its guess as to the likely classification of such material.[539]

1.3.1.3 The National Classification Scheme: the online content targeted

The Australian regulator targeted online content according to a National Classification Scheme as applied to the film industry that covers a range of content categories. For example, child pornographic content was rated as Refused Classification (RC) and was included in the list of

[536] Communications Legislation Amendment (Content Services) Act 2007 (Cth Australia).

[537] These categories will be explained in Section 4.1.3 below.

[538] The RAS involves a number of administrative procedures to be implemented by online intermediaries in order to limit access to material considered inappropriate to minors. See Restricted Access Systems Declaration (2007). Australian Communications and Media Authority, ACMA . See also ACMA, 'Restricted Access Systems Declaration 2007 - Explanatory Statement', (Australian Communications and Media Authority, 2007) at <http:// www.comlaw.gov.au/> Accessed 22 August 2011.

[539] Previously, ACMA was required to have a suspected R18+ rated content classified by the relevant classification body before issuing any type of take-down notice.

prohibited material, but other types of content (*e.g.* involving sex, nudity or violence) could also be rated prohibited and thus included in the ACMA blocklist.

The Australian National Classification Scheme was established by the Commonwealth Classification Act 1995[540] and comprised the Classification Board (the independent body for classification),[541] Classification Review Board (the review agency), National Classification Code and the Classification Guidelines.[542] The content classification was implemented uniformly by the Classification Board, but restrictions on display and distribution (*e.g.* public exhibition, sale and advertisement of films) were enforced by the relevant State or Territory.[543]

The reason that a National Classification Scheme existed was because in 1995 the Commonwealth, with the agreement of all States and Territories, used its constitutional power under Section 122 of the Constitution to regulate. As a result, all States and Territories each enacted legislation giving effect in their jurisdictions to decisions of Classification Boards and various other parts of the Commonwealth Act and enacted related classification and censorship enforcement provisions, *e.g.* offences for exhibiting or distributing unclassified films and so forth. The enforcement legislation was intended to be uniform nationwide, but in reality it was not, because various States and Territories' legislation had different rules, offences and penalties, and also one or more retained the right to apply, in their own jurisdiction, a different classification decision to, for example, a film than that made by the Commonwealth Classification Board.[544]

The material available online was classified according to categories applied to the film industry[545] and included: G-General; PG-Parental Guidance; M-Mature; MA15+-Mature Accompanied; R18+-Restricted; X18+; and RC-Refused Classification).[546] These categories were applied according to classifiable elements of sex, nudity, violence, language and drug use and themes. For example, the MA15+ material involved content unsuitable for under-15s but it was lawfully screened in free air television. The R18+ material involved content unsuitable for under-18s. The X18+ material involved non-violent sexually explicit material depicting consenting adults.

---

[540] Classification (Publications, Films and Computer Games) Act 1995 (Cth Australia).

[541] Formerly named the Federal Office of Film and Literature Classification.

[542] See generally the 'Classification Website, Australian Commonwealth Government', at <http://www.classification.gov.au/>, accessed 07 September 2011.

[543] Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 337.

[544] See Agreement between [Commonwealth, States & Territories] relating to a revised co-operative legislative scheme for censorship in Australia (1995). at <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~30000intergovernmental+agreement.pdf/$file/30000intergovernmental+agreement.pdf> accessed 06 March 2012.

[545] Except for the 'eligible electronic publication' (*i.e.* digital content that is also available offline as print material), which follows the rules applied to the print publications. See Clause 11, Schedule 7, Broadcasting Services Act 1992 (Cth Australia).

[546] See Clause 7, Division 1 of the Classification (Publications, Films and Computer Games) Act 1995 (Cth Australia).

According to the 2008 Guidelines for Classification, Refused Classification (RC) material involved (i) detailed instruction or promotion in crime, violence or drug use; (ii) the promotion or provision of instruction in paedophilic activity, offensive descriptions of depictions of children; (iii) gratuitous and exploitative depictions of violence or sexual violence; and (iv) bestiality and material the advocates the doing of a terrorist act.[547] Nevertheless, the 2005 National Classification Code arguably gave wider scope to RC material and defined such material as publications that:

> (a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or
>
> (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or
>
> (c) promote, incite or instruct in matters of crime or violence.[548]

In short, both RC and X18+ rated materials were included in the list of prohibited or potential prohibited content.[549] The R18+ and the commercial MA15+ materials might also have been rated prohibited or potential prohibited, unless they were subject to age verification and a Restricted Access Systems (RAS). There were two situations where the MA15+ material might have been rated prohibited or potential prohibited: (i) if commercial video or audio content and not subject to RAS; (ii) if provided by mobile premium services and not subject to RAS.[550] Prohibited content was the material classified as such by the Classification Board. Potential prohibited content was the material not rated yet as such but likely to be so if classified. Content rated prohibited or potential prohibited was included in the ACMA Blocklist and the relevant online intermediary notified according to the notification scheme. Child pornography was rated Refused Classification and targeted by the Australian regulator as prohibited or potential prohibited material.

The regulatory scheme applied to the online environment was perhaps more restrictive than the scheme applied to print publications and offline films and videos. For example, most types of RC rated materials (child pornography excluded) were legal to access and possess in most parts of Australia; X18+ rated material was lawfully sold by shops in the Australian Capital Territory to adults and it was lawful for adults to obtain it by mail order in all Australian States and

---

[547] The Guidelines for the Classification of Films and Computer Games 2008 (Cth Australia) is only a tool to assist the Classification Board.

[548] National Classification Code 2005 (Cth Australia). See also Graham, I., 'Outline of "RC" material', at <http://libertus.net/censor/isp-blocking/au-govplan-refusedclassif.html#RClist>, accessed 06 March; and also Graham, I., 'Detailed information and examples of "RC" material', at <http://libertus.net/censor/isp-blocking/au-govplan-refusedclassif.html#RCexamples>, accessed 06 March.

[549] See Clauses 20 and 21, Schedule 7, Broadcasting Services Act 1992 (Cth Australia) as amended.

[550] This does not apply to MA15+ content that consists solely of text and/or static images, whether or not that type of MA15+ content is commercial. See Clause 2, Schedule 7 of the BSA 1992 as amended.

Territories (except in 'prescribed areas' of the Northern Territory).[551] It may be also the case that the regulatory scheme applied to print publications and offline films and videos (where the classifiers are named and the list of prohibited material known) was more transparent and accountable than the online regulatory scheme (in this case, the ACMA list of prohibited websites was exempt from disclosure and the classifiers were not named).[552]

1.3.1.4 The Australian Communications and Media Authority (ACMA)

The Australian Communications and Media Authority (ACMA)[553] was the latest incarnation of what used to be the Australian Broadcasting Authority (ABA). In short, the ACMA was the Commonwealth statutory agency regulating the broadcasting, telecommunications, radio-frequency spectrum management and online content, including both Internet and mobile phone content in Australia in accordance with Schedules 5 and 7 of the BSA 1992 as amended. Generally it was responsible for investigating complaints about the online content, encouraging and regulating the Internet industry self-regulation scheme, developing public awareness policies and international liaisons in the field.

The amended BSA 1992 established a regulatory model that involved both state-regulation and Internet industry self-regulatory practices; and the ACMA played a central role within this regulatory scheme. In fact, ACMA had a number of powers to make Australian online intermediaries come into line in relation to the content these intermediaries hosted or made available. Generally bodies and associations representing the Internet industry in Australia[554] were encouraged to develop CoPs which were to be registered by the ACMA. The compliance with a CoP was voluntary on the part of online intermediaries, but the ACMA could force them to comply with the CoP if necessary. In addition, the ACMA could impose an industry standard if the CoP was considered deficient, whether partially or totally, and after that the relevant industry standard would be mandatory.[555]

In addition, the ACMA operated an Internet hotline[556] that received complaints from Australian residents about alleged prohibited content. These complaints were usually submitted via the online form (or alternatively via electronic mail, fax or mail) and could be made anonymously. The content reported was investigated and assessed according to the National Classification

---

[551] Graham, I., 'Australia's Internet Censorship System', (updated 11 April 2010) at <http://libertus.net/censor/netcensor.html>, accessed 01 September 2011.

[552] Bambauer, D., 'Filtering in Oz: Australia's Foray into Internet Censorship', *Brooklyn Law School, Legal Studies Paper No. 125,* (2008), p 9.

[553] The ACMA was established on 01 July 2005 after the merge of the Australian Broadcasting Authority (ABA) and the Australian Communication Authority. See the Australian Communications and Media Authority Act 2005 (Cth Australia). See also ACMA, 'Australian Communications and Media Authority - The ACMA is a statutory authority within the federal government portfolio of Broadband, Communications and the Digital Economy', at <http://www.acma.gov.au>, accessed 28 March 2010.

[554] See for example the IIA, 'Internet Industry Association: policy, advocacy and representation for Australian business', at <http://www.iia.net.au/>, accessed 22 August 2011.

[555] See Clause 52, Schedule 5, Broadcasting Services Act 1992 (Cth Australia) as amended.

[556] ACMA, 'The ACMA Hotline: combating child sexual abuse', at <http://www.acma.gov.au/hotline>, accessed 01 September 2011.

Scheme guidelines explored above, and if applicable, it might have been labelled prohibited (if already classified by the Classification Board) or potential prohibited (if not yet classified but likely to be prohibited if properly classified by the Classification Board).

The ACMA hotline did not cover all types of online platforms. It was within its remit to tackle publicly available websites and newsgroups hosted in Australia or abroad; it did not investigate electronic mail messages, instant messaging systems or P2P networks, which were a matter of police investigation. Although the hotline was not required to actively search or monitor the online content, proactive monitoring could be performed.[557] In addition, the ACMA hotline was a member of the INHOPE Association[558] and it was able to notify partner hotlines in relation to alleged child pornographic websites hosted overseas.

1.3.2 Mechanics

The Commonwealth government implemented a complaint-based mechanism that addressed both material considered inappropriate to minors and illegal material, *e.g.* child pornography. It targeted prohibited and potential prohibited material hosted in Australia via notification to the Australian Internet content service and hosting service providers as well as to an Australian police force in the case of more serious offences, for example child pornography; and it targeted the relevant material hosted overseas via notification to the 'accredited' filter vendors in a partnership with the Australian ISPs (*i.e.* under the voluntary user-level filtering scheme).

According to the amended BSA 1992,[559] an Internet service provider was a person that supplied or proposed to supply an Internet carriage service to the public (Clause 8 of Schedule 5). An Internet content host is a person who hosts or proposes to host Internet content in Australia (Clause 3 of Schedule 5). There were different definitions of 'content service' and 'content service provider,' that were relevant to the regulation of online content supplied by a content provider, in Schedule 7 of the amended 1992 Act.

Generally Australian content service and hosting service providers were subject to three notices in relation to material hosted in Australia (*i.e.* link-deletion, service-cessation or take-down notices). On the other hand, ISPs were subject to rules established via the relevant CoP in relation to material hosted overseas but accessible in Australia. In this case, the ACMA included the URL in its blocklist and notified the 'accredited' filter vendors; the Australian ISPs were required to inform their customers about the availability of such filters. The following subsections explores the overall mechanics of the scheme.

---

[557] See ACMA hotline FAQ at ACMA, 'Australian Communications and Media Authority - The ACMA is a statutory authority within the federal government portfolio of Broadband, Communications and the Digital Economy', at <http://www.acma.gov.au>, accessed 28 March 2010. See also Clause 44, Schedule 7, Broadcasting Services Act 1992 (Cth Australia).

[558] See INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010.

[559] Broadcasting Services Act 1992 (Cth Australia) as amended.

1.3.2.1 Protecting children from exposure to online inappropriate content

The protection of minors against inappropriate content involved content categorised or likely to be categorised as MA15+, R18+ or X18+. The Australian online intermediaries (*i.e.* content service and hosting service providers of adult content) were required to implement age verification and restricted access systems before making MA15+ and R18+ available online; X18+ content was rated prohibited or potential prohibited and thus subject to NTD, whether or not it has been subject to a RAS.

The implementation of a RAS was under the Restricted Access Systems Declaration 2007,[560] which established the rules (*e.g.* access application procedures, proof of age, risk analysis, warning provisions and preserving records of age verification) for making age restricted content (*i.e.* legal adult content, not child pornography) available by the relevant online intermediaries in Australia so as to prevent indiscriminate access to age restricted material.

Non-compliant online intermediaries were subject to ACMA notices (*i.e.* take-down, link-deletion or service-cessation notices, or the decision to apply for classification) and there were heavy fees for non-compliance. If the material considered inappropriate was hosted overseas, the relevant URL was included in the ACMA blocklist, the 'accredited' filter vendors were notified, and the ISPs are required to inform their customers about the availability of these 'accredited' filtering software. Nevertheless, this voluntary user-level filtering strategy has been considered ineffective to block access to age restricted content hosted overseas:

> It must be noted that compliance with both take-down notices and content referrals may have no impact at all on the accessibility to internet users of the content in question. Australian-hosted content can simply be removed to overseas hosts, and overseas-hosted content can be accessed simply by not using a content filter. Further, while specific notified sites may be blocked by filter products, it is likely that the same or substantially the same content would be accessible from other overseas sites.[561]

1.3.2.2 Online child pornography hosted in Australia

Child pornographic material was rated RC and labelled prohibited or potential prohibited content. Whenever there was a complaint about alleged child pornographic material hosted in Australia, a notice (*i.e.* take-down, link-deletion or service-cessation notice) was issued by the ACMA to the relevant Australian content service provider or hosting service provider, and an Australian police force was also notified. Complaints about child pornographic content could also be made directly by a member of the public or by the police to the relevant Australian online intermediary. There was a memoranda of understanding negotiated between the ACMA and the Australian police that established a protocol for police notification and content take-

---

[560] Restricted Access Systems Declaration (2007). Australian Communications and Media Authority, ACMA . See also ACMA, 'Restricted Access Systems Declaration 2007 - Explanatory Statement', (Australian Communications and Media Authority, 2007) at <http://www.comlaw.gov.au/> Accessed 22 August 2011. This replaced the Restricted Access Systems Declaration (No 1) (1999). Australian Broadcasting Authority, ABA .

[561] Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 344.

down so as not to compromise criminal investigation (for example, ACMA's investigation was suspended whilst the police investigation takes place).[562] After the notice was issued by the ACMA, the online intermediary was expected to take down the material reported by 6 pm on the next business day, according to Schedule 7 of the amended BSA 1992. Failure to do so was a criminal offence and would lead to heavy fees.

1.3.2.3 Online child pornography hosted overseas

Australian Internet content service and hosting service providers were the online intermediaries based in the country and had the ability to host content in Australia or provide the content from Australia (*e.g.* live content services). As a result, they were easily targeted by the national regulator because their operation and assets were grounded in the country. On the other hand, regulation of access to child pornographic content hosted overseas but accessible in Australia was more problematic.

The ACMA dealt with child pornographic content hosted overseas in accordance with rules established by the registered CoP or by the determined industry standard if applicable (see Clause 40(1)(b), Schedule 5 of the BSA 1992 as amended).[563] The relevant rules were in this case under the 2005 CoP.[564]

Generally the ACMA included the relevant URL into its blocklist (of prohibited and potential prohibited content) and notified the developers of Internet Industry Association 'accredited' family-friendly filters so they could include the URL allegedly containing child pornographic content in their products. The ISPs were then required by the CoP to inform about the availability of these products to their customers, who could voluntary decide whether to use the online content filter or not. As a result, if the customer was not using any filtering system provided by the ISP, s/he could still access the URLs notified.[565] Under this user-level voluntary filtering scheme, neither were the ISPs nor were the customers required by law to use the filters. In addition, a few Australian ISPs offered filtered online access, to any user anywhere in the country, by the means of different filtering technologies (*e.g.* ISP-level filtering, dynamic analysis and blocking of peer-to-peer networks). Nevertheless, it was up to the Australian customer to contract these services or not.

---

[562] ACMA, 'ACMA hotline – Frequently asked questions: 25. What is the relationship between the ACMA and law enforcement?', (updated 02 September 2011) at <http://www.acma.gov.au/WEB/STANDARD/pc=PC_310147#25>.

[563] If there was neither a registered CoP nor a determined industry standard, the ACMA would issue a standard access-prevention notice to each ISP known to ACMA according to Clause 40(1)(c), Schedule 5, BSA 1992 as amended.

[564] IIA, 'Codes for Industry Co-Regulation in Areas of Internet and Mobile Content (Pursuant to the Requirements of the Broadcasting Services Act 1992). May 2005 (includes provisions affecting mobile services). Version 10.4. As Registered by the Australian Broadcasting Authority.', (Internet Industry Association, 2005) at <http:// www.iia.net.au> Accessed 26 September 2011.

[565] Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 341.

In addition to this, a member of an Australian police force[566] was notified, according to Clause 40(1)(a), Schedule 5 of the amended BSA 1992. The ACMA hotline was a member of the INHOPE Association[567] and it could therefore forward these overseas URLs to partner hotlines, if any, where the content was hosted.

More recently, the Australian Internet Industry Association (IIA), in partnership with the Australian Federal Police and Interpol, implemented an ISP-level voluntary filtering scheme to block access to website domains allegedly containing child pornographic material. According to the IIA, two major Australian ISPs were implementing the Interpol blocklist and others were expected to follow suit covering around 80% of the Australian Internet. In addition, there were government plans to implement an ISP-level mandatory filtering scheme via legislation to block access not only to child pornography but the entire range of RC rated content. Yet, this plan has been delayed and it faced substantial criticism. These latest filtering developments are explained below.

1.3.3 Regulatory tools: the ACMA notices and the online content filtering scheme

The ACMA hotline notified Australian online intermediaries (*i.e.* content services - live and stored - and hosting services providers) via three different notices in relation to prohibited or potential prohibited content hosted in Australia: the take-down, service-cessation or link-deletion notices. On the other hand, the relevant content hosted overseas was targeted via the filtering scheme involving Australian ISPs and accredited filter vendors; the voluntarily filtering scheme was employed at the user-level. There were plans from the government to make the scheme mandatory and employed at the ISP-level, to enact it via legislation and to target the entire scope of RC rated material, but this development has been delayed and subject to substantial criticism. More recently, the problem of overseas child pornographic websites has taken the lead in this regard: a few of Australian ISPs, with the support of the IIA, started to voluntarily block access to alleged child pornographic material hosted overseas using the Interpol blocklist.

1.3.3.1 Notice scheme

After a report was made, the ACMA would issue a take-down, a link-deletion or a service-cessation notice to the relevant Australian content service or hosting service provider in relation to prohibited or potential prohibited content hosted in Australia. The relevant law enforcement agency was also contacted in the case of child pornographic content following the terms of a memoranda of understanding.[568] There were high fees for non-compliance and generally the

---

[566] There are various separate police forces in Australia.

[567] See INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010.

[568] ACMA, 'ACMA hotline – Frequently asked questions: 25. What is the relationship between the ACMA and law enforcement?', (updated 02 September 2011) at <http://www.acma.gov.au/WEB/STANDARD/pc=PC_310147#25>.

online intermediary complied with the notice in accordance with the 2008 CoP.[569] This investigation did not find any event of a content/hosting service provider challenging the ACMA notices in court, particularly if child pornographic material was involved. In fact, the burden of challenging these notices in courts outweighed the cheap automatic compliance on the part of the company.

It has been argued elsewhere that the content provider could host the material overseas and arguably avoid the Australian regulator in relation to adult pornography.[570] It seems however that in the case of child pornography, if the content provider was an Australian resident distributing child pornography, s/he was significantly less likely to be able to avoid the police. The complications arise when the child pornographic material was hosted overseas (but accessible in Australia) and the provider of such content was outside the reach of Australian authorities.

1.3.3.2 Filtering scheme

a) The voluntary regime at the user-level for overseas content

The voluntary online content filtering scheme was established by the Broadcasting Services Act 1992 as amended. The amended 1992 legislation established the overall filtering scheme and the relevant Internet industry CoPs established the operational details.

After a report was made and the investigation was carried on, the ACMA hotline updated its own blocklist and notified the prohibited or potential prohibited overseas URL to the 'accredited' filter vendors[571] so they updated their own blocklist. The ACMA notifications were issued on a weekly basis via electronic mail. The content of such notifications (*i.e.* the ACMA blocklist) was exempted from disclosure according to the amended FOI Act 1982[572] but it seemed that the procedures for its distribution to and use by filter vendors needed to be more secure; as demonstrated by the ACMA blocklist being leaked on the Internet in 2009.[573] The blocklist maintained by the 'accredited' filter vendors contained not only the overseas URLs

---

[569] IIA, 'Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992 as amended). Registration Version 1.0 - Current and in Force. As approved by Australian Communications and Media Authority on 10 July 2008', (Internet Industry Association, 2008) at <http://www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/content_services_code_2008.pdf> Accessed 07 September 2011.

[570] See for example Taggart, S., 'Down Under Smut Goes Up Over ', *Wired Magazine,* 02 February 2000, sec. Politics : Law at <http://www.wired.com/politics/law/news/2000/02/34043>, accessed 22 August 2011.

[571] The filter vendors are accredited by the Internet Industry Association which has a list of 'family-friendly filters' available on its webpage. See IIA, 'Internet Industry Association: policy, advocacy and representation for Australian business', at <http://www.iia.net.au/>, accessed 22 August 2011.

[572] Freedom of Information Act 1982 (Cth Australia).

[573] See for example Bingemann, M., 'ACMA blacklist leaked on the internet', *The Australian,* 19 March 2009, sec. Australian IT at <http://www.theaustralian.com.au/news/acma-blacklist-leaked-on-the-internet/story-e6frgb5x-1225700508594>, accessed 24 June 2011.

notified by the ACMA but other URLs provided by overseas companies according to their own criteria of content analysis.[574]

Against this background, all Australian ISPs were required to make customers aware of how they could obtain a filter. This requirement could be met by notifying customers of an URL, *e.g.* on a filter vendor's web site from which the customer could purchase and download a filter. Nevertheless, neither were the ISPs nor their customers required to use these filters: it was a voluntary scheme at the user-level. As a result, although the relevant URL was included in the blocklist, it might be available within Australia if the online content filtering software was not used by the ISP or by their customers. In fact, the customers' take up of filters in Australia has been minimal which made the scheme arguably ineffective to limit access to overseas websites.[575]

The Commonwealth government has attempted to increase the take up of online content filters but it has failed. For example, the NetAlert Programme was launched in 2007 to support the filtering scheme but was shut down later in December 2008.[576] The NetAlert Programme was established in 2007 by the Howard government as part of the National Filtering Scheme. It established a series of measures to help parents protect their children from accessing inappropriate content (education, parental support and free Internet content filters) and involved a budget of 189 million Australian dollars. The Programme provided free online content filtering to Australian Internet users and public libraries which would use 84.4 million Australian dollars. Against the backdrop of a low rate of filtering usage by the Australian customers, the Labor government shut down the Programme in December 2008 replacing it with plans for a mandatory ISP-level filtering scheme.[577]

There were a number of Australian ISPs offering filtered access to the Internet as a commercial service using different filtering technologies (*e.g.* human-based or automated content analysis). For example, the ISPs Webshield,[578] in South Australia, and iTXtreme,[579] in Queensland, already offer filtered access to the Internet based on a blocklist of URLs. Although they were

---

[574] Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Main Report', Internet Industry Association - IIA Australia, 2008) at <http://sydney.edu.au/engineering/it/~bjornl/Main_Report_-_Final.pdf>, accessed 07 September 2011, p 121-26.

[575] Bambauer reports that the low take up of filters has been pictured as a governmental failure by the opposition rather than a result of public disinterest. See Bambauer, D., 'Filtering in Oz: Australia's Foray into Internet Censorship', *Brooklyn Law School, Legal Studies Paper No. 125,* (2008), p 6.

[576] Extended technical support was provided to existing customers until 2010.

[577] See 'NetAlert Protecting Australian Families Online', (Australian Government, 2007) at <http://www.dbcde.gov.au/__data/assets/pdf_file/0011/72956/Protecting-Australian-Families-Online-booklet.pdf> Accessed 25 September 2011. See also Coonan, H., 'NetAlert: Protecting Australian Families Online - Media Release', (Ministry for Communications, Information Technology and the Arts, 2007) at <http://www.minister.dbcde.gov.au/coonan/media/media_releases/netalert_-_protecting_australian_families_online> Accessed 25 September 2011; Best, J., 'AU$189m govt porn blocking plan unveiled', *ZDNet,* 10 August 2007 at <http://www.zdnet.com.au/au189m-govt-porn-blocking-plan-unveiled_print-339281091.htm>, accessed 25 September 2011; Tay, L., 'ICT industry all nostalgic for NetAlert', *itNews - For Australian Business,* 08 July 2012 at <http://www.itnews.com.au/Tools/Print.aspx?CIID=219281>, accessed 25 September 2011.

[578] Webshield, 'Webshield: Australia's First Content Filtered Internet Service Provider', at <http://www.webshield.net.au/>, accessed 07 September 2011.

[579] ItXtreme, 'ItXtreme Family Internet', at <http://www.itxtreme.com.au/>, accessed 07 September 2011.

based in those States, their services were available to anyone anywhere in Australia. The Webshield blocks access to any P2P networks and used a blocklist of URLs provided by overseas filtering companies. Similarly, ItXtreme had its blocklist of URLs updated every hour and it implemented dynamic analysis of online content as it was downloaded by the user.[580] These services were arguably unproblematic as long as implemented on a voluntary basis (*i.e.* when the filtering service was implemented at the request of customers or when customers had the option to contract another filter free ISP in the same location). Nevertheless, safeguards are necessary when the system becomes mandatory so as to avoid opaque and unaccountable private censorship.

b) Towards a mandatory regime at the ISP-level for overseas content: Commonwealth government

> To be perfectly clear, webpages containing pornography, hosted by American companies, still exist and are accessible from any Australian personal computer.[581]

The voluntary online content filtering regime employed at the user-level was unable to stop people accessing overseas prohibited or potential prohibited content if neither the ISP nor the customer used any of the 'accredited' filtering software provided. Against this background, the Commonwealth government was attempting to implement a mandatory filtering scheme at the ISP-level in Australia since 2007, when this new approach to filtering was part of the Labor Party's programme during the election campaign.[582] In order to investigate the feasibility of this mandatory scheme, the Commonwealth government had commissioned a number of studies and live trials in Australia.

In January 2003, the Commonwealth Department of Communications, IT and the Arts appointed Ovum to assess the ISP-level filtering technologies available in the market. The report showed that the available filtering technologies had improved over the years but there were still some issues in relation to the financial cost and administrative requirements that should be taken into account before implementing a mandatory scheme nationwide.[583]

---

[580] Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Main Report', Internet Industry Association - IIA Australia, 2008) at <http://sydney.edu.au/engineering/it/~bjornl/Main_Report_-_Final.pdf>, accessed 07 September 2011p 50-2.

[581] Duffy, J., 'Toothless Tiger, Sleeping Dragon: Implied Freedoms, Internet Filters and the Growing Culture of Internet Censorship in Australia.', *Murdoch University Electronic Journal of Law,* 16(2) (2009), 91-105, p 94.

[582] Ibid , p 94 and 97. Duffy has metaphorically addressed this increased regulatory stance (*i.e.* from the current voluntary scheme to a mandatory regime) as a move from a 'toothless tiger' towards a 'sleeping dragon'.

[583] Parry, J., et al., 'Internet content filtering A Report to the Department of Communications, IT and the Arts. Version 1.0', Ovum, 2003) at <http://www.dbcde.gov.au/__data/assets/file/0016/10915/Ovum_Report_-_Internet_content_filtering.rtf.>, accessed 07 September 2011.

Similarly, Collins *et al*.[584] conducted in September 2007 a study commissioned by the Department of Broadband, Communications and the Digital Economy (DBCDE).[585] The investigation addressed the impact of ISP-level online content filtering on Australian online intermediaries and aimed to inform future policymaking in the field. Generally the study found that the impact of mandatory ISP-level filtering in Australia may be significant, because of the diversity and lack of preparation of the ISP industry. The report emphasised the importance of resolving a series of legal and businesses aspects (for example exemption from criminal liability for possessing, creating and distributing the blocklist of URLs) before this policy was implemented nationwide.

Following a ministerial direction received in June 2007, the ACMA commissioned a filtering trial in 2008 to assess the performance of ISP-level filtering using the ACMA Blocklist, which encompasses a range of prohibited and potential prohibited content available online (*i.e.* RC, X18+, R18+ and commercial MA15+).[586] The trial was conducted in a closed laboratory environment and assessed the performance, effectiveness, scope and adaptability of six online filtering products available in the market. It found that filtering technology has advanced significantly (*i.e.* more filters are available and implemented overseas, they showed low degradation performance and were more narrow and customisable). Nevertheless, it reports that the products tested were yet unable to filter content available via non-web protocols (such as emails, file transfer and P2P).

It was unclear whether the proposed mandatory filtering scheme would filter the entire range of categories included in the ACMA blocklist or only the RC category.[587] Nevertheless, the DBCDE presented in December 2009 a series of measures for online regulation, including the proposed mandatory ISP-level filtering which would apparently target only RC rated online content.[588] In line with this was the fact that the RC category was under review following a request of the Commonwealth government and, as a result, the proposed mandatory scheme has

---

[584] The study was on behalf of the Internet Industry Association (IIA). See Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Main Report', Internet Industry Association - IIA Australia, 2008) at <http://sydney.edu.au/engineering/it/~bjornl/Main_Report_-_Final.pdf>, accessed 07 September 2011.

[585] See DBCDE, 'Department of Broadband, Communications and the Digital Economy', at <http://www.dbcde.gov.au/>, accessed 11 September 2011.

[586] See ACMA, 'Closed Environment Testing of ISP-Level Internet Content Filtering: Report to the Minister for Broadband, Communications and the Digital Economy', ACMA, 2008) at <http://www.acma.gov.au>, accessed 28 August 2011. The trial was not concerned with the balance of costs and benefits nor with the potential to be circumvented. It has been suggested that the filtering software tested employed a more complex technology than those applied solely to block access to child pornography websites because of the wider range of content of ACMA blocklist.

[587] The government presented a filtering proposal in 2007 but changed it in 2009. See comparative table in Graham, I., 'Overview / Summary: AU Gov't Mandatory ISP Blocking/Censorship Plan', at <http://libertus.net/censor/isp-blocking/au-govplan-overview.html>, accessed 01 September 2011. See also Duffy, J., 'Toothless Tiger, Sleeping Dragon: Implied Freedoms, Internet Filters and the Growing Culture of Internet Censorship in Australia.', *Murdoch University Electronic Journal of Law,* 16(2) (2009), 91-105, p 102.

[588] DBCDE, 'ISP filtering - frequently asked questions', (updated 27 May 2011) at <http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering_-_frequently_asked_questions>, accessed 28 August 2011.

been put on hold since then.[589] The review of the Refused Classification category was being undertaken by the Australian Law Reform Commission (ALRC) as part of an overall review of the National Classification System. The ALRC has been asked to submit its final report to the Government by 31 Jan 2012.[590]

The mandatory filtering proposed by the Commonwealth government was expected to include a number of provisions to increase the transparency and accountability of the scheme. Nevertheless, it was unclear whether: (i) the scheme would be implemented via Commonwealth legislation or administrative regulation;[591] (ii) there would be any further guidance established via an Internet industry CoP; (iii) there would be any statutory safeguards to make the scheme transparent and accountable.[592]

c) Blocking overseas child pornographic websites voluntarily at the ISP-level: IIA, AFP and Interpol

Although the proposed mandatory filtering scheme against RC rated content has been delayed pending the review of the RC category, the problem of child pornography has taken the lead in relation to the implementation of a blocking scheme. Overseas child pornography was already being blocked voluntarily at the ISP-level after major Australian ISPs (*i.e.* Telstra and Optus, and the small Cyberone) started to voluntarily block access to overseas websites domains (not individual URLs) allegedly hosting child pornographic content in July 2011.[593] The Internet Industry Association announced the scheme as a partnership with the Australian Federal Police and Interpol[594] and, although the voluntary scheme was said to target only child pornography, scope creep has been alleged.[595]

---

[589] See Conroy, S., 'Media Release: Outcome of consultations on Transparency and Accountability for ISP Filtering of RC content', (2010) at <http://www.minister.dbcde.gov.au/media/media_releases/2010/068> Accessed 06 March 2012; and also LeMay, R., 'Filter delayed while RC is reviewed', *ZDNet,* 09 July 2010 at <http://www.zdnet.com.au/filter-delayed-while-rc-is-reviewed-339304437.htm>, accessed 22 August 2011.

[590] See ALRC, 'National Classification Scheme Review', (Sydney, Australia: Australian Law Reform Commission, 2011) at <http://www.alrc.gov.au/inquiries/national-classification-review> Accessed 06 March 2012.

[591] According to Moses, the mandatory filtering scheme proposal is unlikely to receive support from the Australian Senate. See Moses, A., 'Web censorship plan heads towards a dead end', *The Sydney Morning Herald,* 26 February 2009, sec. Technology at <http://www.smh.com.au/articles/2009/02/26/1235237810486.html>, accessed 07 September 2011.

[592] There are a number of different ways to implement filtering at the ISP-level. See Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Main Report', Internet Industry Association - IIA Australia, 2008) at <http://sydney.edu.au/engineering/it/~bjornl/Main_Report_-_Final.pdf>, accessed 07 September 2011, p 15.

[593] Conroy, S., 'Media Release: Outcome of consultations on Transparency and Accountability for ISP Filtering of RC content', (2010) at <http://www.minister.dbcde.gov.au/media/media_releases/2010/068> Accessed 06 March 2012. The media release reports that three ISPs (*i.e.* Telstra, Optus and Primus) are implementing the scheme but there have not been any reports of Primus blocking against any Interpol list. See LeMay, R., 'ISPs don't have to collect voluntary filter data', *Delimiter*, (2011) at <http://delimiter.com.au/2011/10/26/isps-dont-have-to-collect-voluntary-filter-data/> accessed 06 March 2012.

[594] See IIA, 'Internet industry moves on blocking child pornography', *Internet Industry Association Australia,* 2011 at <http://www.iia.net.au/index.php/all-members/892-internet-industry-moves-on-blocking-child-pornography.html>, accessed 07 September 2011. See also Ozimek, J., 'Aus gov, ISPs book seats for firewall demolition: new filters to catch nasty stuff ', *The Register,* 23 August 2010 at <http://www.theregister.co.uk/2010/08/23/aus_firewall_isp/ >, accessed 22 August 2011; and particularly pages 104-7 from 'Official Committee Hansard - SENATE - ENVIRONMENT AND COMMUNICATIONS LEGISLATION COMMITTEE: Estimates', (Canberra, 2011) at <http://www.aph.gov.au/hansard/senate/commttee/s380.pdf>, accessed 06 March 2012.

[595] See Jacobs, C., 'Conroy: Filter alive and kicking', *Electronic Frontiers Australia,* 27 May 2011 at <http://www.efa.org.au/2011/05/27/filter-alive-and-kicking/>, accessed 01 September 2011.

The ISP-level voluntary filtering scheme blocked access to a list of websites domains provided by Interpol, which allegedly contained overseas websites of 'the worst' child pornographic content.[596] According to the IIA, the relevant CoP to regulate the voluntary blocking scheme in relation to child pornographic content in Australia would be delivered soon and the Association expected a voluntary compliance of around 80 to 90% from Australian ISPs, but this has failed to materialise as of January 2012; there has been no media reports of any more than the first three ISPs abovementioned. The IIA reported that those who accessed the blocked webpage domain would be forwarded to an Interpol webpage, explaining the reasons for the blocking and the relevant appeal procedures; the appeal procedures would be managed by the Interpol and AFP. In addition, it reported that those accessing the blocked domain would not be tracked whether accessing it intentionally or inadvertently.[597]

LeMay argues that this scheme has so far failed to meet principles of transparency, accountability and legitimacy (*e.g.* the filtering scheme was being implemented without transparency by the Australian ISPs, there was no public oversight nor reviewing procedures, the blocklist was managed by an international organisation, there was strong potential for scope creep and the ISP's customers were not informed about the changes in their Internet access).[598] The scheme was not implemented via legislation but it was based on agreements negotiated between the relevant organisations (*i.e.* IIA, AFP, Interpol and the participant ISPs) and centred on the blocklist developed and maintained by an international law enforcement agency.

It has been argued however that the legal framework for such a scheme was under Section 313 of the Telecommunications Act 1997[599] about the obligations of carriage service providers to help the police enforcing the criminal laws, but the use of such provision to provide 'help' in the form of an ISP-blocking system was controversial. For example, Graham believes that Section 313 of the 1997 Act did not, of itself, enable the AFP to require ISPs 'to do anything'.[600]

It was unclear whether the voluntary scheme implemented in 2011 and supported by the IIA would be part of the planned legislated and mandatory scheme based on the ACMA list. In fact, this seemed unlikely given the comments made by the Minister for Communications Senator Conroy on 18 October 2011.[601] For him, the government-backed ISP-level blocking scheme was

---

[596] See Interpol's criteria in INTERPOL, 'Criteria for inclusion in the "Worst of"-list', (Interpol, 2011) at <http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list> Accessed 06 March 2012.

[597] See generally IIA, 'Internet industry moves on blocking child pornography', *Internet Industry Association Australia,* 2011 at <http://www.iia.net.au/index.php/all-members/892-internet-industry-moves-on-blocking-child-pornography.html>, accessed 07 September 2011.

[598] See LeMay, R., '5 reasons to worry about the Interpol filter', *ZDNet,* 11 July 2011 at <http://www.zdnet.com.au/5-reasons-to-worry-about-the-interpol-filter-339318271.htm>, accessed 12 September 2011. See also LeMay, R., 'Does the filter breach user agreements?', *ZDNet,* 12 July 2011 at <http://www.zdnet.com.au/does-the-filter-breach-user-agreements-339318375.htm>, accessed 12 September 2011.

[599] Telecommunications Act 1997 (Cth Australia).

[600] See Graham, I., 'Australian ISPs Voluntary Filtering/Blocking', at <http://libertus.net/censor/isp-blocking/au-ispfiltering-voluntary.html>, accessed 06 March 2012.

[601] See pages 104-7 at 'Official Committee Hansard - SENATE - ENVIRONMENT AND COMMUNICATIONS LEGISLATION COMMITTEE: Estimates', (Canberra, 2011) at <http://www.aph.gov.au/hansard/senate/commttee/s380.pdf>, accessed 06 March 2012.

expected to target child pornography as defined under the Australian law (not from an overseas police agency), to include robust transparency and accountability mechanisms and to be enforced via legislation (so as to include reluctant Australian ISPs).[602] Despite these grounds for criticisms, the government has generally welcomed the blocking initiative from IIA, AFP, Interpol and the participating Australian ISPs, because it has proved that such a scheme was technically possible, it paved the way for implementing the government's scheme, and it did not slow the Internet down in the country as some might have feared.[603]

Finally, it was unclear whether the Australian ISPs were implementing filtering mechanisms to tackle child pornography before the scheme was launched, but a number of them already provide filtered access at the ISP-level to the Internet in Australia[604] and this raised concerns about the potential for opaque private censorship.

1.3.4 The nature of the regulatory scheme: state and self-regulation

The Australian online content regulatory scheme has been labeled 'co-regulatory' because it involved not only the state as the main regulator but private actors via the Industry association and the CoPs.[605] The regulatory scheme was considered to be complaint-based but both the Commonwealth regulator and the online intermediaries could proactively monitor the availability of child pornographic content at their own discretion. In line with the discussion made in Section 3.3 of Chapter 2, the regulatory scheme implemented in Australia had all attributes of hybrid regulation. The state was the central regulatory actor (*e.g.* rules were established via legislation and there was a statutory regulatory agency) but a number of responsibilities were delegated to private actors (*e.g.* Internet industry CoP) and the Internet user (*e.g.* via the user-level voluntary filtering scheme). Although the overall regulatory framework was established via legislation, the remaining specificities (*i.e.* the notification scheme, handling complaints, activity of content assessors, filtering programme etc.) were established via CoP designed by the Internet Industry Association. The Commonwealth regulator had a strong legislative mandate to force Australian online intermediaries to come into line in relation to the content available on the Internet; the CoPs were registered and monitored

---

602 LeMay, R., 'We'll filter when the law says: Internode', *ZDNet,* 05 July 2011 at <http://www.zdnet.com.au/well-filter-when-the-law-says-internode-339317922.htm>, accessed 12 September 2011. See also Wyres, M., 'I'm dumping Telstra for the voluntary filter', *ZDNet Australia,* 24 June 2011 at <http://www.zdnet.com.au/im-dumping-telstra-for-the-voluntary-filter-339317382.htm>, accessed 12 September 2011.

603 See pages 104-7 at 'Official Committee Hansard - SENATE - ENVIRONMENT AND COMMUNICATIONS LEGISLATION COMMITTEE: Estimates', (Canberra, 2011) at <http://www.aph.gov.au/hansard/senate/commttee/s380.pdf>, accessed 06 March 2012.

604 Some of them were known to be offering filtered access commercially. See the case of iTXtreme and Webshield mentioned above.

605 See Alston, R., 'The Government's Regulatory Framework for Internet Content', *University of New South Wales Law Journal,* 23(1) (2000), 192-97. See also Wright, A., 'Australia: A Case Study on Internet Content Regulation', Australian Broadcasting Authority, 2002) at <http://www.acma.gov.au/webwr/aba/newspubs/speeches/documents/aw_unesco_paper.pdf>, accessed 22 August 2011, p 14.

by the Commonwealth regulator, which had powers to enforce compliance under threat of heavy fees and enforce its own industry standard if necessary.[606]

1.3.4.1 The Codes of Practice (CoP)

The legal framework for the CoPs were under Schedule 5 of the BSA 1992 as amended. The compliance with the CoP was voluntary on the part of the ISPs but the ACMA could force them to comply with the registered CoP if necessary. As a result, the Australian online intermediaries were subject to a number of obligations not only established by the Parliament but also by the Commonwealth regulator and the relevant Internet industry association. Division 4 and Division 5, Schedule 5 of the 1992 Act as amended regulated the industry CoPs and industry standards, respectively. There were two Internet industry CoPs registered and in force in Australia: (i) the 2005 CoP[607] regulated the Australian ISPs and Internet content hosts; and (ii) the 2008 CoP[608] regulated the Australian content service providers and hosting service providers following the 2007 amendments of the 1992 Act.

The 2005 CoP was registered by the ABA on 26 May 2005. It addressed Schedule 5 of the amended 1992 Act and encompassed three Codes of Practice in the area of Internet and mobile content. Its Code 1 dealt with the obligations of the Australian Internet content hosts (ICHs) in relation to content hosted in Australia (*i.e.* take-down procedures). The Code 2 targeted the Australian ISPs in relation to content hosted in Australia (*i.e.* regulating access to minors within Australia). Finally, the Code 3 addressed the Australian ISPs in relation to content hosted overseas. The Code 3 established, in Clause 19.2, the notification scheme required by Section 40(1)(b) of Schedule 5 (of the amended 1992 Act). According to this, the ACMA notified the suppliers of family-friendly filters directly and ISPs on a regular basis about the relevant prohibited or potential prohibited content hosted overseas. The ISPs were required to inform their customers about the available family-friendly content filters, but it was unclear whether the ISPs voluntarily implemented any ISP-level filtering strategy based on the notifications received from the ACMA. It was unclear how often these notifications about overseas URLs were made to ISPs.[609]

---

[606] Yet, this investigation found no evidence that either the ABA or ACMA ever had ordered an ISP or ICH to comply with a CoP; it may also be the case that not all of them comply with all requirements of the IIA's CoP, because these requirements may be too onerous or impractical administratively.

[607] IIA, 'Codes for Industry Co-Regulation in Areas of Internet and Mobile Content (Pursuant to the Requirements of the Broadcasting Services Act 1992). May 2005 (includes provisions affecting mobile services). Version 10.4. As Registered by the Australian Broadcasting Authority.', (Internet Industry Association, 2005) at <http://www.iia.net.au> Accessed 26 September 2011.

[608] IIA, 'Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992 as amended). Registration Version 1.0 - Current and in Force. As approved by Australian Communications and Media Authority on 10 July 2008', (Internet Industry Association, 2008) at <http://www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/content_services_code_2008.pdf> Accessed 07 September 2011.

[609] One Australian expert, consulted during the validation scheme, said that ACMA often did not notify ISPs about overseas URLs regardless of what the CoP has established.

The 2008 CoP was registered on 10 July 2008 following the 2007 amendments.[610] It only dealt with Schedule 7 of the amended 1992 Act and aimed to provide legal guidelines for compliance to Australian content service providers and hosting service providers. Generally it established the take-down regime to the online content with an Australian connection (*i.e.* stored or live content hosted in or produced from Australia) which was subject to the take-down or link-deletion notices (in relation to stored content), or the service-cessation notice (in relation to live content). Part C of the 2008 CoP established the handling of complaints of end-users in addition to the ACMA notifications.

Generally legal liability of Australian online intermediaries in relation to the content they hosted or made available was established in Clause 91 of Schedule 5 of the amended 1992 Act. They were exempt from liability under State of Territory laws as long as they were unaware of the criminal nature of the content they carried and had no obligation to proactively search this awareness.

Section 1 above addressed the laws and regulations to limit access to online child pornography in Australia. First, it explored the history of online content regulation particularly in relation to child pornography. Second, it addressed Commonwealth, State and Territory criminal laws tackling the production, distribution and possession of online child pornography in addition to the investigatory powers of law enforcement authorities. Third, it explored Commonwealth online content regulatory laws and regulations to limit access to online child pornographic material, be it hosted in Australia or overseas. Section 2 explores the laws and regulations to limit access to online child pornography in Brazil.

2 Brazil

The commercial sexual exploitation of children in Brazil is an old phenomenon. Nevertheless, the production, distribution and collection of online child pornography became a national concern in the mid-1990s soon after the development of the commercial Internet in the early 1990s.[611] The major concern of the regulatory policies put in place was the availability of child pornographic content on both commercial and non-commercial overseas websites,[612] and this was the reason why regulators started to target Brazilian[613] Internet content service, hosting service, and service providers more closely after 2005.

Brazil had outdated anti-child pornography laws and no comprehensive legislation to regulate the activities of online intermediaries amidst a pro-self-regulation agenda that was never

---

[610] Communications Legislation Amendment (Content Services) Act 2007 (Cth Australia).

[611] For an overall description about the development of commercial Internet in Brazil, see ch 4 in Lemos, R., *Direito, Tecnologia e Cultura* (Rio de Janeiro: Ed. FGV, 2005).

[612] Although part of the child pornographic material found on the public Internet and reported to authorities was hosted in Brazil, most reported content was hosted overseas.

[613] Or foreign companies with a representative office in Brazil such as Google Inc., Microsoft and NewsGroup International.

systematically implemented by the Internet industry. On the other hand, law enforcement authorities lacked legal and regulatory tools to facilitate: (i) the immediate removal of alleged child pornography content hosted in Brazil (or hosted overseas but produced, distributed or accessed by people in Brazil); (ii) the identification of alleged offenders and; (iii) the preservation of evidence so as to successfully criminally prosecute alleged offenders.

Against this background, substantial changes occurred after 2005 in relation to anti-child pornography laws and the regulatory landscape. This was first achieved via agreements negotiated between law enforcement authorities and online intermediaries (*e.g.* content service and hosting service providers) to establish measures for notice and take down child pornographic material hosted domestically. New anti-child pornography legislation was enacted in 2008 and amended the old legislation in regard to the definition, types of content, offences, defences and penalties associated with online child pornography. The 2008 legislation put in place a provision that established a notice and take down scheme but only in relation to online child pornographic content.

Later in 2009, agreements were negotiated amongst telcos, backbone providers and law enforcement authorities to facilitate the identification of alleged offenders, preserve evidence and improve cooperation with police. These developments occurred amidst no specific legislation regulating the activities of online intermediaries in Brazil. In addition, other agreements were negotiated with online intermediaries, such as online payment systems to target commercially driven child pornography websites, and with a number of law enforcement authorities, governments bodies and private actors to establish a reporting scheme. Amongst other things, these developments made a number of online intermediaries implement content removal initiatives of their own (*e.g.* automated filtering via file hashing, content analysis and proactive monitoring) without any clear guidance or legislated safeguards to avoid potential abuses.

This section explores regulatory developments aimed at limiting access to child pornography available on the Internet in Brazil.[614] Subsection 2.1 addresses the historical context and political processes that shaped these developments. Subsequently, Subsection 2.2 describes the Brazilian anti-child pornography laws, and Subsection 2.3 explores the regulatory framework in detail.

2.1 Historical context

The problem of child pornographic content available on the Internet gained visibility in Brazil after the mid-1990s, when the commercial Internet started to flourish, and was largely shaped by what has been discussed and developed at the international level.

[614] It focused on Brazilian anti-child pornography laws and regulatory measures as of until January 2011.

For example, following the 1989 UN Convention on the Rights of the Child,[615] the 1st World Congress against the Commercial Sexual Exploitation of Children[616] (CSEC) addressed the problem of online child pornography and recommended the reform of legislation and law enforcement strategies to tackle the problem both nationally and internationally. After the 1st World Congress on CSEC other international conferences (*e.g.* the 1998 ECPAT Expert's Meeting,[617] the 1999 UNESCO Expert's Meeting,[618] the 1999 UNESCO Brazil Meeting,[619] the 2001 2nd World Congress against CSEC,[620] and the 2001 CEDECA-BA International Conference[621]) continued to pursue the reform of national and international legislation, improvement of law enforcement capabilities, creation of Internet hotlines to report alleged illegal content, stronger involvement of Internet industry and further international cooperation. Generally these were the issues debated at the international level that shaped the media landscape and national agenda in Brazil after the mid-1990s.

UNESCO Brasil launched in 1999 the '*ForÉtica-BR,*' a multi-stakeholder committee devoted to discuss and propose public policies in relation to the problem of online child pornography available on the Internet in Brazil. The committee met a few times and eventually published a book,[622] but the group lacked the political force to inform and propose public policies in this regard. In addition, a Round-table[623] organised by the CEDECA-BA[624] in December 2000 was the starting point of a pilot-Internet hotline, the CEDECA-BA Hotline-BR,[625] created to receive and process reports about the availability of child pornographic content on the Internet in Brazil.

---

615 UN Convention on the Rights of the Child. Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989. Entry into force 2 September 1990, in accordance with article 49. 1989 (United Nations).

616 '1st World Congress against Commercial Sexual Exploitation of Children. Declaration and Agenda for Action.', (Stockholm: World Congress against CSEC, 1996) at <http://www.csecworldcongress.org/en/stockholm/index.htm>, accessed 18 April 2011.

617 ECPAT, 'Child Pornography and the Internet Expert's Meeting. 28-29 May 1998.', (Lyon: ECPAT International, 1998) at <http://www.ecpat.net/eng/Ecpat_inter/projects/preventing_pornography/prevent.asp>, accessed 13 May 2005.

618 UNESCO, 'Expert's Meeting. 18-19 Jan 1999.', (Paris: UNESCO, 1999) at <http://www.unesco.org/webworld/child_screen/conf_index.html>, accessed 13 May 2005.

619 UNESCO, 'Fórum Brasileiro de Ética pela Infância e Adolescência na Internet: ForÉtica-BR', (Brasilia-DF: UNESCO BRASIL, 1999) at <http://www.dialdata.com.br/foretica>.

620 '2nd World Congress against Commercial Sexual Exploitation of Children. Yokohama Global Commitment', (Yokohama: World Congress against CSEC, 2001) at <http://www.csecworldcongress.org/en/yokohama/index.htm>, accessed 18 April 2011.

621 For information about this conference, see CEDECA-BA, 'Pornografia Infanto-juvenil na Internet: Uma Violação aos Direitos Humanos', at <http://www.cedeca.org.br/publicacoes/conferencia.pdf>, accessed 18 April 2011.

622 See UNESCO, 'Fórum Brasileiro de Ética pela Infância e Adolescência na Internet: ForÉtica-BR', (Brasilia-DF: UNESCO BRASIL, 1999) at <http://www.dialdata.com.br/foretica> See also UNESCO (ed.), *Inocência em Perigo: abuso sexual de crianças, pornografia infantil e pedofilia na Internet* (São Paulo: UNESCO, Garamound and ABRANET, 1999).

623 See Reis, F., 'Relatório sobre a Mesa-redonda contra a Pedofilia na Internet', (Salvador-BA: CEDECA-BA, 2000) at <http://www.fabiorei.com>, accessed 18 April 2011.

624 CEDECA-BA was a non-governmental organisation that provided free of charge legal and psychological assistance to children victims of sexual abuse in Brazil. See CEDECA-BA, 'Centro de Defesa da Criança e do Adolescente da Bahia', at <http://www.cedeca.org.br>, accessed 31 August 2010.

625 CEDECA-BA, 'HotlineBR CEDECA-BA', at <http://www.hotlinebr.org.br>, accessed 03 November 2005. Note that this hotline is no longer available.

Following this, the 1990 anti-child pornography legislation was updated in 2003[626] and, in 2004, Brazil ratified the 2000 UN Optional Protocol.[627] It was also in 2004 that the Brazilian Parliament[628] published the final report from a Mixed Parliamentary Commission Inquiry created to investigate the commercial sexual exploitation of children in Brazil in general, but which has made a number of recommendations, for example to criminalise a number of conducts and increase penalties in relation to online child pornography offences.[629] Another multi-stakeholder committee, similar to the one created in 1999, was launched by the federal government in 2004 to design a national action plan against child pornography available on the Internet in Brazil,[630] but after a few meetings this committee lost vigour and such a national action plan was neither materialised or implemented.[631] The UN Special Rapporteur issued a dossier in 2004 with recommendations against the problem based on feedback received from a number of countries, including Brazil;[632] these recommendations were generally in line with the international agenda discussed above.

In addition, improvements were made to the CEDECA-BA Hotline-BR in 2004.[633] Also in 2004, the CEDECA-BA commissioned a study to identify regulatory initiatives implemented in Brazil against the proliferation of child pornographic content on the Internet.[634] The investigation addressed the activities of Brazilian Internet hotlines, the Brazilian Federal Police,[635] the Parliament and the Internet industry. It found that a number of Internet hotlines were operating in 2005.

Generally the law enforcement authorities provided channels to receive reports from the public, but non-governmental institutions (*e.g.* the CEDECA-BA Hotline-BR, Censura.Com,[636]

---

626 The development of the anti-child pornography laws in Brazil will be discussed in Section 3.

627 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations).

628 The Brazilian Parliament is a bicameral National Congress consisting of the '*Senado Federal*' (upper chamber) and the '*Câmara dos Deputados*' (lower chamber).

629 See CPMI, 'Relatório Final da Comissão Parlamentar Mista de Inquérito da Exploração Sexual de Crianças e Adolescentes', (Brasília-DF, Brasil: Senado Federal, 2004) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=56335&tp=1> Accessed 14 March 2012, p 306-8.

630 This multi-stakeholder Committee ('Subcomissão Temática de Enfrentamento à Pedofilia e à Pornografia Infantil na Internet') was launched in July 2004 by the Federal Government after they published the report Reifschneider, E. and Reis, A., 'Pesquisa sobre Pornografia Infantil na Internet – Brasil. Proyecto sobre Tráfico de Niños, Pornografia Infantil en Internet y Marcos Normativos en el Mercosur, Bolívia e Chile', (Montevideo-Uruguay: Instituto Interamericano Del Niño, 2004) at <http://www.iintpi.net/informes/index.php>, accessed 25 May 2005.

631 The 2004 Committee resembled the 1999 '*ForÉtica-BR*' initiative, because they both lost the political vigour soon after inception.

632 See Petit, J., 'Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the sale of children, child prostitution and child pornography. E/CN.4/2005/78, 23 December 2004.', (New York: United Nations, 2004) at <http://www.unhcr.org/refworld/category,REFERENCE,UNCHR,,,42d66e480,0.html>, accessed 30 June 2010.

633 The CEDECA-BA Hotline-BR attended the INHOPE Meeting on 12-14 May 2004 in Italy, and secured financial funding from the Canadian Government to continue its operation during 2005.

634 See Oliveira, T. and Reis, F., *Pornografia Infantil na Internet: o enfrentamento no Brasil (unpublished)* (Salvador-BA, Brasil: CEDECA-BA, 2006) 104p.

635 DPF, 'Polícia Federal', at <http://www.dpf.gov.br/>, accessed 25 April 2011.

636 Miranda, A. and Miranda, R., 'Campanha Censura.Com', at <http://www.censura.com.br/>, accessed 25 April 2011.

PORTAL-KIDS,[637] and ABRAPIA[638]) received reposts and faced a number of problems including the lack of permanent financial support and the limited feedback received from both the relevant online intermediaries and the Federal Police. Notably, the investigation found that there was no centralised Internet hotline service liaising with the law enforcement authorities so as to avoid the duplication of reports. Evidence also suggested that the Federal Police lacked both technical expertise and financial support to tackle the problem. It was also the case that they were not able to effectively cooperate internationally. In addition, taking into account legislative bills under consideration by the Parliament, the investigation made a number of recommendations for legislative reform that were used to update anti-child pornography laws in 2008.[639]

Finally, the study showed that the Brazilian Internet industry had so far little involvement with the problem of child pornography and promoted limited feedback whenever demanded. This was the case with the *Comitê Gestor da Internet no Brasil*[640] (CGI.br), a multi-stakeholder commission (with representatives from the federal government, civil society, academia, and Internet industry) created by the Federal Government in 1995 to coordinate all Internet services in Brazil (for example domain names and Internet governance), and formulate public polices, but whose work in relation to child pornographic content regulation has been close to nothing.[641] Until January 2012, there was no comprehensive national legislation to regulate the operation of online intermediaries in general (except for the notice and take down - NTD of child pornographic content available on the Internet established under the 2008 legislation) nor was there a national code of conduct (CoC) to guide their operation. Nevertheless, there were parliamentary discussions in this regard, and they are discussed later.

Amidst no comprehensive legislation to regulate the activities of online intermediaries and a pro-self regulation political discourse that was never systematically implemented, the Internet industry avoided setting up any reporting mechanism, public awareness programmes nor any other initiative to tackle the problem of child pornography available on the Internet in Brazil. Generally they removed alleged child pornographic content from their servers once notified, but hardly gave any feedback about the reports they received from Internet hotlines nor did they develop any regulatory scheme voluntarily (*e.g.* to record access logs, date and IP addresses) to

---

637 'Portal Kids', at <http://www.portalkids.org.br/>, accessed 25 April 2011.

638 ABRAPIA, 'Do Marco Zero a Uma Política Pública Proteção à Criança e ao Adolescente', (Rio de Janeiro-RJ: ABRAPIA: Associação Brasileira Multiprofissional de Proteção à Infância e à Adolescência, 2003) at <http://www.abrapia.org.br>, accessed 12 June 2004.

639 See pages 179-83 at CPMI, 'Relatório Final da Comissão Parlamentar Mista de Inquérito da Exploração Sexual de Crianças e Adolescentes', (Brasília-DF, Brasil: Senado Federal, 2004) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=56335&tp=1> Accessed 14 March 2012.

640 CGI, 'Comitê Gestor da Internet no Brasil', at <http://www.cgi.br/>, accessed 14 March 2012.

641 A federal police officer attended the CGI.br's meeting on 09 April 1999 and exposed the difficulties that law enforcement agencies have to collect evidence in relation to child pornographic content available on the Internet. The panel has decided to establish minimum requirements that relevant online intermediaries should follow in these cases, but this initiative has never came to light. See CGI, 'Reunião de 09 de abril de 1999', (Porto Alegre-RS, Brasil: Comitê Gestor da Internet no Brasil, 1999) at <http://www.cgi.br/acoes/1999/rea-1999-04.htm>, accessed 13 March 2012.

help law enforcement agencies identifying alleged offenders; their key concern was to avoid any regulatory measures that could increase costs and minimise profit.

After June 2005, law enforcement authorities, particularly the Federal Prosecution Service in the State of São Paulo (the MPF-SP)[642] negotiated agreements with major online intermediaries in the State of São Paulo so as to establish common standards to remove material reported as potentially criminal, facilitate the identification of alleged offenders and preserve relevant evidence for criminal investigation.[643] These agreements were gradually replicated by other law enforcement authorities in other regions of Brazil.

In addition, another Internet hotline was created in December 2005. The CEDECA-BA Hotline-BR stopped operating in the late 2005 because of severe financial hardship. Based on the expertise accumulated there, its former members founded another institution named Safernet Brasil[644] and started receiving, processing and forwarding reports in January 2006. These reports were mainly about the availability of child pornographic material found in commercial and non-commercial overseas websites and, particularly, in the social network Orkut[645] owned by the US company Google. Orkut achieved substantial success in the Brazilian social networking market in relation its rival Facebook.[646] Most reports received by Safernet Brasil was hosted in Orkut's servers in the US and only a few reports were about child pornographic websites hosted in Brazil. Although child pornographic content was produced, distributed and accessed by Brazilian nationals via Orkut, the material was hosted in Google's servers in the US, outside the immediate jurisdiction of Brazilian law enforcement authorities. There were reports about child pornographic content exchanged via anonymised P2P and other Internet applications, but Safernet could do nothing about them as it was a matter of police investigation.

The MPF-SP has also received a growing number of complaints about child pornographic content available in Orkut. Although the removal of material reported was not often immediate,[647] the problem here was that Google Brasil, the Google Inc. subsidiary in Brazil, refused to disclose information about access logs and personal data of Brazilian users to law enforcement authorities, even though there was a judicial order for such request. Google Brasil argued that the information requested by the Brazilian authorities was located in the US and

---

642 The Brazilian Federal Prosecution Service Office in the State of São Paulo. See MPF-SP, 'Grupo de Combate aos Crimes Cibernéticos', at <http://www.prsp.mpf.gov.br/noticias-prsp/crimes-ciberneticos>, accessed 18 April 2011.

643 These agreements will be discussed later in Section 4 about the regulatory policies.

644 SAFERNET, 'Safernet Brasil', at <http://www.safernet.org.br/site/>, accessed 28 March.

645 ORKUT, 'A social networking system and discussion site operated by Google Inc.', at <http://www.orkut.com>, accessed 30 August 2010.

646 According to the comScore statistics, Orkut reached in August 2010 more than 36 million unique visitors. See 'Orkut Continues to Lead Brazil's Social Networking Market, Facebook Audience Grows Fivefold', (São Paulo-SP: comScore, 2010) at <http://www.comscore.com/Press_Events/Press_Releases/2010/10/>, accessed 26 April 2011.

647 According to the MPF-SP, the removal of content reported as alleged illegal was not immediate and, in some occasions, not even performed. See page 604 at 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011.

thus not subject to Brazilian sovereignty. This argument was unable to convince the Federal Public Prosecution Service (MPF-SP) which argued that Google Brasil was providing services in Brazilian territory, to Brazilian nationals, and therefore should be subject to Brazilian laws.

Apparently, Google Brasil was trying to protect the privacy of its customers by showing a hard-line stance on privacy grounds. Nevertheless, there were other issues involved, particularly the costs involved in being subject to different regulatory demands around the world (for example those involved in recording access' logs and providing them to the police); it seemed to be more cost-effective to operate under a single jurisdiction than to adapt its services to each different jurisdiction where Google offered its services. As such, the dispute here was not only about privacy or a free Internet but about jurisdiction and minimising operational costs.

Against this background, both MPF-SP and Safernet Brasil threatened Google Brasil with civil and criminal lawsuits to force cooperation but achieved little success. Google Brasil was approached a number of times from 2005 to 2008, but defiantly, and expensively,[648] declined to settle any agreement nor disclose any information about access logs and users' data.[649] Law enforcement authorities argued that Orkut became a repository of illegal material and an incentive to commit criminal offences online, because it had systematically refused to disclose any information about alleged offenders.[650] In April 2006, Safernet Brasil filled a complaint against Google Brasil in the Lower House of the Parliament.[651] In August 2006, the MPF-SP filled a criminal lawsuit against Google Brasil. As a result, other court orders were issued but Google Brasil employed a number of legal technicalities to procrastinate the immediate effect of such orders.

In 2007, Orkut launched an automated and random advertising system worldwide. Given that they were hosting alleged child pornographic and other criminal content via Orkut pages, some ads have been placed randomly on webpages containing illegal content.[652] As a result, Safernet Brasil recorded one of these pages and made a complaint against Google Brasil in August 2007 at CONAR,[653] the Brazilian advertising watchdog. This led to substantial losses in revenues for Google, because the companies being advertised began to unitarily end their contracts.

---

[648] Google Brasil hired well-known and expensive lawyers, *e.g.* the former Ministry of Justice, to defend their claims during the parliamentary public sessions.

[649] For a detailed account of the Orkut debacle, see pages 617-30 at Ibid, .

[650] Alleged criminal content hosted in Orkut has been a concern since the early 2005. See Rivlin, G., 'Hate Messages on Google Site Draw Concern', *The New York Times,* 07 February 2005 at <http://www.nytimes.com/2005/02/07/technology/07orkut.html>, accessed 26 April 2011 See also Martins, R., 'Criminosos agem impunes no Orkut', *O Estado de São Paulo,* 06 February 2006 .

[651] At the Human Rights Commission of the Lower House of the Parliament, *i.e.* '*Câmara dos Deputados*'. See CDHM, 'Comissão de Direitos Humanos e Minorias da Câmara dos Deputados', at <http://www2.camara.gov.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm>, accessed 27 April 2011.

[652] See Regalado, A. and Delaney, K., 'Google Under Fire Over a Controversial Site: Racist Speech, Porn Stir Battle in Brazil; A 'Pandora's Box'', *The Wall Street Journal*, (2007), A1 at <http://online.wsj.com/article/SB119273558149563775.html> accessed 30 August 2010.

[653] CONAR, 'Conselho Nacional de Autorregulamentação Publicitária', at <http://www.conar.org.br/>, accessed 30 August.

Following this, Google Brasil changed the stance taken so far and started to negotiate the terms of an agreement with the MPF-SP and Safernet Brasil, from September 2007 to March 2008.

In March 2008, the higher chamber of the Brazilian Parliament, the Senate, launched a Parliamentary Inquiry Commission[654] (CPI) to tackle the proliferation of online child pornography in Brazil. Following this, the MPF-SP, the Safernet Brasil and a number of other public and private actors were invited to public audiences. During these CPI sessions, a number of agreements were negotiated with major online intermediaries (*e.g.* Internet hosting service, content service and service providers, and online payment systems), so they agreed to employ minimum standards towards content removal, identification of alleged offenders and preservation of evidence for criminal investigations. These developments also led private actors to implement a number of measures of their own to monitor more closely the content they hosted and distributed and to the development of a national reporting scheme for child pornography websites. The CPI also discussed and proposed a new anti-child pornography bill that was enacted in November 2008 and criminalised a number of conducts and increased existing penalties. Other anti-online child pornography bills were proposed amidst a slow paced parliamentary activity in relation to the regulation of other cybercrimes and of online intermediaries in general; child pornography lawmaking has clearly taken the lead here.

Subsection 2.1 above explored the historical context on which the regulatory initiatives to limit access to online child pornographic material were implemented in Brazil. It is against this background that Subsection 2.2 below explores Brazilian anti-child pornography laws both in relation to child pornography *per se* and regulation of online intermediaries that hosted or provided access to such problematic material.

2.2 Legislation

2.2.1 State-regulation: the anti-child pornography laws

The development of modern anti-child pornography laws in Brazil can be divided into three stages. The problem was first addressed in 1990 with the '*Lei No. 8.069/1990*'[655] (hereinafter the 1990 Law). According to Article 241, it was a criminal offence to photograph or publish sexually explicit or pornographic scenes involving children (*i.e.* any person under 12) or adolescents (*i.e.* any person over 12 and under 18). The 1990 Law provided a definition of child pornography (*i.e.* sexually explicit or pornographic scenes involving children under 18) and outlawed its production (*i.e.* to photograph) as well as its non-commercial distribution (*i.e.* to publish).

---

[654] 'Comissão Parlamentar de Inquérito do Senado Federal para apurar a utilização da internet na prática de crimes de "pedofilia", bem como a relação desses crimes com o crime organizado', (Brasília-DF, Brasil, 2008) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 March 2012.

[655] Lei No. 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente 1990 (Brazil).

Later in 2003, following growing concern about the proliferation of child pornographic content on the Internet in Brazil, the '*Lei No. 10.764/2003*'[656] (hereinafter the 2003 Law) amended the 1990 Law. It modified the definition of child pornography and criminalised a number of conducts. The 2003 Law outlawed the production (*i.e.* to produce), commercial distribution (*i.e.* to sell), non-commercial distribution (*i.e.* to show, provide or publish), by any means of communication, including the Internet, of any 'photographs or images depicting sexually explicit or pornographic scenes involving children or adolescents.' The previous definition of child pornography was modified so as to include this type of media (*i.e.* photographs and images). In addition, the 2003 Law imposed, in Article 241, §1º, criminal liability on online intermediaries so as to punish those private actors which (i) provided the means or services to host the child pornographic content; or (ii) provided, by any means, online access to child pornographic content. Online intermediaries were only criminally liable if they had actual knowledge of the illegal material and did not take any action to remove access;[657] they were not required however to actually search this knowledge. The 2003 Law also increased imprisonment sentences.

Finally, the '*Lei No. 11.829/2008*'[658] (hereinafter the 2008 Law) was enacted in 2008 and substantially altered the 2003 Law. It modified the definition of child pornography, criminalised a number of conducts and clarified the provisions on the criminal liability of online intermediaries, putting in place a legislated framework for a notification scheme (but only in relation to child pornographic content available online). The 2008 Law still considered child pornography as 'sexually explicit or pornographic scenes depicting children or adolescents,'[659] but it added that 'sexually explicit or pornographic scenes' meant any representation, by whatever means (*e.g.* photograph or video), of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. This amendment literally repeated the provision found at the 2000 UN Optional Protocol, ratified by Brazil in March 2004.[660]

The Brazilian legislator increased the list of criminal conducts in relation to the production, distribution and collection of online child pornography. As a result, production[661] (*i.e.* to

---

[656] Lei No. 10.764, de 12 de novembro de 2003. Altera a Lei No. 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. 2003 (Brazil).

[657] For this opinion, see Filho, D. R., 'O crime de divulgação de pornografia infantil pela Internet: breves comentários à Lei No. 10.764/03' *Infojus* (2003); <http://www.advogado.adv.br/artigos/2003/democritoreinaldofilho/crimepornografiainfantil.htm> accessed 20 April 2011. See also Leonardi, M., *Responsabilidade Civil dos Provedores de Serviços de Internet* (São Paulo: Juarez de Oliveira, 2005), p 108.

[658] Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil).

[659] See art. 241-E. Ibid .

[660] The UN Optional Protocol was ratified via the Decreto No. 5.007 de 08 de março de 2004. Promulga o Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil. 2004 (entered into force on 08 March 2004) (Brasil).

[661] See art. 240 of the Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil).

produce, reproduce, direct, photograph, film or register, by any means, child pornography), commercial distribution[662] (*i.e.* to sell or to show, with intent to sell, a photograph, video or any other register containing child pornography) and non-commercial distribution[663] (*i.e.* to offer, exchange, make available, transmit, distribute, publish, by any means, including computer systems, child pornography) were outlawed.

In addition, the 2008 Law criminalised the acquisition[664] and the possession[665] of child pornography, and provided some defences.[666] It legitimised the operation of Internet hotlines and exempted them from criminal liability if they possessed child pornographic content only to notify law enforcement agencies.[667] Finally, it criminalised the production, distribution and possession of pseudo-photographs depicting child pornography (*i.e.* modified or juxtaposed photographs or video).[668] For Suiama,[669] the child depicted in the pseudo-photographs had to be real, non-fictitious and thus identifiable.[670] Yet, the legislator's intention was unclear, because the parliamentary proceedings mentioned at some point that the child should be real but it also mentioned elsewhere that even if there was no real child involved the 'ideal child' had been harmed.[671] The 2008 Law also increased imprisonment penalties.

More recently the Senate has approved the Bill No. 100/2010[672] in order to authorise the undercover operation of police agents investigating online grooming of children as well as other online child pornography offences. If this Bill becomes law, police forces would be able to conduct lawful sting operations in Brazil. According to the 2010 Bill, such operation must have

---

662 See art. 241. Ibid .

663 See art. 241-A. Ibid .

664 The 2008 Law employed the term '*adquirir*' (*i.e.* to acquire) and it was unclear whether this meant buying, accessing or knowingly accessing child pornographic content on the Internet. It was perhaps the case that the legislator intended to consider 'to acquire' as 'to buy.' See page 128 at 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011.

665 This state regulatory tool (*i.e.* the criminalisation of possession) was considered an important initiative to limit access to child pornographic content, because it extended the police powers against alleged viewers; proving a possession offence was perhaps easier than proving a distribution offence, but this assumption is debatable.

666 See art. 241-B. Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil).

667 See art. 241-B, §2º, inc. III. Ibid . This provision was general and thus did not establish any monopoly over the processing of reports by a single Internet hotline in Brazil.

668 See art. 241-C. Ibid .

669 Suiama, S., 'Nota Técnica GCCC/PR/SP', (São Paulo: MPF-SP, 2010) at <http://www.prsp.mpf.gov.br/sala-de-imprensa/pdfs-das-noticias/crimes-ciberneticos> Accessed 19 April 2011.

670 This was in line with the stance taken in the US. See Section 2 of Chapter 3 for a discussion about the attempt to criminalise virtual child pornography in the US.

671 They mentioned that the child should be real, *i.e. 'de carne e* osso*',* (see pages 204 and 207) but also that the harm could be posed to the ideal child, *i.e.* '*bem tutelado é a honra*', (see page 367) at 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011.

672 Projeto de Lei do Senado No. 100 de 2010 - Altera a Lei No. 8.069 de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes da polícia na Internet com o fim de investigar crimes contra a liberdade sexual de crianças ou adolescentes (2010). at <http://www.senado.gov.br>, accessed 13 May 2011.

prior judicial authorisation to be conducted, but even with this safeguard, such a legislative proposal might be violating key principles of the Brazilian criminal code (*i.e.* the crime was impossible to be committed, because there was no child involved but rather a covert police officer; and the police was arguably motivating the alleged offender to produce criminal evidence against him/her). It has implications not only for the control of online grooming offences but also for limiting access to child pornography if distributed via closed online groups.

2.2.2 State-regulation: the criminal liability of online intermediaries

The 2008 Law established that private parties (*i.e.* the relevant online intermediaries) were criminally liable for hosting or providing access to child pornographic content hosted domestically if, after being 'officially notified,' they failed to make the content inaccessible.[673] This provision established the limits of criminal liability of online intermediaries and the legal framework for the notice of take down regime but only in relation to child pornography hosted in Brazil. There were no further explanations about what official notification meant, nor which private actors was the law targeting (*i.e.* whether content service, hosting service or Internet service providers).[674] During the parliamentary discussion prior to the approval of the 2008 Law, representatives of the Internet industry lobbied to include the term 'official notification' instead of 'general communication.' This was because the latter could potentially be used by any member of the public (and thus increased the costs of a reporting scheme on the part of the service provider), whereas the former term meant an act of recognised institutions, for example law enforcement agencies and Internet hotlines (so only a few institutions would be able to notify the relevant content to the service provider).

There was no comprehensive national legislation to regulate the activities of online intermediaries in Brazil in general, as there is in other jurisdictions.[675] Resolution of conflicts were generally guided by civil and criminal legislation about telecommunications and broadcasting services. Nevertheless, there were bills under parliamentary discussion in this regard.

---

[673] See art. 241-A, §2°. Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil) This is in line with the provisions found at EU Directive on Electronic Commerce 2000 (DIRECTIVE 2000/31/EC, 08 June 2000). See Chapter 3.

[674] For a description of services provided by online intermediaries, see Reed, C., *Internet Law: Text and Materials* (2nd edn.; Cambridge: Cambridge University Press, 2004) See also Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88.

[675] See Chapter 3 about the legal liability of online intermediaries in the EU.

For example, the Bill N. 494/2008[676] aimed to regulate the activities of online intermediaries (including preservation of access logs, disclosure to law enforcement agencies and a number of obligations and sanctions) in relation to online child pornography criminal investigations. This bill derived from the discussions that led to the agreement negotiated between law enforcement authorities and a number of telcos and backbone providers in 2008 during the CPI sessions.

Another example was the 2010 *Marco Civil* Bill.[677] This legislative proposal established a number of general principles for the online environment and the rights of Internet users in Brazil, particularly the legal liability of online intermediaries and a general notice and take down scheme for problematic online content hosted domestically. The bill has been proposed by the federal government (the Brazilian Ministry of Justice in a partnership with the think tank '*Fundação Getúlio Vargas*')[678] and was under discussion by the public at large before it was submitted to the Parliament. The discussion so far has made evident the political struggle between those for and against online content regulation. On one side were the Internet industry and civil liberties activists (refusing any or allowing little governmental regulation of the Internet) and, on the other side, there were law enforcement and governmental authorities (trying to put in place a number of regulatory measures). Article 20 of the bill established a general principle of legal liability of online intermediaries in relation to problematic content:

> The Internet service provider can only be held responsible for the content produced by third parties if, after a judicial notification, it does not take the measures within the time requested, to make such content unaccessible.[679]

For Thompson, the proposed article established an indiscriminate legal immunity of online intermediaries and placed a heavy burden on the judicial system. He points out that there were no safeguards to protect free speech and the proposed scheme disincentives the establishment and enforcement of terms of service (under the constitutional provisions) by private actors.[680] If the bill becomes law, this may have implications in a number of issues discussed here: (i) the existing agreements negotiated since 2005 in relation to child pornographic content; (ii) for the monitoring being currently conducted by the online intermediaries; (iii) for the parliamentary discussion of the Bill N. 494/2008 about the investigatory powers of law enforcement authorities; and, perhaps, also (iv) for the notification system put into place via the 2008 Law in relation to child pornographic content.

---

[676] See Projeto de Lei do Senado, No. 494 de 2008 - Disciplina a forma, os prazos e os meios de preservação e transferência de dados informáticos mantidos por fornecedores de serviço a autoridades públicas, para fins de investigação de crimes praticados contra crianças e adolescentes, e dá outras providências. (2008). at <http://www.senado.gor.br>, accessed 26 April 2011.

[677] Marco Civil da Internet (2010). at <http://culturadigital.br/marcocivil/>, accessed 26 April 2011.

[678] There has been substantial lobby from telcos and Internet companies *e.g.* Google Brasil around the bill to limit the regulation of online intermediaries in Brazil to a minimum. This *Marco Civil* Bill was considered by some to be a counter-reaction against a highly criticised bill about cybercrime regulation, the Projeto de Lei No. 84 de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. (1999). at <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>, accessed 18 April 2011.

[679] See Marco Civil da Internet (2010). at <http://culturadigital.br/marcocivil/>, accessed 26 April 2011.

[680] Thompson, M., 'Problemas Fundamentais do Marco - Marcelo Thompson @ Cultura Digital', (Brasília-DF, Brasil, 2010) at <http://culturadigital.br/marcelothompson/>, accessed 13 March 2012. See also Thompson, M., 'The Insensitive Internet – Brazil and the Judicialization of Pain', *unpublished,* (2010).

2.2.3 Multi-state regulation: the international laws

Brazil signed the 2000 UN Optional Protocol[681] on 06 September 2000 and ratified it without reservations on 27 January 2004.[682] The ratification updated the 2003 Law's definition of child pornography and paved the way for future criminalisation of possession as well as the implementation of other measures in the 2008 Law, which generally followed the international legislative developments.

Nevertheless, Brazil was not a signatory to the 2001 CoE's Cybercrime Convention.[683] Although the Senate CPI suggested that Brazil should ratify the Convention,[684] the Brazilian Ministry of Foreign Affairs argued that this would demand substantial changes in national criminal laws and thus another international convention ought to be designed instead, so as to reflect the views of a wider international community.[685] Brazil decided therefore not to sign the 2001 CoE's Cybercrime Convention because it was not consulted during its formulation process. It was pursuing instead another cybercrime treaty, under the United Nations authority, whose discussions were being held at the United Nations Office on Drugs and Crime (UNODC) in Vienna.[686] This illustrates the limitations of multi-state regulation to tackle the problem of not only child pornographic content but cybercrime generally at the international level.[687]

2.3 Regulatory policies

The major problem that regulators had to face in relation to limiting the access to child pornographic content until the mid-2005 in Brazil has been mainly the availability of such material in commercial and non-commercial websites hosted overseas but produced, distributed or accessed by people in Brazil. There was also material found in public websites hosted in Brazil but this was not the key concern. Of course, other online platforms (for example anonymised P2P, FTP, real-time messaging systems etc.) are used to access child pornography but these have been outside the regulatory measures discussed above because it was a matter of police investigation.

---

[681] UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations). See the list of ratifications at http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11-c&chapter=4&lang=en . Accessed on 20 June 2011.

[682] The ratification was via the Decreto No. 5.007 de 08 de março de 2004. Promulga o Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil. 2004 (entered into force on 08 March 2004) (Brasil).

[683] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) .

[684] See p. 313 at 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011.

[685] See Harley, B., 'A Global Convention on Cybercrime?' *The Columbia Science and Technology Law Review* (2010); <http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/> accessed 29 August 2010.

[686] See UNODC, 'Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime. Vienna, 17-21 January 2011', at <http://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html>, accessed 17 March 2012.

[687] See Section 4 of Chapter 3 for the limitations of multi-state regulation tackling online child pornography.

Against this background, the Brazilian Internet industry had little involvement helping to tackle the problem until 2005, amidst no comprehensive national legislation to regulate the operation of online intermediaries, a pro-self regulatory discourse that was never implemented, and a permanent struggle by these online intermediaries to avoid any costs involved in implementing regulatory measures. The intergovernmental body CGI.br had also little involvement as discussed above.

In order to address the failure of both domestic state legislation and Internet industry self-regulation, the Federal Public Prosecution Service MPF-SP, the Internet hotline Safernet Brasil, and later, the Senate CPI employed a concerted action to update domestic anti-child pornography legislation and bring private actors into line after the late-2005 so as to facilitate the reporting and removal of content, identification of alleged offenders and preservation of evidence. This concerted action involved a number of regulatory initiatives and implications that are described below.

2.3.1 Agreements negotiated with online intermediaries after 2005

The MPF-SP[688] has received since 2003 a number of complaints from members of the public about the availability of criminal content on the Internet in Brazil. Given the lack of a comprehensive legislated framework to regulate the activities of online intermediaries in Brazil,[689] the MPF-SP negotiated agreements with major online intermediaries (*i.e. Universo On-line*, *Internet Group do Brasil Ltda. IG*, *Terra Networks Brasil S.A., AOL Brasil*, *Click 21 Comércio de Publicidade Ltda.* and the *ABRANET*) in the State of São Paulo in November 2005 to facilitate criminal investigations.[690] This agreement established a number of soft obligations against these private actors. These obligations were to develop reporting mechanisms, to adjust their terms of service, to inform law enforcement authorities when any illegal activity was found, to keep access' logs for at least six months and to develop public awareness initiatives. Nevertheless, there were no sanctions for non-compliance but only the potential threat of legal action from the MPF-SP. Following this agreement, a number of others were negotiated in similar terms around Brazil after November 2005.[691]

---

688 The Federal Public Prosecution Service in the State of São Paulo. ('*Ministério Público Federal de São Paulo*'). See MPF-SP, 'Procuradoria da República em São Paulo. Grupo de Combate aos Crimes Cibernéticos', at <http://www.prsp.mpf.gov.br/noticias-prsp/crimes-ciberneticos>, accessed 27 April 2011.

689 This was the argument put forward by the MPF-SP to justify the use of agreements. See p. 164 at 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011.

690 See Termo de Compromisso de integração operacional celebrado entre o MPF-SP e os principais provedores de acesso de São Paulo. (2005). MPF-SP, São Pauloat <http://www.prsp.mpf.gov.br/prdc/area-de-atuacao/direitos-humanos/dhumint/Crimes%20contra%20Direitos%20Humanos%20-%20Termo%20de%20Compromisso%20celebr.pdf> accessed 31 August 2010.

691 The use of agreements, not legislation, by law enforcement authorities to bring online intermediaries into line has also been used in the US. See 'Attorney General Cuomo and Facebook Announce New Model to Protect Children Online', (New York: Office of the Attorney General, 2007) at <http://www.ag.ny.gov/media_center/2007/oct/oct16a_07.html> Accessed 29 April 2011. See also 'Attorney General Cuomo takes legal action against social networking site that ignores proliferation of child pornography', (New York, NY: Office of the Attorney General, 2008) at <http://www.ag.ny.gov/media_center/2010/june10b_10.html> Accessed 11 April 2011.

The Safernet Brasil accumulated a number of complaints from the public about the availability of child pornographic content in Brazil. In January 2006, the institution informed the ABRANET,[692] a major Brazilian Internet service providers association, and a number of online intermediaries operating in the country (*e.g.* Microsoft, UOL, Terra and Google Brasil) about the existence of alleged child pornographic content hosted in theirs servers; the intention was to remove the reported material and create a permanent channel of communication with these companies for future reports.

Around 80% of the reports received were in relation to alleged criminal content hosted in Google's Orkut.[693] Although the company eventually removed the content reported, it refused to disclose the access' logs and users' data to law enforcement authorities, even when there was a judicial order. Google Brasil argued that the requested information was hosted in the US and thus outside the reach of the Brazilian jurisdiction and, that the Google Brasil was only a public relations office. This argument did not convince the MPF-SP which argued that Google Brasil should be subject to the Brazilian laws and gave the example of other US companies (such as Yahoo! Inc. and Microsoft) which were able to provide these data when requested by the courts[694] or under law enforcement authorities request (in the case of access' logs but not content of private communications).[695] In fact, the Internet Industry Association ABRANET declared that a number of online intermediaries in Brazil already disclose access' information (not content of private communications) to law enforcement authorities without a court order.[696]

The process of bringing online intermediaries into line via agreements led a number of private actors to develop content monitoring and removal mechanisms of their own without constitutional scrutiny nor transparency. For example, News Corp.'s MySpace declared that they monitor the pictures uploaded by users to their servers, operate automated filters (*e.g.* based on hash values derived from images previously analysed by humans) and disclose access logs to law enforcement authorities without the need of a court order. Similarly, Microsoft declared that they disclose the access logs when requested by law enforcement authorities without a judicial order. The Brazilian company UOL declared that they had permanent staff dedicated to analyse the content of webpages created by its customers and that it has developed automated systems to monitor and block access to alleged illegal content posted by users.[697]

---

[692] ABRANET, 'Associação Brasileira de Internet', at <http://www.abranet.org.br/>, accessed 30 August 2010.

[693] A number of Orkut's profiles and communities allegedly hosting child pornographic content were already intensively reported to the MPF-SP before the Safernet Brasil joined efforts with this federal agency.

[694] See p 35 at 'Notas taquigráficas da audiência pública realizada no dia 26 de abril de 2006 sobre utilização da Internet como instrumento para a prática de crimes', (Brasília-DF: Comissão de Direitos Humanos e Minorias da Câmara dos Deputados, 2006) at <http://www2.camara.gov.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/notas-taquigraficas/nt26042006.pdf> Accessed 20 April 2011.

[695] It has also been reported that companies such as Microsoft and Yahoo! disclose access' data to law enforcement agencies without a court order. See p 20 at Ibid .

[696] See p 37 at Ibid .

[697] See the testimony of the News Corps Inc., Microsoft and UOL's representatives at p 129-37, CPI, 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85380&tp=1>, accessed 20 April 2011.

This suggests that online intermediaries started to operate internal procedures of content analysis without proper legislative oversight and transparency after being threatened by law enforcement authorities under the terms of the agreements mentioned above.

2.3.2 Agreement negotiated with Google Brasil in 2008

Google Brasil has insistently refused from 2005 to disclose any access logs of Brazilian nationals producing, distributing or accessing child pornographic content, available in its social network system Orkut, to law enforcement authorities even when the authorities had a court order requesting such information.[698] Nevertheless, Google Brasil finally disclosed the information requested by courts to law enforcement authorities in April 2008[699] and negotiated an agreement for further cooperation with the MPF-SP during the CPI session on 02 July 2008.[700]

Amongst other measures to facilitate the identification of alleged offenders for criminal investigation, Google Brasil agreed to: (i) follow future court orders; (ii) to inform the MPF-SP about any illegal material they find in Orkut; (iii) to remove access to any material reported by law enforcement authorities and preserve the evidence; (iv) to perform content analysis of material uploaded by users (*i.e.* automated *ex ante* filtering via hash values of illegal images previously reported); (v) to develop proactive monitoring initiatives; (vi) to perform human content analysis of reports sent by the Safernet Brasil; (vii) to remove the alleged illegal external links; (viii) and to close the account of users found to be distributing illegal content in Orkut. Google Brasil has developed a number of proactive content monitoring initiatives such as filtering technologies that automatically: (i) detect suspicious images or symbols within images; (ii) remove alleged illegal hypertext links; and (iii) detect suspicious text associated with child pornographic content.[701] The range of obligations was clearly much larger when compared to agreements negotiated by private actors in 2005, and this was perhaps a result of the long lasting defiance showed by Google Brasil to Brazilian law enforcement authorities.

2.3.3 Agreement negotiated with telcos, backbone providers and other private actors in 2008

Soon after Google Brasil disclosed the information requested by law enforcement authorities in April 2008, the CPI created a task-force to analyse the information provided and found another

---

[698] Google Brasil eventually removed alleged illegal material once notified. The MPF-SP argued that the issues with Google Brasil were five: (i) preservation of access logs; (ii) preservation of evidence and immediate notification to law enforcement agencies; (iii) monitoring of private communities; (iv) provision of a costumer service to report child pornographic content; and (v) developing systems to monitor and automatically block access alleged illegal content. See p 165-9 at Ibid, .

[699] In fact, Google Brasil also disclosed the information requested by courts in other previous occasions. See p 625 at Ibid, .

[700] See the English version of this agreement at Term of Adjustment of Conduct settled between the MPF and Google Brasil (2008). CPI da Pedoflia, Brasília-DF at <http://www.prsp.mpf.gov.br/crimes-ciberneticos/GoogleTAC_english_version.pdf/at_download/file> accessed 27 August 2010.

[701] See p 674 and 720 at CPI, 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85380&tp=1>, accessed 20 April 2011.

problem. The massive volume of information, handed to law enforcement authorities by Google Brasil, lead to numerous judicial requests issued to telcos, backbone providers and other intermediaries so as to identify alleged offenders. These companies disclosed the information requested three months later but it was generally inconsistent, ambiguous, invalid or even blatantly wrong; there was no legislation in Brazil requiring online intermediaries to keep accurate access' logs and personal data of Internet users. This led the CPI to compel these companies to employ common standards in relation to content removal procedures, identification of users, and preservation of access logs and the reported content to be used by law enforcement authorities whenever requested.

As a result, another agreement was proposed and negotiated by a number of private actors during the CPI session of 12 December 2008. This agreement was negotiated between law enforcement authorities and online intermediaries more closely related to the Internet infrastructure (*i.e. Telemar Norte Leste S.A., Brasil Telecom S.A., and Tim Celular S.A.*), but the terms of the agreement included online content services provided by some of these companies. Amongst other things, the agreement established that companies were required to: (i) keep access logs and personal users' data for three years (ISPs) and six months (hosting service and content service providers); (ii) disclose access logs, personal users' data and content of communications to law enforcement authorities whenever requested and only by judicial order; (iii) disclose access logs and personal users' data to law enforcement authorities without the need of a judicial order;[702] (iv) develop a permanent channel to receive such requests from law enforcement authorities; (v) record the contents of communication whenever requested by law enforcement authorities and disclose them only by judicial order; (vi) inform law enforcement authorities about any child pornographic found in their servers, disable access and keep the relevant criminal evidence; and (vii) develop a number of public safety awareness measures.[703]

Some companies negotiated the agreement as it was originally proposed by the CPI, but other companies (albeit from the same economic group) decided to commission an independent legal analysis to assess the constitutionality of the agreement before following suit. The legal analysis commissioned by a few reluctant companies highlighted a number of important issues.[704] First, it argued that Brazilian authorities were forcing the companies to act in ways that were not based on existing law. Second, it pointed out that the Senate CPI had no constitutional authority to impose such obligations and sanctions. Third, it considered many of the provisions unlawful, because they forced content providers to handle access logs and users' data (not the contents of

---

[702] In the case of both (ii) and (iii) the companies were prohibited to inform the particular user/s about these requests. The agreement also established the period of time the companies must provide the requested information: (1) within 02 hours, whenever there was an imminent life-threatening situation posed to a child; (2) within 24 hours, whenever there was a life-threatening situation posed to a child; (3) within 72 hours, for all other situations.

[703] See Termo de Mútua Cooperação celebrado entre as prestadoras de serviços de telecomunicações, de provimento de acesso à Internet, a CPI da Pedofilia e outros. (2008). CPI da Pedofilia, Brasília-DF, Brasil at <http://www.safernet.org.br/site/sites/default/files/Teles.pdf> accessed 31 August 2010.

[704] See the legal analysis commissioned by these companies at Sundfeld, C. A., 'Parecer jurídico redigido a pedido das companhias Empresa Brasileira de Telecomunicações S.A. (Embratel), Telecomunicações de São Paulo S.A. (Telesp), Claro S.A., Vivo S.A. e Terra Networks Brasil S.A.', (São Paulo-SP, 2009) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011.

the communication) to law enforcement authorities without a court order. In addition, the document criticised the role of Safernet Brasil, because it considered the Internet hotline a non-governmental institution undertaking a public function without a proper legislative mandate and without any wide public scrutiny.[705] This legal challenge led to a few changes in the original agreement; but in the end, all remaining companies invited to the CPI sessions negotiated the agreement in August 2009, without challenging the Senate CPI in the courts.

The challenge made by these online intermediaries and the overall reluctance to accept the regulatory mechanisms proposed were also motivated by the costs involved in implementing such measures in practice. The private actors did not want to bear these costs, but to use public funds for such regulatory enterprise. As such, the opposition made against the agreement was to politically make the case, to a large extent, for the use of public funds if any online regulatory structure was to be implemented.

2.3.4 Agreement negotiated with online payment systems in 2009

Although child pornography can be produced and exchanged for non-commercial motives,[706] the United Nations Office on Drugs and Crime estimates that the annual market value of child pornography is of about US$250 million,[707] and that the groups involved increasingly use complex payment schemes that enable anonymous payment and make it difficult for the police to trace the money-flow back to offenders.[708] Nevertheless, part of the problem can be addressed because child pornography commercial vendors can have their merchant account unregistered if their commercial websites are reported to the relevant online payment system.

In order to target overseas websites providing access to online child pornographic material upon payment, the CPI decided to target the online payment systems operating in Brazil.[709] In August 2009, it proposed another agreement so as to require the online payment systems (*e.g.* Visa, Mastercard, Amex etc.) to unregister the websites and merchant accounts reported by Safernet Brasil as allegedly selling child pornography as well as to preserve evidence for criminal investigations.[710] The Brazilian initiative aimed to limit access to commercially driven websites

---

[705] See p 912-13 at CPI, 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado"', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85380&tp=1>, accessed 20 April 2011.

[706] See Section 1 of Chapter 3 about online child pornography.

[707] The UNODC Report however did not explain in detail how it produced these figures.

[708] See ch 10.2 about child pornography in UNODC, 'The Globalization of Crime: a transnational organized crime threat assessment', (Vienna: United Nations Office on Drugs and Crime, 2010) at <http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf>, accessed 13 March 2012, p 211-18.

[709] The use of payment schemes to access child pornography on the Internet was also discussed earlier during a Senate public session on 04 July 2007. See p 38 at 'Ata da 21a Reunião da Comissão de Constituição, Justiça e Cidadania em conjunto com a 19a Reunião da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal, 04 de julho de 2007', (Brasília-DF, Brasil: Senado Federal, 2007) at <http://www.senado.gov.br> Accessed 13 March 2012.

[710] See Termo de Mútua Cooperação celebrado entre as empresas associadas da ABECS, a CPI da Pedofilia e outros. (2008). CPI da Pedofilia, Brasília-DF, Brasil at <http://www.safernet.org.br/site/sites/default/files/abecs.pdf> accessed 31 August 2010.

hosted overseas, but available in Brazil, which depended on these payment systems to operate. Generally this initiative followed the same approach taken by the US Financial Coalition Against Child Pornography.[711]

2.3.5 Agreements to establish a national reporting scheme after 2008

Google Brasil and Safernet Brasil negotiated an agreement in July 2008 in relation to the reporting system for child pornography found in Orkut webpages.[712] The agreement established that Google Brasil was responsible to: (i) receive a daily list of Orkut-related URLs allegedly hosting child pornography from the Safernet Brasil; (ii) perform the analysis of the material reported; (iii) remove access to the material and preserve the evidence for future investigation[713] if alleged child pornography is found; and (iv) report back to both Safernet Brasil and the MPF-SP. Google Brasil also agreed to perform proactive monitoring of content (using hashing values of images already found or known and employing these values to automatically filter images uploaded by Orkut users). The daily list of Orkut-related webpages were reported by Safernet Brasil to a permanent staff of content analysts from Google Brasil. In addition, members of the public could also report these webpages to Google Brasil. After assessing these reports, Google Brasil was required to notify both law enforcement authorities and Safernet Brasil if any alleged child pornographic material was actually found.

Similar agreements have been negotiated amongst Safernet Brasil, Federal and State Public Prosecution Services, Federal Government agencies and private parties to develop a nationwide reporting scheme in relation to child pornographic material available on the Internet.[714] All reported websites (except those related to Orkut webpages which are assessed by the Google Brasil staff) were forwarded to a single database of reports, created and maintained by Safernet Brasil.

If child pornographic material was found and it was hosted in Brazil, the online intermediary (*e.g.* the content service, hosting service or Internet service provider, including the online payment systems) was notified and a report was forwarded to the relevant law enforcement authority to start a criminal investigation, under the terms of agreements mentioned above. The Safernet Brasil reported that only 2% of websites reported were found to be hosted in Brazil.

If child pornographic material was found and it was hosted overseas, the Brazilian Federal Police was notified, and also (i) the relevant overseas Internet hotline, if any in the country

---

[711] See FCACP, 'Financial Coalition Against Child Pornography', at <http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703>, accessed 09 June 2010.

[712] See *e.g.* Termo de Cooperação celebrado entre a Safernet Brasil e a Google Brasil Internet Ltda. (2008). SAFERNET, São Paulo-SP, Brasil at <http://www.safernet.org.br/site/institucional/parcerias/google> accessed 31 August 2010. See also SAFERNET, 'Parceria com a Google Brasil', at <http://www.safernet.org.br/site/institucional/parcerias/google>, accessed 17 March 2012.

[713] The evidence was preserved for 180 days and disclosed only via judicial order.

[714] See *e.g.* the agreement negotiated between the Safernet Brasil and the Ministry of Justice at Termo de Cooperação Técnica, Científica e Operacional celebrado entre a SEDH-MJ e a Safernet Brasil e outros (2008). SEDH-MJ, Brasília-DF, Brasil at <http://www.safernet.org.br/site/sites/default/files/SEDHDPF.pdf> accessed 31 August 2010.

where the material was hosted; or (ii) the embassy of the country where the material was hosted. This investigation found no evidence that filtering of websites was performed voluntarily at the ISP-level. There were however online content filtering software available for individual users.

It was not only members of the public who were able to report child pornography available on the Internet. A number of governmental bodies, NGOs and law enforcement authorities have online reporting mechanisms that fed the centralised national database of reports. In addition, the Internet hotline Safernet Brasil did not have a monopoly on receiving, processing and forwarding reports in relation to child pornographic content available on the Internet. Nevertheless, it was the key institution responsible for such task without a clear legislative mandate for doing so.

The operation of Safernet Brasil has been based on Article 5(§3) of the amended Brazilian Criminal Processual Code,[715] which allows for any member of the public to report certain offences (including child pornography) to the law enforcement authority without any special requirements. In addition, the 2008 Law legitimised the operation of Safernet Brasil, under Article 241-B(§2)II,[716] which provided a legal defence for a possession offence when possession was necessary to report the material and, it was done by institutions created, according to the law, to receive, process and forward reports to law enforcement authorities. Against this background, Safernet Brasil has taken part in major national debates around the problem of online child pornography, acquired substantial expertise about the theme, created and maintained so far the national database of reports, and established a series of agreements in relation to the reporting scheme that placed the institution as a well-know Internet hotline for child pornography in Brazil.

Nevertheless, there has been a row between the Federal Public Prosecution Service MPF-SP and Safernet Brasil. The MPF-SP has complained that Safernet Brasil has not forwarded a number of reports in relation to child pornographic websites to the MPF-SP, following an exclusivity clause negotiated in a 2006 agreement. In June 2010, Safernet Brasil argued that: (i) these reports were not forwarded directly to the MPF-SP but to the CPI Commission (where the MPF-SP has a seat); (ii) around 4,000 reports forwarded by Safernet Brasil (from July 2008 to April 2010) have not been actioned by the MPF-SP; and also (iii) requested a meeting to discuss these issues further with the MPF-SP.[717] In November 2010, the MPF-SP published a technical report and claimed that Safernet Brasil was (i) unable to process the volume of reports it received and

---

[715] Código de Processo Penal. Decreto-Lei No. 3.689, de 03/10/41. 1941 (Brazil).

[716] Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil).

[717] SAFERNET, 'Ofício n. 0017/2010/SAFERNET Brasil referente ao cumprimento do termo de cooperação firmado entre a SaferNet e a PR/SP', (São Paulo-SP, Brasil: Safernet Brasil, 2010) at <http://www.safernet.org.br>, accessed 13 March 2012.

(i) provided inconsistent statistics about the reports processed along its operation. Subsequently, the MPF-SP ended the 2006 agreement with Safernet Brasil on 12 November 2010.[718]

There were two agreements where the MPF-SP and Safernet Brasil are parties: (i) one was negotiated in 2006, in relation to the reporting scheme and the exclusivity clause (Clause 3B) to receive all reports processed by Safernet Brasil;[719] and (ii) another was negotiated in 2008, in relation to Google's Orkut alleged child pornographic webpages.[720] As a result, although the 2006 agreement has ended, the 2008 agreement about the reporting scheme for Google's Orkut webpages remained valid.

It seemed that the MPF-SP had the intention to centralise the reporting scheme nationwide irrespective of the legitimacy of other law enforcement authorities to undertake this activity and it was not in Safernet's interests to follow an exclusivity clause with the MPF-SP, because the hotline has been settling agreements with other law enforcement and government bodies in other regions of Brazil. Following these mutual accusations and the end of the 2006 agreement, Safernet Brasil kept forwarding reports it received and processed to other law enforcement authorities, *e.g.* the Brazilian Federal Police and seven Federal Public Prosecution Services across the country.

2.3.6 The regulatory initiatives: self, state and multi-state, and hybrid regulation

A number of regulatory measures have been employed gradually since 2005 to limit access to child pornographic content available on the Internet in Brazil. These measures derived to a large extent from agreements negotiated between law enforcement authorities and private actors. Along these agreements, substantial changes have been made in federal legislation both in relation to anti-chid pornography offences *per se* and the establishment of a NTD scheme for online child pornographic material.[721]

The 2008 Law added a definition of child pornography which was in line with the international legislative developments and criminalised the possession of child pornography. It criminalised the pseudo-photographs but the person depicted in the material had to be a real child. As such, cartoon imagery and texts were arguably not covered by existing criminal law in Brazil.[722] The

---

[718] See MPF-SP, 'Nota Pública: MPF rescinde Termo de Cooperação com Safernet', (São Paulo-SP: MPF-SP, 2010) at <http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/12-11-10-nota-publica-mpf-rescinde-termo-de-cooperacao-com-safernet/> Accessed 29 April 2011. Nevertheless, the existing reporting scheme involving Google's Orkut has not been altered.

[719] Termo de Mútua Cooperação Técnica, Científica e Operacional que entre si Celebram a Procuradoria da República no Estado de São Paulo e a Safernet Brasil. 29 de março de 2006. (2006). São Paulo-SP, Brasilat <http://www.safernet.org.br/site/sites/default/files/mpsp.pdf> accessed 17 March 2012.

[720] Term of Adjustment of Conduct settled between the MPF and Google Brasil (2008). CPI da Pedoflia, Brasília-DF at <http://www.prsp.mpf.gov.br/crimes-ciberneticos/GoogleTAC_english_version.pdf/at_download/file> accessed 27 August 2010.

[721] Generally the federal entity had the monopoly to legislate in criminal matters in Brazil. See Article 22(I) of the Brazilian Federal Constitution. Constituição da República Federativa do Brasil 1988 (Brazil).

[722] Although some may argue that texts could be an offence under Articles 286 and 287 of the Brazilian Criminal Code about incitement to commit a crime and apology of a crime, respectively. See Código Penal. Decreto-Lei No. 2.848, de 07/12/40. 1940 (Brasil).

act of knowingly access online child pornography has not been criminalised neither. In addition, the 2008 Law considers a child any person under the age of 18 and established a NTD scheme but only in relation to child pornography. Brazil ratified the 2000 UN Optional Protocol in 2004, but decided not to join the 2001 CoE's Cybercrime Convention.

In addition, relevant legislative bills have been proposed. A legislative bill based on the 2008 agreement negotiated with the telcos and backbone providers was placed under parliamentary discussion to increase the regulation of online intermediaries, in relation to child pornographic content, so as to facilitate the immediate removal of the material hosted in the country, the identification of alleged offenders and the preservation of evidence. Although there were a cybercrime bill and another bill in relation to the regulation of online intermediaries, the anti-child pornography laws have been enacted in advance.[723] This seemed to reinforce the argument according to which the problem of online child pornography was being used by online regulators as a 'soft spot' to advance regulatory initiatives.[724]

Finally, these regulatory developments led private actors to be more concerned about the content they hosted or distributed, particularly if of child pornographic nature. Following this, a number of content service and hosting service providers developed content monitoring and removal schemes of their own without any clear democratic scrutiny, transparency nor guidance. More importantly, these developments opened the discussion about a national legislative framework to regulate the activities of online intermediaries generally in relation to the content they hosted or distributed, and made evident the intention of private actors to avoid the costs involved in the implementation of a regulatory structure.

2.3.7 The scope and mechanics of the regulatory model

The regulatory model implemented in Brazil to limit access to child pornography available on the Internet targeted online child pornography hosted in Brazil, or hosted overseas but created, distributed or accessed by people Brazil; and it was based to a large extent on agreements negotiated amongst law enforcement and government authorities, and private actors. The focus was mainly on commercial and non-commercial websites available in the public Internet. Child pornography accessed via other platforms were a mater of police investigation.

The notice and take down scheme in relation to child pornography was established via legislation in 2008 but the overall reporting scheme was based on private agreements and was largely maintained and operated by the Internet hotline Safernet Brasil in partnership with online intermediaries, law enforcement authorities and a number of governmental bodies. The scheme was arguably able to remove alleged child pornographic material hosted in domestic

---

[723] The 1999 Brazilian Cybercrime Bill is under Parliamentary discussion since 1999, but the provisions related to child pornography were extracted from it and enacted via the 2008 Law. See Projeto de Lei No. 84 de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. (1999). at <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>, accessed 18 April 2011.

[724] Interestingly, although financial and property related cybercrimes had not advanced in terms of legislation, they used most resources from the Brazilian Federal Police in comparison to online child pornography investigations.

websites but ineffective to limit access to websites hosted overseas. Child pornographic content hosted overseas was targeted via the traditional police channels (*i.e.* the reports were sent to Interpol via the Brazilian Federal Police or directly to foreign law enforcement authorities) and foreign Internet hotlines, if any operating in the country where the material was hosted. There was no evidence that any filtering scheme was operating at the ISP-level in Brazil.

Online intermediaries, for example Internet content service, hosting service and service providers played important roles in the regulatory scheme. In addition to developing content monitoring schemes of their own, they negotiated a number of agreements in order to secure the immediate removal of alleged child pornographic material, report mandatorily any child pornographic material found to the relevant law enforcement authority, preserve evidence, and disclose information about access' logs and contents of communication to law enforcement authorities whenever required (pending a court order in relation to the contents of a communication).

This section addressed the laws and regulations to limit access to child pornographic material available on the Internet in Brazil. First, it explored the history of online content regulation in the country particularly in relation to child pornography. Second, it addressed domestic criminal laws tackling the production, distribution and possession of online child pornography in addition to the investigatory powers of law enforcement authorities. Third, it explored regulations in place to limit access to online child pornographic content, be it hosted in Brazil or overseas.

3 United Kingdom

This section addresses the laws and regulations implemented in the United Kingdom to limit access to online child pornography. It covers not only state and multi-state regulation but relevant legal interpretations given by courts and regulatory policies put in place forcing online intermediaries to remove alleged child pornographic content hosted within the jurisdiction and to block access to related websites hosted overseas. Subsection 3.1 provides an account about how regulation against online child pornography has developed in the UK particularly after the creation of the Internet Watch Foundation (IWF)[725] in 1996; the IWF was the Internet industry 'self-regulatory' body created to tackle child pornographic material available on the Internet in the United Kingdom. Subsequently, state and multi-state regulatory initiatives as well as relevant case law are covered in Subsection 3.2, and the overall regulatory framework is explored in detail in Subsection 3.3.

3.1 Historical context

[725] IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

Generally, the problem of online child pornography gained substantial media visibility after 1994 when a number of events occurred: the commercial Internet started to flourish in the UK; legislation was introduced to tackle pseudo-photographs and the making offences in relation to indecent photographs of children;[726] the police operation Starburst took place; and the IWF was created.

One of the initial concerns was in relation to child pornographic material available via domestic Usenet newsgroups.[727] Such material was exchanged in a number of public feeds named with explicit labels (*e.g.* alt.binaries.lolita) and this led to a joint response from the police and government against UK Internet service providers (ISPs) hosting these newsgroups. Following a meeting on 02 August 1996 between Scotland Yard and the Internet Service Providers Association (ISPA),[728] the Chief Inspector of the Clubs and Vice Unit at Charing Cross Police Station requested around 140 ISPs to remove alleged illegal material[729] found in 133 newsgroups hosted in their servers.[730] The police and the government sent a straightforward message to the ISPs: if they did not act promptly to tackle the problem of child pornographic content hosted on Usenet newsgroups, there would be arrests and a call for legislation to regulate more closely the Internet industry in the UK.[731] There was a real danger of UK Internet industry senior management and directors being arrested and also a number of stories in British tabloids branding these executives as vile child pornography merchants.

Against this background, and under the leadership of the Internet entrepreneur Peter Dowe, several companies set up the Safety-Net Foundation on September 1996 to report the availability of online child pornographic content to UK ISPs and thus avoid state intervention and criminal liability, *i.e.* instead of facing the threat of arrests and legislation, the Internet industry set up a self-regulatory body (*i.e.* an Internet hotline) to receive and examine reports concerning the availability of potentially criminal content hosted in British servers.[732] The

---

[726] See Criminal Justice and Public Order Act (c.33) 1994 (England and Wales).

[727] Usenet was an Internet discussion system that may be considered a hybrid between email and online forum applications (*i.e.* usenet users are able to read and post articles to one or more categories which were threaded to other users and also stored on a web server).

[728] The ISPA UK was founded in February 1996. See ISPA, 'Internet Service Providers' Association UK', at <http://www.ispa.org.uk/home/>, accessed 29 June 2010.

[729] It has been claimed that these Usenet feeds reported by the police contained not only child pornography related images but also mere textual references or even legal adult pornography. See Akdeniz, Y., 'Governing Pornography and Child Pornography on the Internet: The UK Approach', *UWLALR,* 32 (2001), 247 and also Petley, J., 'Web Control', *Index on Censorship,* 38(1) (2009), 78-90, p 83.

[730] See generally Akdeniz, Y., 'Who Watches the Watchmen - Part I: Internet Content Rating Systems, and Privatised Censorship', Cyber-Rights & Cyber-Liberties UK, 1997) at <http://www.cyber-rights.org/watchmen.htm>, accessed 06 June 2011; Akdeniz, Y., 'Who Watches the Watchmen - Part II: Accountability & Effective Self-Regulation in the Information Age', Cyber-Rights & Cyber-Liberties UK, 1998) at <http://www.cyber-rights.org/watchmen-ii.htm>, accessed 06 June 2011; Akdeniz, Y., 'Who Watches the Watchmen - Part III: ISP Capabilities for the Provision of Personal Information to the Police', Cyber-Rights & Cyber-Liberties UK, 1999) at <http://www.cyber-rights.org/privacy/watchmen-iii.htm>, accessed 06 June 2011; Akdeniz, Y., 'The Regulation of Pornography and Child Pornography on the Internet' *The Journal of Information, Law and Technology* 1(1997); <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1> accessed 08 June 2010.

[731] Around the same time, the French police arrested ISPs' directors and confiscated companies' equipment on similar grounds and this sent a strong message to UK Internet industry.

[732] Newey, A., 'Freedom of expression: censorship in private hands', in Liberty (ed.), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (London: Pluto Press, 1999), p 32.

Safety-Net Foundation was not the first Internet hotline to be created; other initiatives appeared in Norway (Save the Children) and The Netherlands (Meldpunt)[733] about the same time as non-governmental organisations. The Safety-Net Foundation was renamed Internet Watch Foundation in November 1996 and was subject to governance and funding reforms in the following years so as to represent not only the UK Internet industry but wider sectors of society. Some non-industry actors were involved from the very beginning of the hotline via the IWF Policy Board.

The initial policy addressing Usenet newsgroups was not proactive. Once a posting in individual newsgroups was reported to the IWF, the image was assessed and, if considered potentially illegal, the company hosting the newsgroup was notified about the material. Nevertheless, this approach was only partially effective, because after removal, the material was posted again in another newsgroup. Because the IWF staff were only allowed to examine and act in relation to individual postings which had been reported to them by a third party, there was nothing that could be done; they had to wait until the new posting was reported again. This situation led to a policy of automated monitoring which was widened in 2002 so as to implement the removal of the entire newsgroup if proved that an image had been found there on a regular basis, or if there was a suggestion of paedophilia content in the groups' name.[734] Around 2002, the use of Usenet newsgroups was fading in importance in the UK and child pornographic content was increasingly accessed via public websites hosted domestically or overseas.

Generally, from 1996 to 2002, the IWF recommended UK online intermediaries to remove alleged child pornographic content by notice and this was in line with the general framework for the criminal liability of online intermediaries established via the 2000 EU Directive on Electronic Commerce.[735] Overall, the notice and take down (NTD) regime implemented by the IWF was considered a successful initiative in removing child pornographic content hosted on UK servers. For example, since 2002, less than 1% of child pornographic content reported to the IWF has been found available on websites hosted in the UK.[736] Nevertheless, these figures took into account only the UK public websites reported to the IWF and thus, it may be suggested that, these numbers night be higher than reported, because many websites or other online repositories hosted in the UK, be they public or closed, might go unreported on the hotline. In addition, these figures excluded child pornography available via other Internet applications

---

[733] 'Meldpunt Kinderporno op internet', at <http://www.meldpunt-kinderporno.nl/EN/default.htm>, accessed 29 February 2012.

[734] This zero tolerance measure proved to be controversial with free speech advocates, because entirely legal newsgroups could have been removed irrespective of their actual content. Nevertheless, the policy was implemented despite these concerns. This study was unable to find whether claims of free speech activists were justified or simply hypothetical concerns that never really posed an issue. In any case, the measure seemed to be in line with Section 1(d) of Protection of Children Act (c.37) 1978 (England and Wales) which makes an offence to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows indecent photographs or pseudo-photographs of children, or intends to do so.

[735] EU Directive on Electronic Commerce. DIRECTIVE 2000/31/EC, 08 June 2000 (European Union).

[736] See IWF, 'Annual and Charity Report 2008', (Cambridge, UK: IWF, 2009) at <http://www.iwf.org.uk>, accessed 07 June 2011.

(such as anonymised peer-to-peer, real-time messaging and closed online groups); these Internet applications were not covered by the IWF's statistics.

In any case, however successful the NTD scheme might have been to tackle child pornographic content hosted domestically, such criminal content was still available via public websites hosted overseas and, in this case, the IWF had no authority to force a foreign online intermediary to take the relevant content down nor was the conventional international police channel able to act expeditiously to remove the material hosted overseas once notified by the IWF.[737] Against this background, a change in policy occurred in 2004 with the implementation of the IWF blocklist to limit access to child pornography related websites hosted overseas but accessed from the United Kingdom. According to the scheme, the IWF managed a blocklist of overseas URLs allegedly containing child pornographic content and provided it to the member UK ISPs, which voluntarily implemented the IWF blocklist against their customers. According to the IWF, blocking was only a 'short-term disruption tactic' to protect inadvertent access to such images, because the most effective way to tackle the problem was to remove the material at its source.[738] Yet the IWF blocklist was implemented by around 98.6% of UK commercial ISPs[739] and there has been pressure to make the remaining ISPs follow suit.

The IWF played a key role in limiting access to online child pornographic content within the United Kingdom. It had interfaces with member ISPs, search engines, online payment systems, mobile operators, law enforcement agencies and overseas Internet hotlines. As such, this case study was mainly centred on the IWF's operation. Nevertheless, state regulation (*i.e.* domestic anti-child pornography legislation), multi-state regulation, and the courts also played an important role setting the regulatory environment in limiting access to child pornography in the United Kingdom and they are addressed in Subsection 3.2 below.

Finally, another mechanism that influenced the regulation in the United Kingdom was the EU Safer Internet Programme[740] which was created in 1996 and particularly provided (i) financial support to the IWF and (ii) helping to establishing a network of hotlines throughout Europe by the means of the Association of Internet Hotlines INHOPE. The latter provided the IWF with a

---

[737] The IWF was a member of the INHOPE Association of Internet hotlines. See INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010. This institution provided support to Internet hotlines in Europe and beyond, encouraged the exchange of expertise and technical reports, and it also informed policymakers. It provided Internet hotlines, such as the IWF, a fast channel to remove alleged child pornographic material hosted overseas where there was another affiliate member. This was only partially effective because not all overseas Internet hotlines were INHOPE members nor were all jurisdictions covered by hotlines.

[738] IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

[739] See the press release by Coaker, V., 'House of Commons Written Answer from the Home Office Minister, Hansard, 16 June 2008, col 684W', (London: House of Commons, 2008) at <http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080616/text/80616w0011.htm#08061620000413>, accessed 02 March 2012; and also 'Parliamentary records. Answer given by Home Office Minister Alan Campbell on 02 November 2009', (London: UK Parliament - House of Commons, 2009) at <http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091102/text/91102w0017.htm#09110238001607> Accessed 26 May 2012.

[740] Safer Internet: A multi-annual Community programme on protecting children using the Internet and other communication technologies. Work Programme (2009). Brusselsat <http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm> accessed 07 July 2011.

fast channel to take down alleged child pornographic material hosted overseas where there was an affiliate Internet hotline member.

3.2 Legislation and case law

3.2.1 Domestic anti-child pornography laws and case law in England and Wales

This subsection describes domestic laws and developments in case law around the regulation of child pornographic material from the mid-1950s to 2010 in England and Wales. It shows how the process of digitisation and networking associated with the Internet challenged domestic state regulation of child pornography. The documentary evidence below was based on legislation and cases as of until 2010.

3.2.1.1 Indecent photographs of children (child pornography)[741]

Child pornography was addressed initially in England and Wales via the Indecency with Children Act 1960 (c.33). Later the problem of child pornography was tackled by the Protection of Children Act (POCA) 1978 (c.37) under the label of 'indecent photographs of a child'. A number of legal interpretations and court decisions also shaped the regulatory landscape, particularly in relation to online child pornography criminal offences that had a deterrent effect in limiting access to such content (*i.e.* possession, downloading, and viewing).

Section 7 of the 1978 Act established that 'a photograph, film (including any form of video-recording), a copy of a photograph or of a film, a photograph comprised in a film, and references to a photograph including the negative as well as the positive version' as media able to contain an indecent photograph of a child. The 1978 Act criminalised the following conducts:

> (a) to take, or permit to be taken, any indecent photograph of a child (meaning in this Act a person under the age of 16); or (b) to distribute or show such indecent photographs; or (c) to have in his possession such indecent photographs, with a view to their being distributed or shown by himself or others; or (d) to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs, or intends to do so.[742]

3.2.1.2 Possession

Later in 1988, the Criminal Justice Act criminalised the possession of an indecent photograph of child in Section 160, making it an 'offence for a person to have any indecent photograph of a child (meaning in this section a person under the age of 16) in his possession'. This was a change from the previous regulatory position in relation to child pornography, because the criminalisation of production and distribution offences (*i.e.* take, distribute, and have in

---

[741] For the relevant legislation and case law in England and Wales see ch 2 of Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008); and also CPS, 'Indecent photographs of children: legal guidance', (London: The Crown Prosecution Service, 2012) at <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/>, accessed 03 March 2012.

[742] Protection of Children Act (c.37) 1978 (England and Wales).

possession with a view to distribution) were tackling only the intentional possession for future distribution. More importantly, it represented a departure from the liberal stance employed so far (*i.e.* that the consumption of pornography in the private sphere should not be regulated by the state because it only harmed the viewer).[743]

Some defences were included whenever the person charged with a possession offence proved '(a) that he had a legitimate reason for having the photograph in his possession; or (b) that he had not himself seen the photograph and did not know, nor had any cause to suspect, it to be indecent; or (c) that the 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'.[744] These defences were known as: (1) legitimate reason; (2) unknown possession; and (3) unsolicited possession, respectively. It is argued elsewhere that the criminalisation of possession of indecent photographs of children helped law enforcement agencies pursuing successful investigations, prosecutions and convictions, because proving the possession was rather straightforward when compared to distribution.[745] But this claim is debatable, because other variables (*e.g.* police officers taking the issue more seriously, and advances in the surveillance technology) could have played a role in those arguably successful police operations.

3.2.1.3 Pseudo-photographs and the act of making

In 1994, the Criminal Justice and Public Order Act amended the POCA 1978 and criminalised the 'indecent pseudo-photographs of children', meaning 'an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.'[746] It also criminalised the act of 'making' which had harsher penalties than the mere possession. This was mainly because the production of child pornographic content was facilitated by the available techniques of digital manipulation of photographs. The amended Section 1 of the the POCA 1978 read as 'it is an offence for a person: to take, or permit to be taken or to make, any indecent photograph or pseudo-photograph of a child.' According to the Criminal Justice and Public Order Act 1994, references to a photograph would included '(a) the negative as well as the positive version; and (b) data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.' Similarly, references to an indecent pseudo-photograph included '(a) a copy of an indecent pseudo-photograph; and (b) data stored on a computer disc or by other electronic means which is capable of conversion into a pseudo-photograph.' A child continued to mean a person under the age of 16.

3.2.1.4 Conveys the impression of a child

---

[743] From the liberal point of view, the need to prevent harm to persons other than the actor is always a morally relevant reason to support state coercion. See Feinberg, J., *The Moral Limits of the Criminal Law: Harm to Self* (Volume 3; New York: OUP, 1986), p ix.

[744] Criminal Justice Act (c.33) 1988 (England and Wales).

[745] Easton, S., *The Problem of Pornography: regulators and their right to free speech* (London: Routledge, 1994), p 131; Akdeniz , Y., 'Possession and Dispossession: A Critical Assessment of Defences in Possession of Indecent Photographs of Children Cases', *Criminal Law Review,* (2007), 274-88.

[746] See Section 84, Criminal Justice and Public Order Act (c.33) 1994 (England and Wales).

In addition, the 1994 Act established that 'if the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated for all purposes of this Act as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult.'[747] Finally, the 1994 Act amended Section 160 of the Criminal Justice Act 1988 and criminalised the mere possession of an indecent pseudo-photograph of a child.

3.2.1.5 Data stored in a computer and photographs

In *R. v Fellows and Arnold* the appellants contended that the data stored in a computer was not a 'photograph' for the purposes of the Protection of Children Act 1978. The appeal was dismissed because:

> […] in their true construction the definitions of 'indecent photograph' set out in §§ 1 and 7 of the 1978 Act were wide enough to include a form of technology which was either not anticipated or was in its infancy when the Act was passed and therefore to include later as well as contemporary forms of copies of photographs. In the instant case, the disk itself was not a photograph, but it contained data which could be converted by appropriate technical means into a screen image and into a print which exactly reproduced the original photograph from which it was derived. The data therefore represented the original photograph in another form and, since the 1978 Act did not restrict the nature of a copy, it came within the definition of 'photograph' for the purposes of the Act.[748]

This decision led to the amendment of the POCA 1978, via Section 84 of the Criminal Justice and Public Order Act 1994 which considered that references to a photograph included 'data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.'

3.2.1.6 Harsher punishments

In 2000, the Criminal Justice and Court Services Act 2000 increased the maximum sentence penalties for offences associated with indecent photographs of children.[749] *R. v Oliver and others*[750] divided indecent images of children into five categories and provided sentencing guidelines based on this taxonomy. Later, these guidelines were amended by guidance from the Sentencing Council.[751]

---

[747] Section 84, Ibid .

[748] *R. v Fellows and Arnold* [1997] 2 All ER 548.

[749] Criminal Justice and Court Services Act (c.43) 2000 (England and Wales).

[750] *R v Oliver and others* [2002] EWCA Crim 2766; [2003] 2 Cr App R (S) 64; [2003] 1 Cr. App. R. 28; [2003] 2 Cr. App. R. (S.) 15; [2003] Crim. L.R. 127.

[751] Sexual Offences Act 2003: Definitive Guideline (2007). Sentencing Guidelines Council, at <http://sentencingcouncil.judiciary.gov.uk/docs/web_SexualOffencesAct_2003.pdf> accessed 10 July 2011.

3.2.1.7 Relevant case law in relation to possession, making and access[752]

In *R. v Bowden*,[753] downloading or printing off an indecent photograph of a child from the Internet was considered 'making a copy of an indecent photograph' because a copy of such photograph had caused to exist on the computer to which it had been downloaded. This judgement created a situation where the prosecution could legitimately choose to charge the act of downloading a copy of an indecent photograph of a child onto a computer as either a 'making' offence or a 'possession' offence.[754] This had implications for law enforcement because agents were arguably committing a making offence in order to collect criminal evidence, but this was resolved via the statutory defences established in Article 46(1) of the Sexual Offences Act 2003.[755]

Akdeniz criticises the reasoning in *R. v Bowden*. He believes that downloading and making an indecent photograph or pseudo-photograph of a child are different in nature; they involve different levels of human agency. As such, they should not result in the same punishment.[756] Gillespie suggests that the treatment of downloading as a 'making' offence occurred, because the punishment of a possession offence was considered lenient at that time (*i.e.* only six months) when compared to a making offence.[757] There were no defences available to those charged with the making offences, in contrast to possession and distribution offences. Unsurprisingly, prosecutors may have opted to charge alleged offenders on making offence grounds because this held harsher sentences.

Atkins and Goodland v DPP[758] established that knowledge was an essential ingredient of both the offences of making and possessing of indecent photographs of children. As such, possession and making offences were subject to *mens rea* because they were not offences of strict liability.[759] In addition, the court decided that an image consisting of parts of two separate photographs taped together did not appear to be a photograph, *i.e.* it was not a pseudo-photograph.

---

[752] Article 5(3) of the 2011 EU Directive requires all member states to take the necessary measures that act of 'knowingly obtaining access […] to child pornography […]' is punishable. See Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union).

[753] *R. v Bowden* [2000] 2 All ER 418.

[754] This ruling was later confirmed in *Atkins v DPP; Goodland v DPP* [2000] 2 All ER 425; [2000] 1 WLR 1427 (QBD) and in *R. v Smith and R. v Jayson* [2002] EWCA Crim 683; [2003] 1 Cr App R 13.

[755] Sexual Offences Act (c.42) 2003 (England and Wales).

[756] Akdeniz , Y., 'Possession and Dispossession: A Critical Assessment of Defences in Possession of Indecent Photographs of Children Cases', *Criminal Law Review,* (2007), 274-88.

[757] Gillespie also suggests that legislation should be amended so as to allow a clear distinction between accessing images for personal use and creating or distributing them. See Gillespie, A., 'Indecent Images of Children: the ever-changing law', *Child Abuse Review,* 14 (2005), 430-43.

[758] *Atkins v DPP; Goodland v DPP* [2000] 2 All ER 425; [2000] 1 WLR 1427 (QBD).

[759] Nevertheless, this was doubted slightly in *R. v Collier* [2005] EWCA Crim 1411 depending on how 'strict liability' is defined.

In *R. v Jayson and Smith*,[760] the court held that downloading an indecent image of a child that was capable of being converted into a photograph on to a screen was an act of making that photograph or pseudo-photograph; and that no offence of making or possessing an indecent photograph of a child was committed by opening an email attachment when the recipient was unaware that the image contained or was likely to contain such indecent image. This judgment confirmed the understanding in *R. v Bowden* about the making offence; making and being in possession were not absolute offences but subject to prior knowledge (*mens rea*).

In *R. v Collier*,[761] it was a defence for the defendant to prove that although he knew or had cause to suspect that the photograph was of an indecent nature, he had not seen it, and he did not know or have cause to suspect that, it was an indecent photograph of a child.

In *R. v Dooley*[762] the Court of Appeal considered whether leaving an image, unprotected against public access, in the 'My Shared Folder' when using P2P software (*i.e.* KaZaA) might be sufficient for a person to be in possession of an indecent photograph of a child with a view to show or distribute it. In addition, the judge drew a distinction between the words "with a view to" and the words "with the intention of."

Finally, in *R. v Porter*[763] the court held that if the person could not access the relevant images (save through the use of specific software) then the person would not be in control of them and thus not be guilty of possession.

Against this background, Walden[764] argues that the advent of the Internet has blurred in the UK the distinctions between the acts of (a) possession and copying;[765] (b) possession and incitement to publish or supply,[766] or some form of conduct 'beyond the mere act of establishing a communication'; (c) possession and distribution or publication. This had important implications for the regulation of access to child pornographic content on the Internet. It showed how relevant case law tried to tackle access related conducts (*i.e.* possession, viewing, downloading, and printing) as production (*i.e.* making) and distribution offences, departing from the liberal stance about the criminalisation of possession. In other words, it has disregarded the traditional liberal defence mentioned earlier not only based on what was prescribed in law (*i.e.* offence of mere possession) but it has expanded this to consider possession as production or distribution offences via case law.[767]

---

[760] *R. v Smith and R. v Jayson* [2002] EWCA Crim 683; [2003] 1 Cr App R 13.

[761] *R. v Collier* [2005] EWCA Crim 1411.

[762] *R. v Dooley* [2006] 1 WLR 775, [2005] EWCA Crim 3093.

[763] *R. v Porter* [2006] EWCA Crim 560; [2006] All ER (D) 236 (Mar).

[764] Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62, p 438.

[765] See *R. v Bowden* [2000] 2 All ER 418.

[766] See *R. v Goldman* [2001] Crim LR 822.

[767] From the liberal point of view, the need to prevent harm to persons other than the actor is always a morally relevant reason to support state coercion. See Feinberg, J., *The Moral Limits of the Criminal Law: Harm to Self* (Volume 3; New York: OUP, 1986), p ix.

3.2.1.8 Children as a person under the age of 18

In 2003, the Sexual Offences Act 2003 amended the Protection of Children Act 1978 and increased the age of a child from 16 to 18 to meet international standards, and also included defences regarding marriage and other relationships in cases where the photograph was of the child aged 16 or over. This seems incongruent with the age of legal consent (16 years) and may put at risk those involved in films or video which used actors aged 16 or 17 in sexual related material.[768] Interestingly, for the first time the words 'child' and 'pornography' were used in regard to indecent photographs of children in England and Wales in a legislative document. The 2003 Act established a number of defences (*i.e.* the defendant was not criminally liable for possessing and or distributing child pornography, mainly to safeguard public authorities against the abovementioned developments in case law) if s/he proved that:

> (a) it was necessary for him to make the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world; (b) at the time of the offence charged he was a member of the Security Service, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of the Service, or (c) at the time of the offence charged he was a member of GCHQ, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of GCHQ.[769]

3.2.1.9 Criminalising non-photographic content (*i.e.* 'cartoon' pornography)

After a consultation process,[770] the Coroners and Justice Act 2009 criminalised the possession of 'prohibited images of children.' This extended the definition of child pornography under the 1978 Act and included non-photographic child pornography. This was another change from previous criminal laws against child pornography in England and Wales. Not only photographic content (*i.e.* indecent photographs and pseudo-photographs of children) was criminalised but non-photographic content such as cartoons, drawings and tracings were taken onboard. This means not only that the scope of material associated with child pornography was expanding but that a causal nexus between the material and the abuse of real children (*i.e.* the evidence of harm) was no longer necessary to justify the criminal sanction.

A prohibited image of a child was a material that was (a) pornographic; (b) fell within Subsection 6 of the 2009 Act; and (c) was grossly offensive, disgusting or otherwise of an obscene character. An image was pornographic 'if it is of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal.' An image fell within Subsection 6 if it was: (a) an image which focuses solely or principally on a

---

768 See Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62, p 451.

769 Sexual Offences Act (c.42) 2003 (England and Wales).

770 See 'Consultation on Possession of Non-Photographic Visual Depictions of Child Sexual Abuse', Home Office, 2007) at <http://scotland.gov.uk/Resource/Doc/1099/0048474.pdf>, accessed 12 July 2010.

child's genitals or anal region, or (b) portrayed any of the acts mentioned in Subsection 7. Subsection 7 read:

> (a) the performance by a person of an act of intercourse or oral sex with or in the presence of a child; (b) an act of masturbation by, of, involving or in the presence of a child; (c) an act which involves penetration of the vagina or anus of a child with a part of a person's body or with anything else; (d) an act of penetration, in the presence of a child, of the vagina or anus of a person with a part of a person's body or with anything else; (e) the performance by a child of an act of intercourse or oral sex with an animal (whether dead or alive or imaginary); (f) the performance by a person of an act of intercourse or oral sex with an animal (whether dead or alive or imaginary) in the presence of a child.[771]

Defences were included in the 2009 Act: 'it is a defence for the person to prove any of the following matters: (a) that the person had a legitimate reason for being in possession of the image concerned; (b) that the person had not seen the image concerned and did not know, nor had any cause to suspect, it to be a prohibited image of a child; (c) that the person: (i) was sent the image concerned without any prior request having been made by or on behalf of the person, and (ii) did not keep it for an unreasonable time.'

The 2009 Act established that an image included moving or still images produced by any means, or any data stored by any means which is capable of conversion into an image. It excluded however both indecent photographs and pseudo-photographs of a child, which were to be construed in accordance with the POCA 1978. The 2009 Act established that a child was a person under the age of 18 and 'where an image showed a person the image was to be treated as an image of a child if: (a) the impression conveyed by the image is that the person shown is a child, or (b) the predominant impression conveyed is that the person shown is a child despite the fact that some of the physical characteristics shown are not those of a child'[772], following the same approach established by the 1994 Act. Finally, the 2009 Act established that references to an image of a person included references to an image of an imaginary person and that references to an image of a child included references to an image of an imaginary child.

3.2.1.10 The Regulation of Investigatory Powers Act (RIPA) 2000[773]

Another legislative development not strictly related to substantive online child pornography criminal offences but with important implications for their investigation was the RIPA 2000. It is important because of: its deterrent effect on those attempting to access child pornographic content on the Internet, its potential to violate privacy of individuals in general, and the excessive pressure it may place on online intermediaries.

Generally the 2000 Act established a regime for the interception of communication, acquisition and disclosure of data, carrying out covert surveillance, use of covert human intelligence sources and encryption to catch up with the increased use of digital technologies by alleged

---

[771] Coroners and Justice Act (c.18) 2009 (England and Wales).

[772] Ibid .

[773] Regulation of Investigatory Powers Act (c.23) 2000 (England and Wales).

criminals. This piece of legislation allowed the police and other law enforcement agencies to request information (*i.e.* communication records of individual Internet users) from online intermediaries without a court order.[774]

The RIPA 2000 regulated the disclosure of electronic keys (*e.g.* cryptographic or otherwise) associated with alleged digital criminal evidence. It made it a criminal offence the refusal to supply the actual encrypted traffic and the encryption key; this could lead to up five years in prison if there was suspicion that the material was child pornography, under Article 53. In addition, the RIPA 2000 gave powers to law enforcement agencies to force an online intermediary to fit equipment to facilitate surveillance as well as to demand secret access to customers' private communication. The 2000 Act provided an oversight regime to avoid governmental abuse but it has been criticised over the lack of adequate safeguards and the threats it posed to civil liberties in the UK. For example, the Big Brother Watch Campaign reported a number of improper uses of the RIPA 2000 provisions by local authorities,[775] particularly its use to monitor petty cases.

Although not directly involved in the structures of online content removal,[776] the RIPA 2000 might have played a deterrent factor on those who accessed or exchanged child pornographic content on the Internet domestically, because the legislation facilitated the identification of alleged offenders. It facilitated the policing of ISPs' infrastructure by law enforcement agencies without the need of a court order, particularly in the case of Internet applications that were beyond the reach of the IWF (such as closed websites, P2P, emails and real-time messaging).

The preservation of evidence for future criminal prosecution involving online child pornography related offences arises under the 2009 EU Data Retention Regulations.[777] This came into force in April 2009 and established that online intermediaries must retain communication data on all users for 12 months, including mobile phone locations and e-mail logs. ISPs could voluntarily store web access logs but access to such information was regulated by the RIPA 2000.

3.2.2 Multi-state regulation: the criminal liability of online intermediaries in Europe

For Edwards, European online intermediaries were in a difficult position in the late 1990s, because there was no comprehensive legal framework to protect them against legal liability derived from the potentially criminal content they hosted and transmitted. According to her, they were pushing their argument forward against an indiscriminate liability based on the following grounds: (1) the lack of effective legal and actual control over the content they hosted or distributed; (2) they were mere intermediaries; and (3) the costs for monitoring content would

---

[774] An interception warranty from the Secretary of State was only required to disclose the content of letters.

[775] See 'The Grim RIPA: Cataloguing the ways in which local authorities have abused their covert surveillance powers', (London: Big Brother Watch, 2010) at <http://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf>, accessed 12 March 2012.

[776] And this is the reason why the RIPA 2000 was only peripherally covered in this case study.

[777] The Data Retention (EC Directive) Regulations 2009 (European Union).

call into question their economic survival.[778] As a result, these arguments set the context where the legal framework for the legal liability of online intermediaries[779] in Europe was established via the 2000 EU Directive on Electronic Commerce (hereinafter Directive).[780]

The 2000 Directive was explored in Chapter 2 and it constituted a multi-state regulatory initiative regulating the activities of online intermediaries in Europe with substantial implications in the United Kingdom. Although the IWF has employed a NTD regime since 1996 to avoid criminal liability being placed on member ISPs hosting potentially criminal content, the coming into force of the Directive in 2002 established a legal framework for the operation of the hotline. The Directive defined online intermediaries (*i.e.* information society services providers but also intermediary service providers) in a broader sense so as to include ISPs, Internet hosts, weblogs, search tools and social networking systems. It incorporated a safe harbour principle (*i.e.* online intermediaries are free from legal liability so long they cooperate when asked to do so) and established a NTD regime in relation to the online criminal content in Section 4.

The general framework of the NTD regime was established via Articles 12, 13 and 14 of the Directive. Articles 12 and 13 established that the online intermediaries were exempted from all liability when they operated as (i) a mere conduit (*i.e.* it does not initiate the transmission, does not select the receiver nor does select or modify the information); or when they (ii) performed mere caching operations to increase performance of transmission. Article 14 established that criminal liability could arise when online intermediaries operated as (iii) content hosts[781] but this was subject to condition in relation to knowledge and control,[782] (*i.e.* the host provider must have actual knowledge of the illegal activity and, upon obtaining such knowledge, acted expeditiously to remove or disable access to the content). In addition, Article 15 established that online intermediaries were not required to actively seek this knowledge or awareness, therefore, there was no general obligation to monitor the online content. Nevertheless, they could be forced to monitor and intercept communications under the RIPA 2000 provisions mentioned above.

3.2.3 Multi-state regulation: the international laws

The United Kingdom signed the 2000 UN Optional Protocol[783] on 07 September 2000 and ratified it on 20 February 2009. The 2000 Protocol established a definition of child pornography

---

[778] Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88, p 58.

[779] Note that the Directive did not apply to backbone providers.

[780] EU Directive on Electronic Commerce. DIRECTIVE 2000/31/EC, 08 June 2000 (European Union).

[781] Storing and hosting content more than transiently. See articles 14(1)A and 14(1)B of the Directive.

[782] See generally Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62.

[783] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) . See the list of ratifications at http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11-c&chapter=4&lang=en . Accessed on 20 June 2011.

in Article 2 and suggested that signatories should criminalise a number of conducts in relation to child pornographic content (such as production, distribution and possession). It also established a number of provisions to protect children against sexual exploitation.

In addition, the United Kingdom signed the 2001 CoE's Cybercrime Convention[784] on 23 November 2001 but ratified it only on 25 May 2011, apparently because of issues relating to procedural provisions.[785] The 2001 Convention established a number of provisions in relation to substantive and procedural criminal law to facilitate international police cooperation (mainly within Europe) and it entered into force in the UK on 01 September 2011.

The length of time between signature and ratification of these international treaties showed the problematic implementation of multi-state regulation already discussed in Chapter 3. The implementation of anti-child pornography international law domestically was subject to a variety of political debate, different cultural and legal national contexts, and varying policing capabilities. As a result, it took longer than some might expect and motivated the development of more immediate regulatory responses at the national level such as website blocking and informal cooperation amongst Internet hotlines. In the end, something had to be done about the problem nationally while the issues were not resolved at the international level.

3.3 Regulatory policies

Section 3.2 above explored state and multi-state regulation, including the regulation of online intermediaries, around the problem of online child pornography in the United Kingdom as of until 2010. The focus was placed not only on criminalisation of content and types of conduct associated with online child pornography but on criminal liability of online intermediaries and investigatory powers of law enforcement agencies to identify alleged offenders. Generally this was the legal landscape where regulatory policies were implemented in the UK to limit access to child pornography available on the Internet. This section presents an overview of the regulatory policies in place and address particularly how online intermediaries were forced to remove alleged child pornographic content from domestic servers and to limit access to such material within the United Kingdom.

The IWF played a central role within the regulatory scheme to remove child pornography from UK online intermediaries and block access to child pornographic overseas websites. In short, the IWF received and processed reports from the public, it notified the UK online intermediaries about potentially criminal content to preserve evidence and took down the material reported, it managed a blocklist of overseas URLs[786] that was implemented by member ISPs, and it

---

[784] Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. accessed 20 June 2011.

[785] This is suggested by Murray. See Murray, A., *Information Technology Law: the law and society* (Oxford: OUP, 2010), p 406.

[786] The URL stands for the Uniform Resource Locator, the technical term that specifies where an online resource is located and the mechanism for retrieving it (*e.g.* http://www.sheffield.ac.uk/law).

interacted with a number of public bodies (*e.g.* the police and the Home Office) and private actors (*e.g.* search engines, social network systems, online payment systems and overseas Internet hotlines). The Internet Watch Foundation was created in 1996 as self-regulatory Internet industry body to tackle the availability of criminal content on the UK Internet. It has experienced substantial growth both in relation to the number of reports received from the public and to the number of members it has.[787] Its (i) scope; (ii) mechanics; (iii) regulatory tools; (iv) interface with other actors; (v) nature; and (vi) criticisms are explored below.

3.3.1 Scope: the online criminal content targeted

According to the 2011 remit, the IWF targeted three different types of online criminal content: (1) child pornographic content hosted anywhere in the world; (2) criminally obscene adult content hosted in the UK; and (3) prohibited images of children (*i.e.* non-photographic child sexual abuse images, also cartoon child pornography) hosted in the UK. The IWF preferred to use the term 'potentially criminal content' instead of 'criminal content,' because it had no judicial authority to consider the content removed as criminal. In addition, it preferred the term 'child abuse images' over 'child pornography,' because it believed that the latter represented more accurately the violent nature of these images. Yet, the term child pornography is used hereinafter, because of its wide acceptance in the literature and international legal documents.[788]

The scope of material covered by the IWF's remit has been reduced and enlarged over the years. For example, incitement to racial hatred was part of the IWF's remit until 2011. In addition, the IWF has been involved in labelling and rating policies (under its R3 Safety-Net Agreement) to tackle online harmful content but these policies were discontinued after 2002, which left only the anti-criminal online content policies within the remit. On the other hand, the IWF's remit was also subject to increment following the criminalisation of certain types of online material. For example, the Home Office asked the IWF in 2007 to receive reports of online extreme pornography[789] within its remit of obscene material, which was approved by the IWF Board and implemented in January 2009. Similarly, the IWF remit was changed again in April 2010 so as to include the prohibited images of a child,[790] following a request from the Ministry of Justice in June 2009.[791] This increment is not surprising because, as material become illegal under UK law, so the IWF would alter its remit to extend the protection offered to member ISPs. As such,

---

[787] For example, it processed 1,291 reports in 1997, whereas 48,702 reports were processed in 2010. In 1997, the IWF had only 05 member ISPs but its membership increased to 102 companies in 2009. See IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

[788] A personal interjection is needed here: although the author prefers to use the term child pornography, he believes that sexual abuse committed against a child, be it materialised via child pornography/child sexual abuse images, is an outrageous aggression; he does fell angry and upset with this revolting violence; and he does feel compassionate about those who are recovering from the trauma. The preference of one term over another is merely methodological.

[789] Following Section 63 of The Criminal Justice and Immigration Act (c.4) 2008 (England and Wales).

[790] Following Sections 62-69 of the Coroners and Justice Act (c.18) 2009 (England and Wales).

[791] See IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

they are able to avoid the risk of the liability for hosting or distributing potentially criminal material.

There has been political pressure to include other types of content (*e.g.* terrorism related content and copyright infringement) within its remit (*e.g.* via the NTD and blocking measures) which produced fears of scope creep. Nevertheless, the IWF reported that only child pornographic content was covered by the blocking policy, and the use of the scheme to target other kinds of controversial content has been opposed not only by Internet industry representatives[792] but other sectors of society such as children right's organisations.

3.3.2 Mechanics: the basic operation of the IWF

Generally any online criminal content found in the open Internet (*i.e.* websites, newsgroups, social network systems) that fell within the IWF's remit could be submitted anonymously and confidentially via the IWF website. Once submitted, the report was assessed by the IWF content analyst according to the IWF threefold remit. This leads to two situations: (1) the content reported was judged to be legal or it was outside the IWF remit thus no further action was taken; or (2) the content was regarded as potentially criminal under UK law and the analyst would trace the source server where the content reported was hosted.

If the content reported was hosted in the United Kingdom, irrespective of its criminal nature (*i.e.* child pornography, criminally obscene adult content or a prohibited image of a child), the domestic police agency (*i.e.* the Child Exploitation and Online Protection Centre - CEOP)[793] was notified and a NTD was sent to the relevant host provider so they were under notice to remove the reported content and preserve evidence for future criminal investigation. In addition, the webpage was monitored until the content was removed.

If the content reported was hosted overseas and it referred to child pornography, then the relevant international hotline (if any operating in the country) and the UK police agency (*i.e.* the CEOP, which would contact Interpol) were both notified. In addition, the webpage URL was added to the IWF blocklist that was used by the member ISPs to make these images inaccessible from the United Kingdom. The IWF constantly monitored this URL to check if the content has been removed. When this occurred, the URL was removed from the IWF blocklist. Although the IWF had no authority to request overseas providers to take down alleged child pornographic websites, (i) it has begun notifying them anyway on a voluntary basis; and (ii) some major international providers (such as Google and Yahoo!) applied the list against all their services worldwide.

---

[792] See McIntyre, T., 'Internet Filtering: Implications of the "Cleanfeed" System', *Third Year PhD Presentation Series* (Edinburgh: School of Law, University of Edinburgh, 2010) at <http://www.law.ed.ac.uk/file_download/communities/245_tj%20macintyre%20-%20internet%20filtering-%20implications%20of%20the%20cleanfeed%20system.pdf>, accessed 29 February 2012.

[793] CEOP, 'Child Exploitation and Online Protection', at <http://www.ceop.gov.uk/>, accessed 29 February 2012.

A series of internal procedures for the NTD scheme was established via the Service-level Agreement[794] negotiated between the Association of Chief Police Officers (ACPO) and the IWF. This institutional agreement[795] set a standard investigatory protocol in relation to potentially criminal content hosted in UK servers and provided detailed information about the internal procedures and liaisons with the law enforcement agencies. The Agreement established that the IWF was responsible for assessing and tracing the online content that contravenes the UK law in England and was hosted in the United Kingdom. If the relevant content was hosted in the UK, (i) the IWF sent a preservation of evidence request and a NTD to the relevant ISP; (ii) a request of investigation by the relevant police agency was made; and (iii) the relevant ISP was called by phone so they received proper advice by the IWF staff in relation to the investigator's visit and after the fact monitoring.

The IWF reports that it did not deal with closed groups (such as P2P, real-time messaging and closed websites) but only with the public space Internet. However, it could pass the reports about closed platforms on to police agencies so they could perform the investigatory activities. In addition, the IWF argued that its blocklist only contained URLs of child pornographic content hosted overseas, so both the criminally obscene adult content and the non-photographic child pornography were outside the blocklist policy.

The IWF acquired in 2004 the status of relevant authority to receive reports in relation to online child pornography, following Section 46 of the Sexual Offences Act 2003.[796] This was negotiated via the Memorandum of Understanding signed by the IWF, the Crown Prosecution Service (CPS) and the ACPO,[797] and came into existence because what the IWF was doing was not covered by the legislation and arguably illegal, particularly after *R v. Bowden*.[798] The Memorandum was established to 'protect those who report the availability of a potentially illegal image to law enforcement agencies' so as to use a defence against a 'making offence' as defined in Section 46 of the abovementioned 2003 Act, and it addressed the factors affecting the plausibility of this defence which included (i) the way the material was discovered; (ii) the speed it was reported; (iii) secure handling and storage; (iv) copying the minimum to achieve the result. Generally this was to avoid the indiscriminate use of the making defence, to protect the IWF's staff from criminal liability and to regard the reports made to the IWF as reports made to a relevant authority.

---

[794] Service Level Agreement between the Association of Chief Police Officers and the Internet Watch Foundation (2010). IWF and ACPO, at <http://www.acpo.police.uk/documents/crime/2010/201010CRIIW01.pdf> accessed 14 June 2010.

[795] Interestingly this agreement was negotiated between the IWF and the Association of Police Officers, which was neither a police agency nor a Public Prosecution Service.

[796] Sexual Offences Act (c.42) 2003 (England and Wales).

[797] 'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003', (2004) at <http://www.cps.gov.uk/publications/docs/mousexoffences.pdf> Accessed 07 June 2011.

[798] *R. v Bowden* [2000] 2 All ER 418.

In short, the IWF did not require the UK online intermediaries to do anything. It merely informed the relevant intermediary that it received a report of content, or found content, which was hosted on the online intermediary's server, that its staff looked at this content, assessed it and concluded that it was potentially illegal under UK law. This put the intermediary under notice and thus at risk of losing their immunity under the 2000 EU Commerce Directive.[799] The online intermediaries were free to examine the material and perhaps take a different view, but in practice they usually took the reported content down expeditiously to avoid any criminal liability.

3.3.3 Regulatory tools: notices of take down and the IWF blocklist

3.3.3.1 Notices of take down (NTD)

The IWF was founded in 1996 amidst the problem of availability of child pornographic content on the UK Usenet newsgroups. It implemented a notice and take down policy so the member ISPs could be notified and expeditiously remove the reported image from the Usenet newsgroup they were hosting. Nevertheless, after removal, the images were usually published again in the newsgroup feed, and this lead the IWF to change its NTD policy and include the automated monitoring of the newsgroups content. The IWF changed this NTD policy in 2002 so as to suggest the removal of the entire newsgroup if (i) potentially criminal images were found on a regular basis or if (ii) the name of the newsgroup was related to paedophilia (*e.g.* alt.binaries.lolita). Although the use of newsgroups has decreased over the years in the United Kingdom, they were still subject to this automated monitoring measure.

The NTD scheme in relation to websites hosted domestically followed a similar approach.[800] Once reported and assessed as potentially criminal by the IWF, the relevant online intermediary was notified to remove the reported material and preserve evidence for further police investigation. This was to avoid any criminal liability and was in line with the provisions of the 2000 EU Directive on Electronic Commerce. According to the IWF, the content reported was removed from domestic servers in less than 24 hours after notice. Indeed, the UK member ISP was highly motivated to expeditiously remove the content reported to avoid the risk of criminal liability, and this could be the reason why the NTD scheme employed against content hosted domestically has been arguably successful. According to the IWF, since 2003 less than 1% of website related child pornographic content reported to the IWF was found to be hosted in the United Kingdom, in comparison to 18% in 1997.[801] Nevertheless, these figures referred only to websites reported to the IWF, and therefore, perhaps a larger proportion of potentially criminal content, not reported to the IWF, could be hosted in the UK and available via P2P networks, private online repositories, or exchanged via emails).

---

[799] EU Directive on Electronic Commerce. DIRECTIVE 2000/31/EC, 08 June 2000 (European Union).

[800] A NTD Code of Practice was adopted by all IWF members in 2002.

[801] See IWF, 'Internet Watch Foundation Annual Report 2003', (Cambridge, UK: IWF, 2004) at <http://www.iwf.org.uk>, accessed 07 June 2011.

Given that the NTD scheme was not effective to remove child pornographic content hosted in a overseas website[802] because amongst other reasons the IWF had no authority to request the removal from a foreign host provider, or the traditional international police channels were often slow, and the foreign police authorities generally had other pressing priorities, another approach was implemented: the blocking of child pornographic websites.

3.3.3.2 The IWF blocklist: blocking access to child pornography websites hosted overseas

> Effectively, therefore, the UK has put in place, without public debate, new laws, or a system of public accountability, a universal non-transparent scheme of online censorship that is in theory capable of blocking any particular piece of Internet content, whether illegal or not.[803]

The IWF blocking scheme addressed child pornography URLs available to UK Internet users but hosted overseas, where the NTDs have limited effect and the developments in relation to international treaties were slow. The implied rationale here was: if overseas law enforcement agencies were unable to act swiftly to take down the content reported, the IWF had to do something about it domestically.[804] Nevertheless, the IWF cautiously stated that the blocking scheme was unable to stop persistent viewers. On the contrary, it was designed to protect UK Internet users from unwanted and inadvertent exposure to illegal images, *i.e.* it was only a 'short term disruption tactic to protect users from stumbling across child pornography images whilst processes to have them removed overseas are instigated'.[805] In addition, the IWF emphasised that any discussion about tackling online child pornography must include the effort towards the harmonisation of international laws and pan organisational cooperation.[806]

The regulatory landscape around 2002 was susceptible to the implementation of a blocking strategy in the United Kingdom. For example, the IWF reported that its Board allowed the release of a blocklist containing URLs allegedly hosting child pornographic content to ISP members so they could implement blocking or filtering solutions earlier in 2002.[807] Similarly, Hunter mentions that John Carr, an Internet consultant on child safety, wrote to Paul Goggins, from the Home Office, in July 2003 demanding a governmental response to the issue of child pornographic content available on websites hosted abroad.[808] Later, the British Telecom Group

---

[802] The NTD scheme is also unable to remove material from non-permanent hosting locations (*e.g.* peer-to-peer and real-time messaging).

[803] Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 653.

[804] See Ozimek, J., 'IWF chief: We don't need crusaders', *The Register,* 08 September 2009 at <http://www.theregister.co.uk/2009/09/08/iwf_peter_robbins_interview/>, accessed 07 June 2011. See also IWF, 'Internet Watch Foundation Annual Report 2004', (Cambridge, UK: IWF, 2005) at <http://www.iwf.org.uk>, accessed 07 June 2011, p 18.

[805] See IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

[806] See IWF, 'Internet Watch Foundation Annual Report 2004', (Cambridge, UK: IWF, 2005) at <http://www.iwf.org.uk>, accessed 07 June 2011, p 18.

[807] See the Highlights Section at IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011.

[808] See Hunter, P., 'BT Site Block: BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns', *Computer Fraud and Security,* (9) (2004), 4-5.

plc. (BT) completed pilot tests around a website blocking system in May 2004. The idea of a blocking scheme faced initial resistance from ISPs but was fully implemented in 2004 by the BT via the 'BT Anti-child Abuse Initiative,' aka BT Cleanfeed.

The IWF compiled a list of URLs allegedly containing child pornographic content hosted overseas. This blocklist contained around 500 to 800 entries and it was updated twice daily so as to remove the URLs already taken down. The blocklist was then passed on under a license and via a secured interface to member ISPs that employ their own blocking solution (*e.g.* BT Cleanfeed, and WebMinder).[809] In order to receive the IWF blocklist, the member ISPs were required to pay a membership fee called 'CAIC income' and this subscription fee varied according to the size of the ISP.[810] The IWF only managed the blocklist and its implementation was entirely on the member ISP. They discouraged its member ISPs from adding more URLs or tinkering with the list but there were no safeguards to restrain ISPs from doing so. In addition, there was nothing stopping the list being passed on to other Internet hotlines and private companies (*e.g.* online content filtering providers, mobile operators and search engines) operating overseas and this could raise concerns about whether one country could determined what should be blocked in another.

It seems that member ISPs did not collect information from users trying to access the blocked URLs via their systems. For example, Hunter points out that around 230,000 attempts to access blocked URLs were made in less than a month and were detected by the BT via its Cleanfeed system. He reported that the BT did not keep the source IP address of users trying to access blocked URLs, but the BT and other ISPs could at least theoretically be forced to do so under the RIPA 2000 provisions.[811] Nevertheless, identifying 230,000 IP addresses may be extremely time-consuming and would discourage law enforcement agencies, with already scarce resources, to pursue investigations in this regard.

There was no law to mandate filtering or blocking of child pornographic content in the United Kingdom and the adoption of the IWF blocklist was done 'voluntary' by member ISPs.[812] A number of ISPs refused to join the scheme because of financial costs involved in implementing the blocklist and also because of free speech concerns.[813] The government threatened passing

---

[809] The BT Cleanfeed is one amongst a number of blocking systems available in the market. See ch Europe Overview in Deibert, R. J., et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010), p 283. See also Clayton, R., 'Anonymity and traceability in cyberspace', *Technical Report Number 653* (Cambridge: University of Cambridge, 2005) at <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html>, accessed 20 June 2011.

[810] Davies, C., 'The hidden censors of the internet', *Wired UK*, (2009) at <http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet?page=all> accessed 13 July 2010.

[811] Hunter, P., 'BT Site Block: BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns', *Computer Fraud and Security,* (9) (2004), 4-5.

[812] See interview with the IWF Director of Communication in Marling, C., 'Interview with Sarah Robertson, director of communications for the Internet Watch Foundation', *Broadband Genie,* 08 April 2009 at <http://www.broadbandgenie.co.uk/blog/full-internet-watch-foundation-interview-20090408>, accessed 07 June 2011.

[813] Williams, C., 'UK.gov to get power to force ISPs to block child porn ', *The Register,* 02 April 2009 at <http://www.theregister.co.uk/2009/04/02/eu_filtering_framework/>, accessed 20 June 2011.

legislation to force the remaining ISPs to follow suit,[814] but backed down later. [815] Nevertheless, the government required public bodies to contract Internet access services only from contractors implementing the IWF blocklist[816] which made clear its desire to see other ISPs following suit. In addition, even those ISPs that did not employ the blocklist could get their feed via BT or other large provider and thus would be using the IWF blocklist indirectly anyway. It is estimated that around 98.6% of UK commercial ISPs[817] and around 100% of mobile operators employed the IWF blocklist, which was a significant coverage under a 'self-regulatory' model

3.3.4 Interface with other actors: the IWF and other online intermediaries

The IWF developed a number of interfaces not only with those within the UK Internet industry[818] but with other online intermediaries such as search engines, mobile operators, online payment systems, overseas Internet hotlines and social network systems, to take down and limit access to potentially criminal content available online. For example, Google implemented both the IWF blocklist of URLs and the IWF blocklist of child pornography related keywords on the results provided by its search engine in the United Kingdom.[819] The IWF was a partner of the Mobile Alliance Against Child Sexual Abuse Content,[820] a self-regulatory international initiative to make the mobile infrastructure hostile to child pornographic content and has contributed to the development of the Mobile Operators Code of Practice.[821]

The IWF was also a partner of the European Financial Coalition, a police-lead initiative to limit purchases of child pornographic content via commercial websites,[822]and it provided reported URLs of websites allegedly selling child pornography related material to the online payment systems, so they could block online payments to the reported illegal commercial website. The

---

[814] See Coaker, V., 'House of Commons Written Answer from the Home Office Minister, Hansard, 15 May 2006, col 716W', (2006)

[815] Williams, C., 'Home Office backs down on net censorship laws', *The Register,* 16 October 2009 at <http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/>, accessed 20 June 2011.

[816] 'Procurement Policy Note – Blocking access to web pages depicting child sexual abuse. Action Note 05/10', (The Office of Government Commerce, 2010) at <http://www.ogc.gov.uk/documents/PPN_05_10_Blocking_illegal_sites.pdf> Accessed 09 July 2011.

[817] See 'Parliamentary records. Answer given by Home Office Minister Alan Campbell on 02 November 2009', (London: UK Parliament - House of Commons, 2009) at <http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091102/text/91102w0017.htm#09110238001607> Accessed 26 May 2012.

[818] The terms of this cooperation was established via the IWF membership process and are found in Article 5 of the ISPA UK Code of Practice. See ISPA, 'ISPA Code of Practice', at <http://www.ispa.org.uk/about_us/page_16.html>, accessed 10 July 2011. See also ISPA, 'Internet Service Providers' Association UK', at <http://www.ispa.org.uk/home/>, accessed 29 June 2010.

[819] Thompson, B., 'Google censoring web content', *BBC News (the billblog),* 25 October 2002 at <http://news.bbc.co.uk/1/hi/technology/2360351.stm>, accessed 20 June 2011; See also IWF, 'Annual and Charity Report 2006', (Cambridge, UK: IWF, 2007) at <http://www.iwf.org.uk>, accessed 07 June 2011.

[820] See 'Mobile Alliance Against Child Sexual Abuse Content', *GSM World,* 2008 at <http://www.gsmworld.com/newsroom/press-releases/2008/775.htm>, accessed 09 July 2011.

[821] 'UK code of practice for the self-regulation of new forms of content on mobiles. Version 2 published on 10 June 2009', (2009) at <http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf> Accessed 07 September 2011.

[822] See 'The European Financial Coalition against Commercial Sexual Exploitation of Children Online', at <http://www.ceop.police.uk/efc/>, accessed 26 May 2011.

IWF requested the ICANN[823] to unregister the domain names of URLs included in the IWF blocklist. Finally, the IWF was a member of the INHOPE Association[824] which comprised a number of Internet hotlines operating in different jurisdictions.

3.3.5 The nature of the IWF: a hybrid creature?

Although the IWF was often considered an Internet industry self-regulatory body, it was perhaps not entirely the case because it operated in a context of substantial governmental interference and has been subject to changes in its governance structure to include wider sectors of society.

Its governance structure has changed over the years. The organisation was revamped in 2000[825] after a review of the IWF, commissioned by the UK Department of Trade and Industry, was published in 1999.[826] Its governance structure was revised again in 2003, and another governance review was commissioned in 2006 because of the growing membership. The IWF Board of Trustees had 10 members: 6 non-industry members selected via open selection procedure; 3 industry members (elected by the Funding Council) and 1 Independent Chair. They served for a mandate of three years term renewable once. The Board of Trustees and the Funding Council oversaw the operation of the IWF. There was a Board Executive comprised of the Audit Committee, Communications Committee and a Remuneration Sub-Committee.[827]

Its funding came initially from the Dawe Charitable Fund in 1996 but moved to the members of the IWF Management Board in 1997. In 2010, a new funding scheme was developed and approved but generally the funding came from the European Union (around 25%) and the UK Internet industry (75%), including the membership fees from the IWF blocking scheme.[828]

In 2005, the IWF achieved Charity Status which allowed the organisation to pursue different funding streams and financial subsidies.[829] Its charitable status has been criticised largely because of its close association with the UK Internet industry (in the end, the IWF is tackling unintended consequences of the Internet industry's economic activity) and arguable lack of

---

[823] The ICANN is the private sector, non-profit corporation, responsible for managing and coordinating the Domain Name System (DNS) to ensure that every address is unique and that all users of the Internet can find all valid addresses. See ICANN, 'Internet Corporation for Assigned Names and Numbers', (updated 01 February 2008) at <http://www.icann.org/>.

[824] INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010.

[825] Davies, C., 'The hidden censors of the internet', *Wired UK*, (2009) at <http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet?page=all> accessed 13 July 2010.

[826] Marwick, P. and Hall, D., 'Review of the IWF', (London: KPMG, 1999) .

[827] IWF, '2008 - Annual and Charity Report ', (Cambridge, UK: IWF, 2009) at <http://www.iwf.org.uk>, accessed 07 June 2011.

[828] Marling, C., 'Interview with Sarah Robertson, director of communications for the Internet Watch Foundation', *Broadband Genie,* 08 April 2009 at <http://www.broadbandgenie.co.uk/blog/full-internet-watch-foundation-interview-20090408>, accessed 07 June 2011.

[829] IWF, 'Annual and Charity Report 2005', (Cambridge, UK: IWF, 2006) at <http://www.iwf.org.uk>, accessed 07 June 2011.

charitable character; a formal complaint was lodged to the Charity Commission in 2009,[830] but this complaint has been dismissed. The Charities Act 2006[831] describes a number of purposes capable of being charitable (*i.e.* including the advancement of human rights and a number of other purposes for the public benefit) and the IWF could arguably fit them as these criteria were generally subjective.

The IWF has altered its governance structure so as to include wider sectors of the society in addition to representatives from the UK Internet industry. Yet, its major funding sources remained in the Internet industry and covered a wide spectrum of members from traditional ISPs to mobile phone companies. There were calls however to include members of the judiciary and increase 'publicness', because of the arguable public functions the IWF performed.[832]

For Price and Verhulst, self-regulation rarely exists without any form of government interference and can take many forms such as 'coerced self-regulation' where voluntary action is coerced via the governmental threat for compliance.[833] As such, it seems that the regulatory approach taken in the United Kingdom is not so self-regulatory nor so voluntary as it might seem at first: the police and the government has been playing a substantial role in the operation of the IWF since its creation in 1996. For example, Walden argues that the activities performed by the IWF are government sanctioned, whether directly or under the veil of self-regulation.[834] Indeed, its 'voluntary' nature has been formed and employed amidst both the police and government threats for regulatory action. The IWF had also strong liaisons with the police and could be seen sometimes undertaking policing and judicial activities rather than performing social responsibility as a self-regulatory industry body. What has been employed was not pure self-regulation but the hybrid regulation addressed in Chapter 2.

This section addressed the laws, cases and regulation to limit access to online child pornographic content in the United Kingdom. It covered state and multi-state regulation as well as key court's decisions in relation to anti-child pornography laws, and overall relevant regulatory landscape. Against this background, the IWF's operation was explored in detail, taking into account its scope, mechanics, regulatory tools, interface with relevant actors and legal nature.

4 Final remarks

---

[830] See Ozimek, J., 'The IWF: Charity disparity?', *The Register,* 20 February 2009, sec. Law at <http:// www.theregister.co.uk/2009/02/20/iwf_charity/>, accessed 02 March 2012.

[831] Charities Act (c. 50) 2006 (England and Wales).

[832] See Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69.

[833] Price, M. and Verhulst, S., 'In the search of the self: Charting the course of self-regulation on the Internet in a global environment', in Chris Marsden (ed.), *Regulating the Global Information Society* (London: Routledge, 2000), 57-78. See also Price, M. and Verhulst, S., *Self Regulation and the Internet* (The Hage, The Netherlands: Kluwer Law International, 2005).

[834] Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62, p 459.

Child pornographic material hosted in Australia was targeted via notices of take down sent by the federal regulator ACMA to relevant Internet content service or hosting service providers. Overseas child pornographic websites were targeted via a voluntary user-level filtering scheme employed since 2000. Nevertheless, a voluntary filtering scheme employed at the ISP-level was launched by the Internet Industry Association in July 2011 to block access to overseas child pornographic websites by the means of a partnership with the Australian Federal Police and Interpol. In addition, the federal government has been trying since 2007 to implement a nationwide mandatory filtering scheme at the ISP-level via legislation to target not only child pornographic content but other types of material included in the federal regulator's blocklist.

In Brazil, the major problem that regulators had to face in relation to limiting the access to child pornographic content until the mid-2005 has been the availability of this material in commercial and non-commercial websites mainly hosted overseas but produced, distributed or accessed by Brazilian residents. Against this background, the Brazilian Internet industry has had little involvement helping to tackle the problem until 2005, amidst no comprehensive national legislation to regulate the operation of online intermediaries. In order to address the failure of both domestic state legislation and Internet industry self-regulation, the Federal Public Prosecution Service MPF-SP, the Internet hotline Safernet Brasil, and later, the Senate CPI have employed a concerted action to update the domestic anti-child pornography legislation and bring private actors into line after 2005.

The United Kingdom operated a regulatory model based on Internet industry self-regulation, centred on the Internet Watch Foundation. The model was not based in legislation nor was directly managed by the government, but it was centred in the work of a self-regulatory body created by the Internet industry that, via a number of interfaces with both public and private actors, operated a system taking down alleged child pornographic content hosted domestically and blocking access to overseas URLs hosting such material.

Although all three jurisdictions employ a hybrid regulatory approach, they are rather different. The Australian regulatory model was established by legislation and relies on a statutory regulator to enforce its rules. Brazil employed a regulatory model based on agreements. The United Kingdom is more self-regulation orientated and relies on a private regulator.

This chapter explored the laws and regulations to limit access to online child pornography in Australia, Brazil and the United Kingdom: it is the documentary evidence. It aimed to provide a detailed account of current regulatory policies. The following Chapter 5 employs the evaluative criteria designed in Chapter 2 against this case study material and develops the analysis further in order to produce a comparative evaluative report on each jurisdiction.

CHAPTER 5: EVALUATING CURRENT MODELS: APPLYING THE EVALUATIVE CRITERIA

This chapter employs the evaluative criteria designed in Chapter 2 against the case study material explored in Chapter 4 to produce an evaluative report on each jurisdiction for the criteria.

The evaluative criteria have three broad categories: (1) free speech - involving issues of unchecked private censorship, scope creep, lack of focus and excessive use of architecture-based regulatory tools; (2) privacy protection - involving issues of increased unchecked and more invasive surveillance powers given to law enforcement authorities; and (3) general democratic values and good regulation - involving issues around the lack of transparency, accountability, legitimacy, proper oversight, and citizen involvement as well as inefficiency and ineffectiveness of regulatory intervention which includes difficulties in evaluating hybrid regulation, crime displacement, unchecked regulatory powers and insufficient safeguards.

Such criteria derive from relevant academic literature and may incorporate other issues arising from each particular case study. As such, the criteria were designed not only as an evaluative but also as a mapping mechanism so as to identify new issues found during fieldwork. Two situations can therefore occur: (1) issues neglected by the literature but found in the field can be added to the criteria; and (2) some items from the evaluative criteria may be irrelevant, or not emphasised in a particular jurisdiction. As a consequence, not all comparators of the evaluative criteria may be discussed in regards to one particular jurisdiction, but only those which were considered relevant in that jurisdiction.

Furthermore, the evaluative criteria are not expected to privilege any jurisdiction in terms of 'best' regulatory practices according to pre-established top-down criteria, because each jurisdiction has a regulatory culture of its own and therefore concepts such as ineffectiveness and inefficiency have to be understood under such cultural underpinnings. This is not an obstacle, for example, to discuss whether the Brazilian model over or under regulates for freedom of speech in comparison to Australia or the United Kingdom. In short, although the regulatory analysis developed here is aware of the dangers of such cultural relativism, it is free to explore a number of avenues for comparison.

Chapter 2 explored a number of regulatory arrangements for online child pornography in a decentred, polycentric, multi-jurisdictional and resilient regulatory environment as well as the negative consequences of hybrid regulation for free speech, privacy protection and general democratic values. Against this background, this chapter explores and compares in detail the different levels of state involvement and the specific public-private hybrid arrangements employed in Australia, Brazil and the United Kingdom; it addresses the different ways whereby hybrid arrangements between public and private actors were designed and implemented to

target the problem of child pornographic material available on the Internet. The critical analysis of such regulatory configurations is expected to help improving current policymaking both domestically and internationally, to identify advantages and disadvantages of each arrangement, and to identify the safeguards needed. Notably, it is also expected to help in moving forward the debate about economic effectiveness of regulation versus principles of justice (*i.e.*, increased regulation to protect children with sufficient safeguards to protect civil liberties and minimise unintended consequences) forward and to show that the problem of controlling online child pornography is not only legal but also regulatory.

1 Summary of case study material

Chapter 4 explored the regulatory models in place in the three chosen jurisdictions. In Australia, although many actors were in the regulatory environment (for example, the Commonwealth statutory regulator, the content service, hosting service and Internet service providers, the Internet industry association, and law enforcement authorities) the state played a central role coordinating the overall regulatory regime. The interface with online intermediaries was performed by a statutory body, the ACMA, and the regulatory regime relies to a great extent in legislation and Internet industry Codes of Conduct. The evaluation criteria applied to the Australian case study material raised the following issues: (1) its potential for scope creep and indiscriminate private censorship; (2) lack of sufficient focus; and (3) problematic transparency, accountability and effectiveness.

In Brazil, many actors were involved in the regulatory intervention such as the Federal Public Prosecution Service, a non-governmental Internet hotline, the Senate and major online intermediaries. Nevertheless, the state was also the main driver of regulatory intervention via the abovementioned Prosecution Service and the Senate both of which forced online intermediaries to come to line with a number of regulations based on agreements. It is also worth noting the role of Safernet Brasil, a NGO Internet hotline, which helped putting the problem in the governmental agenda and providing technical expertise. The mechanics of the regulatory regime is only partially based on legislation; it is to a greater extent based on agreements. The evaluation criteria applied to the Brazilian case study material raised the following issues: (1) regulation via undemocratic channels, unchecked private censorship, and the need of legislated safeguards; (2) problems in terms of legitimacy, transparency and effectiveness or regulatory measures; and (3) crime displacement as well as the issue of which actor is supposed to bear the regulatory costs.

In the UK, although the state was a key actor whether enacting relevant legislation or forcing online intermediaries to do something about the problem (for example, the police), the Internet industry self-regulatory organisation IWF was the main interface with online intermediaries; the key regulator was not statutory but from the Internet industry. Anti-child pornography and legislations escalated over time to cope with developments in digital communication

technologies but the mechanics of the regulatory regime was not legislated; it follows a self-regulatory approach and was implemented voluntarily by the online intermediaries involved. The evaluation criteria applied to the UK case study material raised the following issues: (1) unchecked private censorship, overblocking, scope creep, and alleged violation of the European Convention on Human Rights; and (2) lack of legitimacy, judicial oversight, transparency, accountability, and effectiveness. Although most of the implications discussed in regards to the UK regulatory regime are in relation to the operation of the IWF, some apply to the relevant online intermediary such as ISPs, hosting and content providers.

2 Freedom of expression

2.1 Unchecked private censorship, scope creep, lack of focus and excessive use of architecture-based regulatory tools

In Australia, concerns about free speech violations occurred mainly in relation to the filtering and blocking measures targeting overseas child pornography websites. First, there was a filtering scheme in place grounded in legislation, managed by a statutory regulator, and implemented via Codes of Practice set up by the Australian Internet industry. It was voluntary at the user-level and thus the reported child pornography websites were still available if customers decided not to use the filtering software provided. This voluntary scheme did not much harm free speech, but it was ineffective in stopping people accessing child pornographic material, because customers could opt to use the filters or not. In addition, it had low usage rate by Australian users. This has forced regulators to take more controversial filtering measures onboard.

As a result, major Australian ISPs decided to implement voluntarily, at the ISP-level, a blocklist of alleged child pornography websites provided by Interpol. This scheme was not based on legislation, the relevant safeguards (for example, put back and appealing procedures) were neither robust nor clear, and the assessment of material in the blocklist was performed by an international police agency, not local Australian police forces. Unchecked private censorship was an issue because the blocklist was managed by Interpol, which had an assessment criteria of their own and this might not be in line with the Australian legislation. In addition, the scheme targeted entire websites not the individual URLs; it was therefore wide in scope, although only child pornography was said to be targeted. In addition, the safeguards provided were poorly stated and there were doubts about the possibility of enforcement; it was unclear whether Australian residents could make Interpol accountable for potential abuses.

The Commonwealth government was trying to implement a mandatory blocking scheme via legislation to target overseas websites and cover the broad range of Refused Classification rated material (meaning not only child pornography but other violent material), and it was therefore much wider in scope than the voluntary scheme put in place by the major Australian ISPs. The RC category was under review following a request of the Commonwealth government and, as a

result, the proposed mandatory scheme has been put on hold since then. The proposed blocking scheme based on legislation was also expected to have a more robust range of legislative safeguards. Nevertheless, it was still unclear whether it would be implemented via legislation or administrative regulation, whether there would be any guidance set up by an Internet industry CoP, or whether there would be any statutory safeguards to make the scheme transparent and accountable. The scope of the proposed mandatory blocking scheme was under discussion because it was unlikely that a RC-wide blocklist would pass parliamentary scrutiny and thus an only-child pornography blocklist had more chances to become law under the current political environment.

It has been suggested that online content filtering and blocking are more adequate when implemented via legislation, because it is more democratic, legitimate, and subject to the constitutional channels of accountability and transparency.[835] Although the regulatory framework for online content was established via legislation in Australia (in conjunction with guidance provided by the relevant CoPs), the voluntary blocking scheme implemented recently by major ISPs was employed without a clear legislative mandate and without any statutory safeguards to prevent indiscriminate private censorship. Yet, the fact that there is a statutory regulator and censorship measures are implemented via legislation provides no automatic guarantee that free speech will be protected; the actual implementation of policies and their impact have to be assessed in practice.[836]

Chapter 2 showed that blocklists are often secretive, developed under opaque procedures, largely exempt from public scrutiny, created by institutions unaccountable in the relevant jurisdiction, and that could also be indiscriminately tinkered with by the private actors involved if no sufficient safeguards and transparent procedures are in place. This seemed to be the case in Australia.

For example, blocklists provided by ‘accredited’ family-friendly filter vendors and also the Interpol blocklist were created and maintained by overseas companies. They were built according to assessment criteria that may not be entirely in accordance with Australian anti-child pornography laws. As such, the responsibility for assessing apparent illegality of online material is delegated to foreign organisations (not under the control of Australian law) without proper redress procedures.[837] These blocklists were relatively unproblematic when employed

---

[835] See Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006). See also Bambauer, D., 'Filtering in Oz: Australia's Foray into Internet Censorship', *Brooklyn Law School, Legal Studies Paper No. 125,* (2008).

[836] Duffy argues that this is particularly worrying because of insufficient constitutional protection for free speech in Australia. He argues that censorship laws in relation to online content in Australia has developed since 1999 whereas free speech protection legislation is still stuck in the 1990s. See Duffy, J., 'Toothless Tiger, Sleeping Dragon: Implied Freedoms, Internet Filters and the Growing Culture of Internet Censorship in Australia.', *Murdoch University Electronic Journal of Law,* 16(2) (2009), 91-105, p 104. Bambauer has also reported the lack of express guarantee for free speech in the Commonwealth of Australia Constitution. Bambauer, D., 'Filtering in Oz: Australia's Foray into Internet Censorship', *Brooklyn Law School, Legal Studies Paper No. 125,* (2008), p 8.

[837] Ibid , p 10-11.

voluntarily at the user-level.[838] because it is up to Internet users to decide whether they trust or want a censor to filter content for them, but there was scope for free speech violations and unchecked private censorship when these filters are made mandatory for all users or employed voluntarily at the ISP-level.

Another issue is the lack of sufficient focus. The Australian online content regulation targeted both harmful and illegal content as prohibited or potential prohibited materials. As such, it employed measures that targeted not only child pornographic material but a wide range of content deemed inappropriate to children. For example, adult pornography, violent content, highly offensive material and also 'adult discourse on social and political issues' such as texts and images related to suicide, crime, corruption and marital problems, were targeted.[839] Again, this is relatively unproblematic when implemented voluntarily at the discretion of individual users, but potential threats to free speech arises when there are limited options available for unfiltered access to the Internet. Although the voluntary scheme employed by major Australian ISPs was said to target only overseas child pornography websites, the Australian online censorship regime was wide in scope and this could be even more problematic in relation to free speech protection if the proposed scheme is made mandatory via legislation without robust safeguards implemented in practice such as independent audit of blocklists.

In Brazil, the interface between public and private actors controlling online child pornography was largely based on agreements negotiated between law enforcement authorities and online intermediaries. There were neither filtering nor blocking regimes in place but this does not mean that regulatory measures are exempt from criticisms. Although the NTD scheme, enacted via legislation in 2008, applied only in relation to child pornography, relevant regulatory measures including the overall reporting scheme, liability of online intermediaries, specific regulations of the notice and take down scheme, and safeguards against both the governmental and private indiscriminate censorship were not legislated.

It has been argued elsewhere that the absence of a statutory basis for the regulatory framework may lead to regulation performed via non-democratic means in the online environment.[840] This seemed to be, at least partially, the case in Brazil. Although these agreements: (1) were arguably in accordance with the current legal constitutional environment; and (2) were derived from a dialogue amongst law enforcement authorities (for example Federal and State Public Prosecution Services and the Federal Police), both houses of Parliament (there were a number of public sessions), an NGO (Safernet Brasil), and relevant private actors from the Internet industry; there were no representatives from the judiciary; and the consumer rights, civil

---

[838] It is important to bear in mind however that even when filtering is employed voluntarily at the user level, Internet service and content providers, and also filtering manufacturers, should be transparent about what they filter and the limitations of the technology employed so parents and Internet users in general are better informed.

[839] See Graham, I., 'Blinded by Smoke: The Hidden Agenda of the Net Censorship Bill 1999', *Libertus.net*, (1999) at <http://libertus.net/censor/rdocs/blinded.html> accessed 01 September 2011.

[840] See Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006) and also Lemos, R., *Direito, Tecnologia e Cultura* (Rio de Janeiro: Ed. FGV, 2005), p 93.

liberties and children rights' activists were largely absent from the debate. In addition, these agreements were not enacted via the democratic and formal channels of the Parliament as in the case of a legislation.

Furthermore, the agreements created obligations and sanctions not defined by current legislation and pushed online intermediaries to implement monitoring and removal measures of their own without adequate safeguards and without a comprehensive legislated framework regulating the activities of online intermediaries in Brazil.[841]

Legislative safeguards seem to be needed to avoid abuses from both law enforcement authorities and private actors in Brazil. The implementation of regulatory measures via agreements and without a comprehensive statutory basis represents a potential threat to both privacy protection (in relation to the way access' logs and contents of online communications were disclosed to law enforcement authorities) and free speech (in relation to unchecked censorship performed by both public and private actors).[842] This begs the question of whether legislated safeguards are the way forward (irrespective of the fact that the scheme is established by legislation or based on agreements) or whether such protection can be left to the regulatory actors' will. The examples of Australia and Brazil seem to indicate the need of more robust legislated safeguards to prevent abuses and unchecked censorship.

The problematic regulatory role of private actors controlling online content is also an issue in Brazil, particularly in relation to the Internet hotline Safernet Brasil, which was a key interface with online intermediaries because it managed a national database of reports and had an authoritative position to force online intermediaries to remove the material reported. Safernet Brasil received, processed and forwarded reports to law enforcement authorities concerning the availability of child pornography on the Internet (mainly websites). It also created, and maintained a central database of reports that was shared by a substantial number of law enforcement authorities.

There has been little opposition to the website reporting scheme implemented by the hotline, particularly because child pornographic content was considered blatantly illegal and thus expected to be removed immediately without further discussions.[843] Nevertheless, judgement of illegality of content should be a function of the courts, because there is a possibility that non-

---

[841] There was a bill under discussion within the government but it was unclear when it would be submitted to Parliament; the bill is expected to address the issue of NTD in relation to all types of online content, and this may have implications for the existing notification scheme in regards to online child pornographic content. See Marco Civil da Internet (2010). at <http://culturadigital.br/marcocivil/>, accessed 26 April 2011.

[842] Notably, the need of legislated safeguards has been stressed in other jurisdictions as well. For example, Nunziato suggests that online intermediaries should be considered as public organisations in relation to free speech laws, because they are arguably performing public functions, and then goes on to recommend that legislated safeguards should be put in place so as to force these private actors to refrain from unchecked censorship of online speech. See Nunziato, D., *Virtual freedom: net neutrality and free speech in the Internet age* (Stanford: Stanford University Press, 2009).

[843] For this opinion see Leonardi, M., 'Controle de conteúdos na Internet: filtros, censura, bloqueio e tutela', in Newton de Lucca and Adalberto Simão Filho (eds.), *Direito & Internet: aspectos jurídicos relevantes* (vol. II; São Paulo: Quartier Latin, 2008), 377-401.

child pornographic material (such as legal adult pornography, cartoon pornography and texts) be considered child pornography by the content analyst of the Internet hotline. Excessive reporting and high removal rates were an issue in Brazil.[844] Another problem was the level of dependency that public authorities had in relation to one unaccountable private institution; Safernet Brasil was not subject to wider public scrutiny. The Internet hotline was generally unaccountable to the public, it was under no permanent judicial oversight, its activities were not subject to any external audit,[845] and its financial sources (it was funded in a non-permanent way by public and private actors) raised doubts about its true independence.

In the UK, the problem of unchecked private censorship was also emphasised, particularly because of the central role that a private actor from the Internet industry had in the regulatory arena. The fact that the main interface with online intermediaries was a self-regulatory body raised a number of concerns in relation to free speech protection. For example, the problem of overblocking, *i.e.,* when not only the targeted illegal but also legal content is blocked, has been associated with IWF blocklist.[846] Another issue was the lack of control and transparency around the implementation of the IWF blocklist on the part of ISPs: there were no safeguards to avoid controversial material being added to the IWF blocklist by member ISPs. As such, it was very likely that UK Internet users had different filtered access to websites depending on the ISP they subscribed to. Internet service and content providers had contractual agreements with each costumer that determined the kind of service they provide, and these contracts did not establish that the user had an absolute right to access anything on the Internet. Such position represents a discretionary power that can be used to chill free speech; online intermediaries were not under any public obligation to restraint from including other material in the blocklist provided by the IWF.[847]

In any case, it is no easy task to know when overblocking occurs. In principle, it should be an objective judgement based on what type of content is considered illegal and what has been included in the blocklist. If the blocklist contains legal material, overblocking is occurring. Nevertheless, some jurisdictions deny access to the contents of such blocklists (for example, Australia) and there is also the problem of interpreting the law to identify what illegal material is in practice, especially in the case of borderline material such as child erotica and explicit

---

[844] Excessive reporting occurs when members of the public wrongly consider offensive content such as extreme pornography as illegal. Excessive removal rates occurs when the relevant online intermediary removes the reported content indiscriminately because it has more incentive to do so than to risk being criminally liable. See for example the complaint made by the MPF-SP about the great volume of obscene content reported to them by Google Brasil as if the material was child pornography. Suiama, S., 'Nota Técnica GCCC/PR/SP', (São Paulo: MPF-SP, 2010) at <http://www.prsp.mpf.gov.br/sala-de-imprensa/pdfs-das-noticias/crimes-ciberneticos> Accessed 19 April 2011.

[845] For example, the MPF-SP audited the operation of its partner Safernet Brasil for the first time only after five years from initial institutional cooperation, and the Internet hotline failed the test. See Section 4.5 above.

[846] The Wikipedia incident discussed below can be understood as an example of overblocking but it also shows the difficulties in establishing what is, or is not, illegal under the UK law without the adequate judicial scrutiny. That were also claims that the secretive blocklist of URLs contained not only child pornography related websites but perfectly legal material. See, *e.g.,* Ozimek, J., 'A censorship model', *The Guardian,* 02 August 2009, sec. Global at <http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/02/internet-censor>, accessed 20 June 2011.

[847] There were public calls to make these online intermediaries subject to wider civil liberties protection via legislation. See Section 4 of Chapter 2.

sexual material involving adolescents. In the end, what should be a result of objective judgment may become a subjective judgement call on the side of content analysts.[848] Greater transparency about what has been blocked (for example, via independent audits), the development of industry standards of good practice and permanent automatic monitoring are needed to check whether overblocking has occurred or not.

This criticism was particularly strong after the 2008 Wikipedia incident. On 04 December 2008, the IWF received a complaint about the availability of an album cover[849] depicting potentially criminal content under UK law; this was an image of a naked child with a cracked glass effect covering her genitals made available on the free-encyclopaedia project Wikipedia.[850] Subsequently, the IWF included the reported URL in its blocklist and, because of the technical nature of the blocking system, not only this specific image was blocked within the United Kingdom, but the ability of UK users to add new content or to edit existing content were also undermined. This produced a public outcry, particularly because the image was freely available via commercial websites such as Amazon.com.[851] Following this, the IWF Board started its appeal process[852] and, although it considered its content analyst right to block the image, under UK law,[853] the Board decided to remove the URL from the blocklist because of contextual issues, *i.e.* the image was not within a paedophilia related context.[854] For Edwards, this incident made evident the problematic operation of a non-judicial body assessing the illegality of content online because the IWF had no legal authority to assess the illegality of content, there were no adequate appeal process nor was explicit notice sent to content providers.[855] It is worth stressing however that in addition to the problem of overblocking, the 2008 Wikipedia incident showed the difficulties in establishing the illegality of borderline child pornographic images without adequate judicial oversight.[856]

The IWF's operation also raised fears of scope creep. This relates to the fact that, after the blocking scheme is implemented, other types of content (such as terrorism related, incitement to racial hatred, copyright infringement, politically sensitive and adult pornography) may be

---

[848] Interestingly, many ISPs filtered for other things such as viruses and phishing messages but these did not lead to strong criticisms as in the case of child pornography. Perhaps, this is because the problem of online child pornography draws much more public attention and thus are pushing the law and regulatory measures quickly and with greater public support, which is a real threat to free speech and privacy protection.

[849] The 1976 Virgin Killer's album by the German heavy metal band Scorpions.

[850] Wikipedia, 'Wikipedia: a multilingual, web-based, free-content encyclopedia project based on an openly editable model.', at <http://en.wikipedia.org/wiki/Main_Page>, accessed 09 July 2011.

[851] Petley, J., 'Web Control', *Index on Censorship,* 38(1) (2009), 78-90, p 90.

[852] Indeed, this shows a certain degree of responsiveness. See IWF, 'Content Assessment Appeal Process', at <http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process>, accessed 09 July 2011.

[853] The Protection of Children Act (c.37) 1978 (England and Wales).

[854] See IWF, 'IWF statement regarding Wikipedia webpage' (2008); <http://www.iwf.org.uk/media/news.archive-2009.251.htm> accessed 13 July 2010. See also Ozimek, J., 'IWF chief: We don't need crusaders', *The Register,* 08 September 2009 at <http://www.theregister.co.uk/2009/09/08/iwf_peter_robbins_interview/>, accessed 07 June 2011.

[855] Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88.

[856] This point was made by one of the UK experts consulted during the validation scheme.

included in the blocklist.[857] For McIntyre, the UK Internet industry has opposed so far the inclusion of other less contentious types of material within the IWF blocklist,[858] but there were nor legislative safeguards to limit censorship escalation towards other regulatory targets; neither industry standards in relation to redress procedures, independent audits, and monitoring of overblocking.

The IWF has also been criticised on other grounds. For example, McIntyre[859] stresses that the IWF blocking regime violates the right to free speech under Article 10 of the European Convention on Human Rights (ECHR).[860] In addition, McIntyre stresses that the IWF blocking scheme violates the right to free speech because the scheme is not prescribed by law and have to be performed under the conditions and safeguards established by Article 6 of the ECHR.[861]

Nevertheless, the right to free speech is not without limitations. It permits a certain degree of interference as it is prescribed by law and necessary in a democratic society. According to Article 10(2) of the ECHR, it may be subject to '[…] 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 [...].' The issue here is not that blocking schemes should be scrapped entirely but that they should be implemented according to the law and subject to sufficient safeguards so as to secure the right to impart and receive information.[862]

Finally, it has been reported that the IWF blocking system could be easily circumvented and used as an 'oracle' to obtain the list of URLs blocked,[863] and the secretive blocklist can leak as it

---

[857] Edwards, L., 'Editorial: From child porn to China, in one Cleanfeed ', *Script-ed,* 3(3) (2006), 174-5 Also Petley, J., 'Web Control', *Index on Censorship,* 38(1) (2009), 78-90, p 87.

[858] McIntyre, T., 'Internet Filtering: Implications of the "Cleanfeed" System', *Third Year PhD Presentation Series* (Edinburgh: School of Law, University of Edinburgh, 2010) at <http://www.law.ed.ac.uk/file_download/communities/245_tj%20macintyre%20-%20internet%20filtering-%20implications%20of%20the%20cleanfeed%20system.pdf>, accessed 29 February 2012.

[859] See McIntyre, T., 'Blocking child pornography on the Internet: European Union developments', *International Review of Law, Computers and Technology,* 24(3) (2010), 209-21. See also Akdeniz, Y., 'To block or not to block: European approaches to content regulation, and implications for freedom of expression', *Computer Law & Security Review,* 26 (2010), 260-72.

[860] EU Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14. 1950 (04 Nov 1950) (European Union).

[861] See McIntyre, T., 'Blocking child pornography on the Internet: European Union developments', *International Review of Law, Computers and Technology,* 24(3) (2010), 209-21. This criticism is also advanced by Akdeniz. See Akdeniz, Y., 'To block or not to block: European approaches to content regulation, and implications for freedom of expression', *Computer Law & Security Review,* 26 (2010), 260-72

[862] It is worth noting that free speech involves not only the right to impart information but also to receive information. Walden argues that the legal debate around free speech is moving from the right to (or regulation in relation to) impart information towards the right to (or regulation in relation to) receive information, because it is increasingly more difficult to monitor the publication and availability of user generated content, particularly hosted overseas, by content and hosting providers, in comparison to the easier implementation of automatic content filters by ISPs. See Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62, p 461-2.

[863] See Clayton, R., 'Anonymity and traceability in cyberspace', *Technical Report Number 653* (Cambridge: University of Cambridge, 2005) at <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html>, accessed 20 June 2011. Updates and fixes could have been implemented by the BT since the release of the report in 2005.

happened in Australia in 2009,[864] the material blocked can be moved to a different location in a different URL (so the blocking system has to be updated permanently). Another criticism is that blocking schemes implemented domestically inhibits international cooperation,[865] because this deviates attention from policies that may remove the material at its source.

Such numerous criticisms made to the IWF derives in part from the fact it is a private regulator acting as a gatekeeper for content control, working in line with the anti-child pornography laws but largely in a self-regulatory manner; and that by over regulating, the IWF risks chilling free speech. The problem here is the lack of transparency, legitimacy and accountability of a private actor undertaking censorship duties as well as the inexistence of robust and clear scheme of safeguards to guide its operation and make it accountable to the public.[866]

2 Privacy protection

2.1 Increased unchecked and invasive surveillance powers given to law enforcement authorities

The crusade against online child pornography has updated not only substantive criminal laws and regulations but it has also increased the investigatory powers of law enforcement authorities and facilitated the disclosure of personal data by online intermediaries to the latter. This has certainly a deterrent effect on those trying to access child pornographic material, but more importantly, it facilitated the launch of a number of international police operations. Nevertheless, increasing invasive surveillance powers of law enforcement authorities can also have unintended consequences such as the violation of privacy of individuals, wrongful accusations and trial by the media, if proper checks and balances are not in place.

The three case studies showed that anti-child pornography laws and investigatory powers of law enforcement authorities have been updated to catch up with the increased use of digital technologies by online criminals involved with online child pornography offences. Under these updated provisions, many police operations took place domestically and internationally. These legislative developments also make evident the need of a framework of checks and balances to avoid abuses and facilitate the compensation for unlawful interceptions.

Chapter 4 showed that Australia has a robust legislative framework to regulate the issuing of warrants and use of surveillance equipment, and also an oversight scheme to protect against

---

[864] Bingemann, M., 'ACMA blacklist leaked on the internet', *The Australian,* 19 March 2009, sec. Australian IT at <http://www.theaustralian.com.au/news/acma-blacklist-leaked-on-the-internet/story-e6frgb5x-1225700508594>, accessed 24 June 2011; See also Moses, A., 'Leaked Australian blacklist reveals banned sites', *The Sydney Morning Herald,* 19 March 2009, sec. Technology at <http://www.smh.com.au/articles/2009/03/19/1237054961100.html>, accessed 24 June 2011.

[865] Villeneuve, N., 'Barriers to cooperation: An analysis of the origins of international efforts to protect children online', in Ronald J. Deibert, et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010), 59-70.

[866] See a similar point advanced by Laidlaw in relation to search engines. Laidlaw, E., 'Private Power, Public Interest: An Examination of Search Engine Accountability', *International Journal of Law and Information Technology,* 17(1) (2008), 113-45.

unlawful interceptions. In Brazil, there were bills under discussion in Parliament about the preservation of access' logs and the contents of online communications as well as about the way they could be requested by and disclosed to law enforcement authorities. Although, a number of agreements with ISPs established protocols for the disclosure of customers' data to aw enforcement authorities, as for 2010, a court order was needed to access the contents of an online communication,[867] whereas the access logs (including IP address, GMT's data and time etc.) could be disclosed to law enforcement authorities without a court order.[868] In the UK, the RIPA 2000 established a regime for the interception of communication, acquisition and disclosure of data, carrying out covert surveillance, use of covert human intelligence sources and encryption; this allowed the police and other law enforcement authorities to request information from online intermediaries without a court order.[869]

This investigation and the methods employed were unable to reveal many relevant points in relation to privacy protection. As such, further research is needed to explore in detail the laws and regulations in this area and their impact on the privacy of Internet users. It is also necessary to identify which type of violations occur in each jurisdiction in relation to child pornography related investigations and the existing safeguards. The documentary analysis alone was unable to identify how these provisions work in practice and how violations of privacy occur. Another research method such as interviews and participant observation are necessary to uncover the implications that such legislative developments may have in terms of privacy protection.

3 Democratic values and good regulation

3.1 Lack of transparency, accountability, legitimacy, proper oversight and citizen involvement

Although the Australian regulatory scheme was established via legislation and therefore under the existing constitutional accountability and transparency principles, access to the ACMA blocklist of prohibited and potential prohibited material was particularly controversial following the denial of a Freedom of Information (FOI) request. In February 2000, the Electronic Frontiers Australia (EFA)[870] submitted a request to the Commonwealth regulator, under the FOI Act 1982,[871] demanding detailed data about the online content added to the ACMA blocklist.

The regulator at that time, the ABA, released part of the information requested but denied access to other parts of the blocklist arguing that the disclosure would have an adverse effect on the

---

[867] Following Article 5(X and XII) of the Brazilian Constitution. See Constituição da República Federativa do Brasil 1988 (Brazil). US-based companies are required by law to disclose the contents of an online communication, without a court order, in some critical circumstances *e.g.* the reports of child pornography and immediate threat to life. See '18 U.S.C. § 2702 US Code - Section 2702: Voluntary disclosure of customer communications or records', (USA, at <http://codes.lp.findlaw.com/uscode/18/I/121/2702>, accessed 20 March 2012.

[868] This is subject to legal controversy, because some believe that even the disclosure of such data is also subject to a judicial order.

[869] Regulation of Investigatory Powers Act (c.23) 2000 (England and Wales).

[870] See EFA, 'Electronic Frontiers Australia', at <http://www.efa.org.au/>, accessed 22 August 2011.

[871] Freedom of Information Act 1982 (Cth Australia).

ABA's ability to administer the regulatory scheme either properly or efficiently; indiscriminate disclosure would make public a list of overseas websites containing material forbidden in Australia. As a result, the EFA appealed to the Administrative Appeals Tribunal (AAT) in October 2000 and a final decision was issued on 12 June 2002.

Although the Tribunal emphasised the 'honourable reasons' presented by the EFA and that 'secrecy may of itself undermine the public's confidence' in the federal regulator, they ruled in favour of the ABA: the list of URLs included in the blocklist were exempt from disclosure under the FOI Act 1982. The Tribunal decided that the documents in dispute (URLs and IP addresses) were exempt from disclosure, and argued that the adverse effects of disclosing such information outweighed the public interest.[872] Two weeks later, the federal government proposed amendments to the FOI Act 1982 so as to exempt from disclosure even a wider spectrum of prohibited material included in the blocklist. Perhaps, to minimise criticisms and accelerate the approval, the Parliamentary debate around these amendments focused on the harms of disclosing URLs and IPs allegedly hosting child pornographic material overseas, despite the fact that a broader range of content categories might have been added to the ACMA blocklist.

The Tribunal decision and the following statutory amendment raised a number of issues not only in relation to the transparency but the accountability of the federal regulator as well as the potential for scope creep, because not even independent audit could scrutinise the ACMA blocklist. This was one of the reasons why some critics argued that regulation of online material in Australia is more opaque and unaccountable when compared to regulation of traditional media such as print publications, offline films and videos, and DVDs.

> The online censorship regime operates in stark contrast to the offline censorship regime. Not only is online content censored, information about what is censored is also censored. Offline material is classified by the government appointed Classification Boards. Members of the Boards are publicly named, and titles of classified material, including that 'Refused Classification' (i.e. banned from sale etc.), are made publicly available in the Board's online classification decision database. Publishers/distributors of offline material are entitled to 'appeal' a Classification Board decision by applying for review by the Classification Review Board, which from time to time overturns a classification decision and grants lower a classification rating, including in relation to material that was refused classification/banned by the Classification Board.[873]

In regards to the accountability of the scheme, the ACMA hotline was required to report to the Minister of DBCDE every six months about the operation of its blocklist and the Minister was required to report this to the Commonwealth Parliament following a resolution from the

---

[872] See The AAT decision in Electronic Frontiers Australia Incorporated and Australian Broadcasting Authority Q2000/979 (2002). Adminstrative Appeals Tribunal, at <http://www.efa.org.au/FOI/AAT2000-979_dec.pdf> accessed 01 September 2011.

[873] Graham, I., 'Australia's Internet Censorship System', (updated 11 April 2010) at <http://libertus.net/censor/netcensor.html>, accessed 01 September 2011. See also Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52, p 348.

Senate.[874] Nevertheless, these six-months reports ceased being made after 2005 and no explanation for this has ever been publicly stated. Decisions about including any prohibited or potential prohibited material available online to the blocklist were made by unnamed staff. They assessed the potential prohibited nature of the reported content and this decision cannot be appealed because it was not subject to review under Schedule 5 of the amended 1992 Act.[875] In addition, the ACMA was not required to inform the relevant overseas content service and hosting service providers about overseas websites included in the blocklist.

In Brazil, in regards to the transparency of policies in place, it has been claimed that the notification scheme was transparent and democratic, because many institutions can report, manage and have access to the national database of reported websites. Nevertheless, it was also the case that many online intermediaries were developing regulatory measures of their own in non-transparent ways after law enforcement authorities made them come into line and the agreements were in place.

The lack of legitimacy of policies was also an issue in Brazil. The fact that regulatory measures were put forward by the Public Prosecution Service (the MPF-SP and others), a non-governmental organisation (Safernet Brasil), the Senate (via the CPI) and online intermediaries may indicate that these policies are legitimate. Nevertheless, this is debatable because during policymaking there were no representatives from the judiciary; and consumer rights, civil liberties and children rights' activists were largely absent from the debates that led to legislative changes and negotiation of agreements.

The lack of transparency was also an issue in the United Kingdom. For Davies, the image of a heroic body fighting online child pornography saved the IWF from greater scrutiny,[876] but the lack of transparency and public scrutiny in relation to its operation have been criticised, particularly the NTD and blocklist schemes, where no information was given by the member ISPs to the content provider that the relevant content has been removed or blocked, nor was any specific message given to those who try to access the website URL or blocked (some ISPs provided only a standard 403 message without reporting the reason for blocking it).[877] It is important to bear in mind however that the IWF creates the blocklist but it is up to member ISPs to implement it. As such, it was up to the member ISPs to provide this information to a content provider and, perhaps, it was not in their interest to give any transparent information about the

---

[874] See 'Six Month Report on Co-Regulatory Scheme for Internet Content Regulation', (Australia: Minister for Communications, Information Technology and the Arts, 2000) at <http://www.archive.dbcde.gov.au/__data/assets/file/0013/11560/Six-month_report_on_co-regulatory_scheme_for_internet_content_regulation_January_to_June_2001.rtf>.

[875] See Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Part 2', Internet Industry Association - IIA Australia, 2008) at <http://www.dbcde.gov.au/__data/assets/pdf_file/0019/95311/Part_2_-_Attachments_Final.pdf>, accessed 07 September 2011, p 123.

[876] Davies, C., 'The hidden censors of the internet', *Wired UK*, (2009) at <http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet?page=all> accessed 13 July 2010.

[877] Whether a 403 or 404 page is displayed or not, is a choice for the relevant ISP.

specific website blocked because this could reveal they were blocking more than prescribed by the IWF.

In short, these criticisms about the lack of transparency apply to both the IWF and the ISPs that operate the website blocking scheme. Nevertheless, the IWF reported on these accounts that its blocklist was independently audited and considered to be following the best standards. Finally, there were criticisms about the lack of appeal process and put back procedures, but it seemed that after the Wikipedia incident, the IWF established a series of provisions in this regard.[878]

In terms of accountability, Petley argues that the existence of the IWF masks the fact that the state is covertly censoring the Internet in the United Kingdom via third parties, and this arguably undermines the ability of content authors, whose photographic or non-photographic material may be deemed illegal, to defend themselves in courts. In addition, he argues that there is a strong governmental support for the operation of the IWF but no 'sustained parliamentary or public scrutiny or debate.'[879] This highlights the issue of censorship performed via indirect manners, *i.e.* the fact that the state undertakes censorship without the political cost (for example, of proposing legislation and facing both the political opposition and challenges in courts) by forcing online intermediaries to do the politically unattractive work via self-regulatory non-transparent initiatives that go unnoticed by the population at large.[880]

The IWF has also been accused of performing privatised policing and censorship of online content and of acting as self-appointed judges.[881] Although the nature of child pornographic content may be self-evident and the IWF seemed to be focusing on the more dangerous images,[882] not on borderline material such as child erotica, it has been put forward that the evaluation of content legality should be a responsibility of the courts.[883] This raises the question of whether the perception of illegality, the determination of potential illegality, or even the determination of illegality is inherently a judicial responsibility. In fact, these processes are performed by different social actors, on a daily basis, on a number of different areas, not just on the Internet. The judgement of IWF's staff has never been exempt from judicial redress; although it seems that there are not strong incentives for free speech activists or UK online intermediaries to challenge IWF's decisions in courts in relation to alleged child pornographic content. The problem is perhaps that digital communication technologies made possible for these processes, related to the perception and determination of illegality, to operate in an

---

878 See IWF, 'Content Assessment Appeal Process', at <http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process>, accessed 09 July 2011.

879 Petley, J., 'Web Control', *Index on Censorship,* 38(1) (2009), 78-90, p 84 and 87.

880 See Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006), p 133, about 'indirection'.

881 Akdeniz, Y., 'Controlling Illegal and Harmful Content on the Internet', in David Wall (ed.), *Crime and the Internet* (London: Routledge, 2001), 113-39.

882 In relation to levels of seriousness of indecent photographs of children for sentencing purposes. See Sexual Offences Act 2003: Definitive Guideline (2007). Sentencing Guidelines Council, at <http://sentencingcouncil.judiciary.gov.uk/docs/web_SexualOffencesAct_2003.pdf> accessed 10 July 2011, p 109.

883 This is one of the reasons why the IWF labels the content it notifies as 'potentially illegal' rather than 'illegal'.

automated manner, in larger scale, and therefore with wider implications if something goes wrong.

Despite the fact that the IWF has suffered governance reforms along its existence, it has been criticised for not representing the public at large, for lacking citizen involvement in most aspects of its operation and for its self-appointed private nature that lacked adequate legislative foundations. The problem here is the dubious constitutional nature of the IWF as a private body performing a quasi-judicial (investigating content and assessing its illegality) and a public function (determining what should be or not be seen by the Internet users) in the United Kingdom, which led some to advance the argument for increase 'publicness' (or its transformation into a statutory body) of the IWF, or to include in its Board not only members of the Internet industry but legal professionals and charity representatives, chaired by an independent member of the judiciary.[884] Although the IWF has been externally audited by independent experts, perhaps more public oversight is needed to increase transparency. It may be the case that the IWF should be embraced by the government in order to be under broader public scrutiny, subject to judicial review and the traditional channels of accountability.[885] Nevertheless, there seems to be little motivation in this regard as well as to enshrine the IWF and its functions in law. The IWF has been debated and referred to in both Houses of Parliament, in a number of court cases, and it often cited as an example of good practice by the British government; at least, in practice, it has been legitimised by the executive, legislative and judiciary. Nevertheless, as explained in regards to the Australian regime, this is no automatic guarantee that free speech will be protected in practice and that a robust scheme of safeguards are needed.

It is difficult to define the regulatory nature of the Internet Watch Foundation. Is it a private organisation undertaking a public function? Is it a government body or a charity? Is it a 'quasi-public'[886] or a 'quasi-private' organisation? In which legal framework should the IWF be placed? Ultimately, the IWF is a hybrid creature that incorporates features of a statutory regulatory body and, at the same time, constitutes an Internet industry self-regulatory organisation. It on one hand this hybrid configuration overcomes a number of disadvantages of a state or self-regulatory institution, on the other hand, it is also subject to the criticisms of both models. It is worth noting that these questions are not only theoretical, but have practical implications for the accountability of the IWF. For example, McIntyre stresses that questions are crucial to determine the grounds for the IWF's accountability, *i.e.* whether the IWF should be

---

[884] Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69, p 655.

[885] Ozimek, J., 'A censorship model', *The Guardian,* 02 August 2009, sec. Global at <http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/02/internet-censor>, accessed 20 June 2011.

[886] Wall, D., 'Policing and the Regulation of the Internet', *Criminal Law Review. December Special Edition: Crime, Criminal Justice and the Internet,* (1998), p 85.

viewed as a (1) public body, and therefore subject to judicial review; or as a (2) body undertaking a public function and thus subject to the Human Rights Act.[887]

The lack of sufficient safeguards is another issue found in the UK both in relation to the NTD and blocking schemes. The NTD regime established by the 2000 EU Directive on Electronic Commerce,[888] and on which the IWF operation is based, was not without criticism. For Edwards, the Directive is unclear about what 'expeditious' take-down means, is omissive about the rules of a notification regime and lacks both adequate mechanisms of appeal and put back procedures.[889] As a result, the lack of safeguards on the part of the online intermediaries could lead to excessive and indiscriminate content removal, because there were no incentives to do otherwise.[890] In addition, there was no safeguard in place to stop ISP members tinkering with the IWF blocklist.

In short, online intermediaries were subject to increased control by domestic regulators and had no incentive to challenge these regulatory measures in courts as advocates of free speech or civil rights. Unless the issue at stake involved financial expenses on their part (for example, the implementation of notification mechanisms associated with online copyright infringement in the UK or the debate over the use of public funds to finance the regulatory infrastructure in Brazil).[891]

In addition, Edwards points out that the strategy[892] employed by online intermediaries around the late 1990s no longer apply and thus there has been increased regulation and liability being placed on them over the years.[893] This seems to suggest that it is necessary to design and implement safeguards, statutory or otherwise, to prevent abuses committed by either governments or online intermediaries worldwide.

---

[887] See McIntyre, T., 'Internet Filtering: Implications of the "Cleanfeed" System', *Third Year PhD Presentation Series* (Edinburgh: School of Law, University of Edinburgh, 2010) at <http://www.law.ed.ac.uk/file_download/communities/245_tj%20macintyre%20-%20internet%20filtering-%20implications%20of%20the%20cleanfeed%20system.pdf>, accessed 29 February 2012, p 8.

[888] EU Directive on Electronic Commerce. DIRECTIVE 2000/31/EC, 08 June 2000 (European Union).

[889] In fact, informing the alleged provider of online child pornographic content that his/her content has been removed may be problematic, because it can alert alleged culprits they are under police investigation. See Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88.

[890] Similarly, Walden points out that the exercise of indiscriminate editorial powers by online intermediaries are likely to escalate as a result of more user-generated content being produced, because online intermediaries may try to avoid the risk of criminal liability and litigation via the implementation of *ex ante* automated filtering, content analysis and similar strategies. See Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: OUP, 2009), 427-62, p 458. This was also the case in Brazil; see Chapter 6.

[891] See Halliday, J., 'BT and TalkTalk denied Digital Economy Act appeal', *The Guardian,* 12 June 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jun/21/bt-talk-talk-digital-economy-act>, accessed 21 June 2011. See also Halliday, J., 'Digital Economy Act will cost nearly £6m', *The Guardian,* 17 June 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jun/17/digital-economy-act-cost>, accessed 20 June 2011.

[892] The reasons for being exempt from legal liability were: it is impossible to monitor; they are mere conduits; and that the high costs of monitoring would limit the growth of the digital economy.

[893] Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88, p 81. See also Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009).

For example, the 2011 EU Directive was concerned about these safeguards in relation to the blocking of child pornography websites in Europe. According to Article 25(2):

> These measures [*against websites containing or disseminating child pornography*] 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.[894]

Although there are a number of criticisms on the work of the IWF, this organisation has survived so far and changed its governance structure and regulatory methods to address some of these criticisms. It operates according to current UK domestic legal framework, has substantial support from the government and both Houses of Parliament, and it has inspired other European countries in the area of online content regulation, particularly in relation to child pornographic material.

Indeed, the IWF operates in a problematic area where regulatory configurations involving public and private regulators are still in their infancy and are subject to constant change and permanent learning. In addition, such complicated operation involves numerous reports from the public and thus extensive and detailed analysis of material that may result in errors and wrongful actions. This is the reason why a robust scheme of safeguards is needed to meet standards of accountability and transparency as well as to minimise violations of free speech and focus only on the problem they were designed for: child pornographic material. Such claim for stronger accountability of the IWF which act as a gatekeeper of online content is also made elsewhere in relation to other private organisations such as search engines. This makes evident the importance that private actors have in regulation of content, the need of state intervention to design and enforce minimum standards of accountability, transparency and citizen involvement, and a flexible system to enforce sanctions whenever necessary.[895]

3.2 Difficulties in evaluation of hybrid regulation

In Australia, the online content regulatory regime was implemented to address preoccupations about the easy access to material available on the Internet which was either pornographic or unsuitable for children and young people in addition to material of more serious nature such as child pornography. Although regulatory measures were arguably effective to remove child pornography available in public websites hosted in Australia,[896] they were unable to stop people

---

[894] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union).

[895] See *e.g.* Laidlaw, E., 'Private Power, Public Interest: An Examination of Search Engine Accountability', *International Journal of Law and Information Technology,* 17(1) (2008), 113-45*;* Nunziato, D., *Virtual freedom: net neutrality and free speech in the Internet age* (Stanford: Stanford University Press, 2009) and Perritt Jr., H. H., 'Towards a hybrid regulatory scheme for the Internet', *University of Chicago Legal Forum,* (2001), 215-332.

[896] Given that this is a complain-based regime, unreported child pornographic content may still be available in public websites hosted in Australia. Also, there is evidence to suggest that other Internet applications and platforms may give access to child pornographic content hosted in Australia in private repositories, but this is a matter of intensive police investigation.

accessing such material hosted overseas, or even the child pornographic material hosted in Australian but available in online private repositories accessed via Internet platforms and applications other than websites. This ineffectiveness was partially because the voluntary filtering scheme established via legislation depended on the will of customers to buy and use any of the 'accredited' family-friendly filters. This approach changed after the IIA's ISP-level voluntary scheme came into effect in July 2011, but (1) this new initiative only affected the customers of participating ISPs and (2) it only targeted overseas websites, not the applications and platforms such as e-mail, private websites, file transfer protocol, P2P and other anonymised channels. These applications and platforms were outside the scope of the planned mandatory blocking regime put forward by the Commonwealth government. As a result, existing policymaking targeted only a small part of the problem, it did little to protect children from inappropriate material available on the Internet and it may be giving parents a false sense of security.[897]

In Brazil, the provisions implemented via legislation (particularly the possession offence and the limitation of criminal liability of online intermediaries), the number of agreements negotiated amongst law enforcement authorities and private actors, the creation of a national reporting scheme as well as the monitoring and removing schemes developed by the online intermediaries, all have been arguably effective in limiting access to commercial and non-commercial child pornography websites hosted domestically. Nevertheless, the problem remained in relation to websites hosted overseas and the many other platforms where child pornography was distributed and accessed in Brazil. Indeed, the fact that only a portion of reported websites were found to be hosted domestically did not mean that online child pornography was non-existent in the country. In addition to material that goes unreported but is hosted in the country whether available via websites or other anonymised online platforms, Brazilian residents are able to produce, as well as distribute and access child pornographic material hosted overseas. Blocking of overseas child pornography websites has not been employed in Brazil, neither voluntarily nor mandatorily. On the one side, this decision avoided a number of potential threats to free speech, but on the other side, it left part of the problem unchallenged.[898]

Another important issue derived from the Brazilian case study concerns who is to bear the costs of implementing the regulatory measures. Much of the opposition made by online intermediaries against regulation from the government, and perhaps the lack of participation of the Brazilian Internet industry in a self-regulatory environment, had to do not with the protection of free speech and privacy of users online, but rather with the will of online intermediaries to avoid bearing the costs in implementing regulatory measures advanced by the

---

[897] Graham, I., 'The Net Censorship Dilemma: Liberty or Tyranny', (updated 06 June 2009) at <http://libertus.net/liberty/>, accessed 01 September 2011.

[898] The decision not to employ blocking mechanisms might be a result of substantial public opposition to censorship measures, particularly after the end of the military dictatorship in the mid-1980s and also as a result of the political and financial costs associated with such endeavour.

state. Given that there was neither a statutory regulator of online content (like in Australia) nor a self-regulatory Internet industry body (like in the UK) to bear most of the regulatory costs involved, agreements that did not established clearly who would finance such regulatory enterprise was a good compromise for the Internet industry, until legislation makes clear who is to bear these costs. In fact, there is a strong lobby from the Internet industry for the use of public funds to finance the regulatory costs.

If on the one hand, the government is expected to enforce the anti-child pornography laws and protect children online, on the other hand, it should achieve such aims with efficient and effective regulations without imposing excessive financial burden on online intermediaries to make these regulations work. In principle the Internet industry should be more pro-active in the search of and funding of solutions. Nevertheless, whether the state should use public money to implement regulatory measures or which portion of such expenses is to be on the side of private actors, is to be decided via the democratic political debate, particularly in Brazil where private companies are already under substantial strain from tax collection offices at the federal, State and local levels.

In the UK, the NTD employed domestically is considered arguably successful but the figures used to support this argument (for example, the reduction of child pornographic content hosted in the UK to 1%) is related to reports sent to the IWF and thus a larger number of content hosted in the United Kingdom could go unnoticed.[899] In relation to the NTD scheme employed against websites hosted overseas, it is only partially effective because of the difficult international cooperation discussed in Chapter 2. In addition, the blocking scheme can be circumvented by a persistent viewer and both the NTD and blocking schemes addressed only the public open Internet (involving public websites and newsgroups).[900] Another problem with the NTD scheme was its limitations in taking down alleged illegal content hosted in overseas websites. Moore and Clayton reported that, even though taking down child pornographic content hosted domestically by the IWF took about 24 hours, the longevity of reported websites hosted abroad was far longer, because cross-national policing was usually slow and the foreign police often had more pressing priorities.[901] The IWF reported however that this situation has changed; there has been a significant reduction in the length of time these webpages stay ‘live’ in other countries after being reported.[902]

---

[899] See *e.g.* Bottomley, K. and Pease, K., *Crime and Punishment: interpreting data* (Buckingham: Open University Press, 1986) about the many ways that crime statistics are created and used.

[900] See Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69. See also Ozimek, J., 'Scorpions tale leaves IWF exposed: 'Look, that regulator isn't wearing any clothes'', *The Register,* 09 December 2008 at <http://www.theregister.co.uk/2008/12/09/iwf/>, accessed 20 June 2011.

[901] Moore, T. and Clayton, R., 'The Impact of Incentives on Notice and Take Down', (Cambridge: University of Cambridge, 2008) at <http://www.cl.cam.ac.uk/~rnc1/takedown.pdf>, accessed 05 July 2010.

[902] See page 3 of the IWF, 'Annual and Charity Report 2010', (Cambridge, UK: IWF, 2011) at <http://www.iwf.org.uk>, accessed 02 March 2012.

In all three jurisdictions, access to online child pornography remains unchallenged and the availability os such material is only partially targeted. Regulatory measures targeting national and overseas websites (for example, via NTD schemes or website blocking) advances the control over online content but it addresses only part of the child pornographic content available on the Internet. This is not only partially effective but may also lead to crime displacement: it pushes offenders towards more complex technologies such as anonymised P2P channels, hidden Internet, and highly secured networks, which are outside the reach of current regulatory measures undertaken by the hybrid public-private regulators addressed in this research; they are a matter of intensive police investigation.

This raises concerns about why to invest resources in policies that can only provide limited results instead of investing heavily in the harmonisation of laws and regulatory standards at the international level as well as preventing the commercial and non-commercial sexual exploitation of children in the 'offline' world. For Akdeniz, for example, institutions such as the IWF should tone down the emphasis on ineffective and costly initiatives and instead pursue international cooperation to remove foreign websites via an integrated and worldwide NTD scheme.[903]

4 Conclusions

This chapter employed the evaluative criteria against the case study material explored in Chapter 4 to produce an evaluative report on each jurisdiction. It also showed that each chosen jurisdiction has a different configuration to force the online intermediaries removing or blocking access to the reported child pornographic material. Nevertheless, although substantially different in regards to the way each models is designed and operated, they all involve a public-private configuration that aims to remove the material reported domestically and limit access to material hosted abroad. Such configuration, or functional equivalent, may involve a statutory regulator controlling the online intermediaries via legislation and CoCs set up by the Internet industry; the Public Prosecution Service, the Senate and a non-governmental Internet hotline forcing online intermediaries to comply with agreements; or an Internet industry regulator, closely connected with the police and government, that forces its own members to comply with self-regulation rules.

In Australia, there is a statutory regulator that controls the availability of child pornographic material on the Internet and operates under substantial legislation and regulations as well as CoCs formulated and implemented by the Australian Internet industry. It employs a NTD scheme domestically and it blocks child pornographic material via a voluntary scheme at the ISP-level in partnership with the Interpol. Such blocking scheme is expected to be based on legislation and wider in scope in the future, pending parliamentary approval.

---

[903] See Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008). See also Hogge, B., 'Lessons and questions for the IWF', at <http://www.openrightsgroup.org/blog/2008/lessons-and-questions-for-the-iwf>, accessed 07 June 2011.

In Brazil, the Federal Public Prosecutor Service, the Senate and the non-governmental Internet hotline, Safernet Brasil, were the key regulatory actors to force online intermediaries in Brazil to come into line in regards to regulatory policies for removing child pornographic material hosted domestically and disclosing information of alleged offenders. Such policies are partially based in legislation (for example, the NTD scheme only in relation to child pornography) but mostly grounded on agreements negotiated with relevant members of the Internet industry. So far, there has not been any scheme for blocking material hosted overseas.

In the United Kingdom, the private regulator IWF is the key interface with the British Internet industry. The system is grounded on a self-regulatory approach whereby online intermediaries created, financed, and agreed to comply with the Internet industry regulator's decisions in regards to policies against online child pornography. It employs a NTD scheme domestically and an ISP-voluntary scheme to block access to overseas URLs that includes around 100% of ISPs in the UK.

All three models presented problems of their own and were subject to similar criticisms when assessed by the evaluative criteria developed in Chapter 2. First, despite the different configurations and regulatory measures employed, all models presented problems in relation to private censorship whether there was a statutory or a private regulator, particularly where a blocking system was in place. In Brazil, although blocking of websites was not employed, private censorship was also an issue because online intermediaries were developing measures of their own as a response to the pressure put by the Federal Public Prosecution Service.

Second, in all three jurisdictions, privacy protection was an issue because of the increased investigatory powers given to law enforcement authorities and lack of robust safeguards to protect users from wrongful accusations and abuses. Nevertheless, further research is needed to advance these claims further and also to assess the deterrent effect that such increased powers have on those who access child pornographic material on the Internet.

Third, a lack of transparency, accountability, legitimacy, proper oversight, and citizen involvement were issues in all three jurisdictions. The three models were also successful to remove reported websites hosted domestically, but these policies are only partially effective because child pornographic material can be accessed and exchanged via other platforms and anonymised channels, and hosted overseas where enforcement is problematic.

Generally, the evaluative criteria served the purpose of assessing the three regulatory models for free speech and privacy protection as well as in regards to the principles of good regulation such as transparency, accountability and legitimacy. Nevertheless, some improvements can be made to the original evaluative criteria developed in Chapter 2. These items are: (1) how the regulatory measures are funded; (2) how each jurisdiction assess the success of regulatory policies employed. Another important addition to the criteria is to include both the domestic and international dimensions of each criteria in order to assess the regulatory policies and liaisons

implemented at the international level, which is crucially important for regulating content on the Internet.

It is also worth noting the importance of choosing a jurisdiction like Australia that relies on a statutory regulatory framework and a statutory regulator to control online content to show that employing such model is no guarantee that accountability, transparency and legitimacy criteria are meeting proper regulatory standards, for example that free speech and privacy are protected, and the principles of good regulation are in place.

In fact, the problematic public-private configurations applied to online content regulation presented problems in all the three jurisdictions in relation to the evaluative criteria, irrespective of the fact that there is more or less state influence. This seems to contradict the assumption that more state regulation minimises the violations of free speech and privacy protection commonly associated with private regulators. Yet, the claim for more 'publicness' of the IWF for example seems legitimate, particularly, because of current lack of closer judicial oversight and need of more public scrutiny.

Indeed, the way forward for these public-private configurations is towards a greater degree of 'publicness' but with flexibility and stronger involvement of the Internet industry via an escalation of sanctions if codes of conduct are violated. This involves the creation and implementation of a scheme of safeguards that clearly states the minimum standards that regulatory actors should meet both domestically and internationally. These safeguards should also be established via legislation in line with international standards.[904]

The next chapter is the conclusion of this research. It draws on findings from this evaluative report and links them with the theories of regulation, governance and criminology addressed in Chapter 2.

[904] There is also the question of whether such improved regulatory model can be replicated in other jurisdictions.

CHAPTER 6: CONCLUSION

This research employed the evaluative criteria developed in Chapter 2 against the anti-child pornography laws and regulations in place in Australia, Brazil and the United Kingdom to assess the implications of hybrid regulation for free speech, privacy protection and democracy in the online environment. This provided an opportunity to explore different features of public-private regulatory configurations found in these jurisdictions, and also to address a number of issues raised in the literature review chapter.

This conclusion chapter explores the findings from Chapter 5 and links them back to what was discussed in Chapter 2, showing what regulatory and governance theorists as well as criminologists may learn from this research.

1 Regulatory models, the role of the state and functional equivalents

Chapter 2 divided the regulatory strategies applied to online content into three different models taking into account the main regulatory actors involved. They were: (1) state and multi-state regulation; (2) self-regulation; and (3) hybrid regulation. Generally, state and multi-state regulation are centred in the notion of the state imposing standards backed by the threat of criminal sanctions domestically and internationally, respectively; self-regulation involves the development and enforcing of rules by a group of private actors; and hybrid regulation is a mixed approach that involves both state and private actors acting as regulators.

Although these three 'pure' regulatory models were useful to understand and compare the ways access to child pornographic material is regulated on the Internet, the existing models explored in the three jurisdictions were much more complex than these categories. Despite the fact that the state played a central role within the regulatory dynamics, the regulatory mechanics, the relevance of public and private regulatory actors, and the instruments to address the problem varied in each jurisdiction. The public-private configurations regulating access to online child pornographic material in Australia, Brazil and the United Kingdom showed different levels of state influence and participation of the private actors from the Internet industry. This is in line with the literature which states that decentred and polycentric regulatory regimes reject a clear distinction between the public and the private, because these actors are combined in a number of different ways; and that not only the knowledge is fragmented in the regulatory arena but also the exercise of power and control.[905]

In all three jurisdictions, the state played a significant role, and sometimes regulated directly. This may be a result of the criminal nature of the regulatory target, which demanded action in less flexible forms. The state still enjoyed substantial powers enforced via institutions and

[905] Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46; and Black, J., 'Critical reflections on regulation', *Australian Journal of Legal Philosophy,* 27 (2002), 1-35.

instruments designed to address the problem domestically. Nevertheless, there was also fragmentation in the regulatory environment and the distinctions between state and private regulatory actors were blurred to some extent. For example, private actors also regulated domestically: online intermediaries performed unchecked private censorship and disclosed information about users in non-transparent ways, Internet hotlines were set up to assess the potential illegality of material available online, private international organisations such as the INHOPE cooperated cross-nationally.

Understanding and exploring the anti-online child pornography regulatory environment in terms of a decentred and polycentric model strengthened the analysis and exposed the array of complex interrelationships established amongst different relevant actors, be they state regulatory bodies and law enforcement authorities, online intermediaries and manufacturers of software and hardware, Internet users and hotlines, vigilante groups, legislators or free speech advocates. The evidence collected showed that, to some extent, the regulatory actors behaved independently, and that regulatory intervention altered the behaviour of actors, changed the configuration of the system, and produced unintended consequences.

Such understanding of the regulatory problem is often found in the literature about online content regulation. For example, Murray proposes a three-dimensional dynamic regulatory matrix to represent the regulatory landscape and intervention taking into account different examples, including the ICANN, the development of the video cassette recorder (VCR) standard, and the copyrights infringements via filesharing.[906] His representation of regulatory intervention considers that actors behave independently, that the behaviour of one actor can influence the action of others, and that it is difficult to predict the result of such actions: the regulatory environment is plastic, complex, and resilient in such a manner that it mimics the functioning of the living organisms. These assumptions are also used elsewhere to suggest that regulatory actors' normative understanding of cyberspace (for example communitarianism and spontaneous ordering) and the dynamic resilience of the Internet should be part of lawmaking and policymaking processes in order to increase the regulatory effectiveness and the respect for regulatory authority in cyberspace.[907] Reed also employs these assumptions in order to analyse how laws and regulations can work for those willing to 'act lawfully',[908] for example copyrights protection, resolution of domain names' disputes, and establishment of technical standards.

Although these discussions advance knowledge about online content regulation, there is one important question to ask: is this way of understanding the regulatory phenomenon applicable to online content of a more violent nature such as child pornography?

---

[906] Murray, A., *The regulation of cyberspace: control in the online environment* (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006), p 234-51. See also Murray, A., 'Symbiotic Regulation', *The John Marshall Journal of Computer & Information Law,* XXVI(2) (2008), 208-28.

[907] See *e.g.* Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012), p 219; Guadamuz, A., *Networks, Complexity and Internet Regulation: Scale-Free Law* (Cheltenham, UK: Edward Elgar, 2011); and also Post, D., *In search of Jefferson's moose: notes on the state of cyberspace* (Oxford: OUP, 2009).

[908] Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012), p 1.

In regards to child pornography, the relevant Internet users (involving producers, distributors and viewers of online child pornography) are unwilling to act lawfully; they are the alleged offenders using the resilient and dynamic nature of the regulatory environment to produce, distribute and access child pornographic material. It is improbable that a desired regulatory settlement would follow organically from within the extant regulatory environment: Chapter 2 showed that the state was needed to bring institutions and individuals into line forcefully. Again, although there are many actors within the regulatory landscape, the state remains a prominent regulatory actor domestically in relation to anti-online child pornography regulation, whether making or enforcing the laws.

Understanding the problem of online child pornography regulation in terms of network complexity theories helps visualising the extent of the regulatory problem and the many nodes that affect the regulatory target, particularly at the international level, but at the moment, the everyday regulatory practice takes a more pragmatic approach that focuses on the most relevant regulatory nodes such as state regulators and online intermediaries. It is yet to be seen how such sophisticated theory can be employed by regulators in practice.

This is where the model proposed by Hood and Margetts is helpful, because the state is at central stage using its detectors and effectors as well as its nodality, authority, treasure and organisation.[909] As such, one potential application of Murray's three-dimensional hybrid matrix might be to consider each node (or actor) subject to state regulation. As such, policymakers would consider the organic (or symbiotic) nature of the regulatory environment, represent the relationships and tensions already in place, and harness the regulatory matrix instead of relying on blunt command-and-control measures, in addition to identifying ways by which the state could achieve its regulatory aims using detectors and effectors.

It is important therefore that policymakers are aware of the relevant actors involved and their interrelationships when designing regulatory intervention mechanisms. Perhaps, future research on the subject should develop strategic computational models that take into account such interrelationships that change the configuration of the regulatory environment and produce probable scenarios to guide intervention. For example, the implications (expected 'success', unintended consequences and costs) of a particular regulatory intervention that aims to block access to child pornographic material in Brazil can be analysed in advance against different scenarios and improved before it is applied in practice. Again, the configuration and relevance of such interactions are context dependent and vary according to the jurisdiction where they occur.

It is also worth noting that although the problems these three jurisdictions face are similar, and that the regulators involved are aware of advances made in other jurisdictions, the choices over

---

[909] Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007).

the regulatory strategy used were a result not only of the local social environment[910] but also of 'irrational policymaking, faith and politics'.[911] In Brazil for example there was no blocking scheme and a lack of participation from the Internet industry. In Australia, not only child pornography was targeted but also adult pornography available online, and there was a statutory regulator. In the United Kingdom, there was a blocking scheme in place and also an Internet industry regulator. In short, these public-private regulatory arrangements addressing the regulation of access to child pornographic material on the Internet varied in each jurisdiction depending on a number of factors related to the local regulatory culture: they are local regulatory solutions to a multi-jurisdictional problem.[912]

This raises the question of whether it is more adequate to employ a taxonomy not based on 'pure' regulatory models, but on the function that these regulatory arrangements play in order to compare regulatory arrangements employed in different jurisdictions.[913] In other words, it is perhaps more useful to compare these jurisdictions not in terms of the main regulatory actors involved (because regulatory responsibilities are shared in different levels depending on the jurisdiction studied), but in terms of their 'functional equivalents'[914] (a common ground for comparison): the function that the regulatory arrangements plays - in this case, limiting access to online child pornography. In this case, the research question is no longer 'who is the central regulatory actor in this jurisdiction?', but becomes 'how is the public-private arrangement limiting access to child pornography on the Internet in this jurisdiction?'. The comparative process would be based not on the relevant regulatory actor, but in terms of the regulatory functionalities.

2 Problematic international interfaces of local regulatory arrangements

Another layer of complexity of online child pornography regulation is the multi-jurisdictional nature of the Internet. In an ideal world for regulators, the international environment should be a domestic jurisdiction, and every digital transaction performed by users would be monitored and the contents of a communication known. As such, it would be possible to pass unified and standard criminal laws to punish people worldwide who produce, distribute or access child pornography; to increase criminal liability of online intermediaries uniformly; have law enforcement bodies with enforcement authority over the entire environment; have architecture-

---

[910] Braithwaite, J. and Ayres, I., *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: OUP, 1992), p 101.

[911] Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007), p 13.

[912] The discussion about the relative success of these policies obtained domestically and the failure of international interfaces is discussed in Section 2 below.

[913] It is worth noting however that such taxonomy based on main regulatory actors involved helped selecting, classifying and comparing the regulatory intervention of each jurisdiction.

[914] For Nelken, this concept of 'conceptual equivalents' can also be misleading because it neglects the role of non-legal institutions, alternatives to law and other groups within civil society such as the family. Nevertheless, the influence of such groupings are taken onboard the concept in relation to online child pornography regulation. See Nelken, D., 'Comparing Criminal Justice', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (3rd edn.; Oxford: OUP, 2007), 139-57, p 153.

based regulatory technology capable of monitoring all data transferred via the digital networks. Many of the regulatory obstacles that need international agreements, protocols and standards would disappear. Nevertheless, this is not the case. The anti-child pornography laws and regulations vary, the authority of law enforcement institutions are only within the domestic territory, online intermediaries operate both nationally and internationally under varying rules; the regulatory environment is complex, dynamic and international.

For example, despite arguably successful regulatory action targeting websites hosted domestically, other measures such as website blocking have also been employed to limit access to overseas websites. This requires the cooperation and action of other regulatory actors and increases the complexity of regulatory inter-relationships, which has to extend beyond national boundaries. State regulators have to interact more closely with overseas online intermediaries, international agencies, delegate more regulatory powers to private actors, and increase powers of law enforcement authorities.

Generally, the local regulatory arrangements involving public and private regulatory actors in place in all three jurisdictions were arguably successful at limiting the availability of online child pornographic material domestically. Nevertheless, the international interfaces of these arrangements need improvements (meaning the mechanisms of communication for these local regulatory arrangements to interact at the international level). These interfaces involve not only the establishment of legal consensus via international treaties, but require international standards and protocols established by the states and private actors involved, because the exercise of regulatory power is fragmented at both the domestic and international levels. This shows that the multi-jurisdictional challenge of the Internet is not only legal but regulatory.

There is scope for these protocols and standards to advance at the international level *vis-à-vis* the inability of international treaties to obtain worldwide consensus on regulatory policies addressing the availability of online child pornography. Whilst international law may establish general terms for action, international protocols and standards can be established in a more flexible and creative way between countries or amongst a group of countries independently.

In the light of this, international law can be established generally where a rough consensus can be obtained at the international fora, but the detailed operational protocols and standards can be implemented bilaterally by these public-private arrangements tackling online child pornography domestically (for example, the key regulatory actors such as online intermediaries and the statutory or Internet industry regulator). In addition, these varying regulatory arrangements may operate domestically according to a self-enforced regulatory approach[915] subject to escalation of state sanctions if private actors violate the Internet industry codes of conduct.

---

[915] See *e.g.* Braithwaite, J. and Ayres, I., *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: OUP, 1992).

At the international level, these public-private arrangements can be considered as regulatory nodes (operating in a particular jurisdiction) within an international network and with the ability to communicate with other nodes via protocols and standards (international interfaces) established in advance by the nodes involved. Such model of international interaction resembles the operation of the Internet to some extent because: (1) domestic regulatory nodes communicate via international interfaces independently of a central international regulator; (2) standards and protocols (international interfaces) may undergo permanent improvements by the domestic nodes involved until there is a consensual and optimum standard for these domestic nodes to communicate with each other; (3) once one optimum international interface become preferred, it will motivate other domestic nodes to take part and adhere to the network.

3 Evaluative criteria for anti-child pornography regulatory policies

The academic literature discussed in Chapter 2 provided the building blocks on which to develop evaluative criteria to assess the regulatory measures in place in Australia, Brazil and the United Kingdom. Such evaluative criteria have three broad categories: (1) free speech; (2) privacy protection; and (3) general principles of good regulation and democratic values. The criteria were made as flexible as possible to reflect the different priorities and agendas, cultural regulatory contexts and cultures, and more importantly, to incorporate fieldwork issues not previously found in the academic literature. The literature provided most of the issues covered in the case study material, but other issues such as the lack of citizen involvement in policymaking, the economics of regulation, and cross-national differences in terms of the importance given to certain criteria within the three categories were obtained from the empirical evidence collected.

The existence of blocking schemes raised the most pressing concerns about free speech. In Australia, although there was a statutory regulatory body in place, not only state censorship but also private censorship was an issue. This was largely because there were filtering schemes in place via state regulation (involving legislation creating the user-level voluntary regime) and self-regulation (involving the implementation of ISP-level voluntary regimes). As such, censorship powers were given to private online intermediaries in addition to state controlled regulation of child pornographic content. Free speech concerns were also an issue in the UK where there was a voluntary ISP-level blocking scheme managed by the IWF. In Brazil, there was not any blocking scheme in place legislated or otherwise to limit access to child pornographic content hosted overseas and thus the issue of free speech protection had little relevance. Moreover, Brazilian free speech advocates were less active when the issue at stake was child pornography regulation.

The legitimacy of regulatory measures was a concern in Australia. Although the Australian regulatory scheme was designed via legislation, there was little evidence to suggest that Australian citizens participated actively in the policymaking process. A voluntary filtering

scheme at the ISP-level to block access to online child pornography was implemented via self-regulation before legislation in this regard was discussed in the Commonwealth Parliament. Regulation via agreements between law enforcement authorities and online intermediaries set the stage in Brazil and this also led to concerns over their legitimacy. It may be true that these agreements: (1) were arguably in accordance with the current legal constitutional environment; and (2) were derived from partnerships amongst law enforcement authorities, both houses of the Parliament, a non-governmental organisation, and major online intermediaries. Nevertheless, these regulations were not enacted via the democratic channels of the Parliament as would have been the case with legislation. There were no representatives from the judiciary; and consumer rights, civil liberties, and children rights' activists were largely absent during the discussions that led to these agreements being negotiated. In the United Kingdom, IWF's legitimacy as an Internet industry self-regulatory body was also subject to criticism. The lack of citizen involvement in anti-child pornography policymaking was not strongly addressed by the academic literature but highlighted in the documentary evidence.

This was the case in Australia where legislation created a regulatory environment that encouraged, and even supported financially, the use of content filtering software by Australian users, whereas the recent developments over the voluntary ISP-level regime dependent on the Interpol blocklist may be a disincentive to local industry, because it is developed by an international organisation, the Interpol, and it excludes therefore Australian filtering companies.

Another area worth exploring is the economics of regulation around the problem of online child pornography. Different regulatory tools will predominate in different settings also because of a cost-benefit factor.

> First, different instruments are likely to generate different kinds of administrative (transaction) costs associated with their use. Monitoring and enforcement costs will be entailed for the government; compliance costs, for the private sector. Second, different instruments, in attaining a specified objective, are likely to generate different incentive structures for affected parties, which in turn will have different effects on the amount of social resources expended in attaining the objective.[916]

In Brazil, the economic interest of online intermediaries to avoid the costs associated with regulation drove regulation and influenced the nature of the agreements negotiated. In Brazil, private online intermediaries and relevant telecommunications economic groups influenced substantially the regulatory measures put in place via agreements so as to avoid bearing the costs to implement the proposed regulatory measures. There was a consorted action by powerful economic groups to influence the agreements on their benefit and to support a 'hands-off government' legislative approach. Often this was pushed forward under a free speech and privacy protection discourse which were arguably more morally acceptable and appealing. These issues were not clearly manifested in the Australian and the UK case study material.

---

[916] Trebilcock, M., et al., 'The Choice of Governing Instrument', (Ottawa: Canadian Government Pub. Centre, 1982) at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997355>, accessed 12 July 2012, p 27.

In Australia, most of the regulatory cost is under ACMA's governmental budget. Nevertheless, major ISPs, the IIA, the AFP and Interpol developed a voluntary model and it seems the resulting costs are under the Australian Internet industry. In Brazil, there was permanent opposition from online intermediaries to avoid the costs of regulation. They were lobbying for legislation that establishes the use of public money from a technology related Trust to implement such measures. In the United Kingdom, the IWF's operation was largely funded by the Internet industry, and it was not clear how the costs of regulatory mechanisms in place designed to identify alleged offenders and disclose information to law enforcement authorities are funded.

Generally, different regulatory instruments are likely to have direct and indirect costs of creation, implementation and operation. The direct costs may be related to personnel and equipment to enforce the rules established via legislation and regulations, for example software, hardware, and institutional operation. There indirect costs may be related to the time used during the political and parliamentary discussions, and the potential inhibition of creativity and digital economy developments.

Another issue concerns the apparent separation between 'online' and 'offline' sexual exploitation of children. Reed distinguishes between 'offline' and 'online' child pornography to emphasise the scale and difficulties associated with regulating content in the online environment.[917] Nevertheless, although each has regulatory challenges of their own, these problems are interconnected: the 'offline' and 'online' problems should be tackled together by policymakers. For example, although 'online' child pornography arguably seems to be larger in scale and demand than 'offline' physical sexual abuse committed against children and the production of related material, the 'online' problem needs the intensive 'offline' traditional policing enforced domestically as well as the cooperation amongst international police forces to be tackled properly. It seems counter-productive to spend the limited governmental resources only tackling the 'offline' commercial sexual exploitation of children and neglect the other forms of sexual violence committed against children on, or related to, the Internet. Similarly, it seems unwise to spend all resources available to tackle the overwhelming range of threats posed to children in the online environment, and neglect the existing 'offline' physical abuse of children. In any case, more research is needed in this area to uncover the economic agendas moving the regulation of access to online child pornography forward, to identify who financially benefit from the regulatory choices made, and to unveil the actual costs involved to implement such measures.[918]

---

[917] Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012), p 55-7.

[918] The networked information economy is recurrent theme of the work of Lessig and Benkler but with focus on peer production, commodification of ideas, and the concept of creative commons, not the economics of regulation around the control of online child pornography on the Internet. See Lessig, L., *Free Culture: The Nature and Future of Creativity* (New York: Penguin Books, 2004) and also Benkler, Y., *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (London: Yale University Press, 2006).

The partial effectiveness of regulatory policies and the problem of crime displacement were a concern in all jurisdictions, particularly because the content policies in place addressed only web-based applications and platforms, whereas child pornographic content was exchanged and accessed via more resilient online channels. This makes evident the multi-jurisdictional challenge that the Internet poses to content regulation and the need of regulatory policymaking to advance in this regard.[919] Indeed, efficiency of regulatory intervention is another issue worth exploring, particularly the question of whether it is efficient to spend these different resources on regulation that is only partially effective. Although some of these policies, for example website blocking, may be effective to protect people from inadvertent access to child pornographic content, they are less effective to limit access generally and have a number of unintended consequences such as potential violation of civil liberties and crime displacement. They may also be distracting attention from more relevant issues, for example increased international cooperation, children welfare, and awareness programmes.[920]

Nevertheless, such 'programmed inefficiency'[921] of regulatory instruments may be a necessary concession for the democratic political process, human rights protection, interest groups' demands and other non-strictly market driven rationales. In the area of online child pornography, the regulatory problem cannot be tackled solely from a narrow cost-benefit approach: there should be a broader understanding of the costs involved that goes beyond the limits of a narrow economicist approach.[922] This understanding is crucial to approach important questions such as: what is the optimal degree of efficiency to limit access to online child pornography? How many resources should governments and private actors spend on such problem? What is the optimal level of enforcement? How much child pornography should be left unregulated? Why not to use these scarce resources entirely in preventing 'offline' commercial sexual exploitation of children? These are key questions left to the implementation phase which are commonly outside the political debate around lawmaking and should be taken onboard whenever the 'success' or failure of anti-child pornography regulations are assessed.

Judging success of regulatory intervention in relation to anti-online child pornography regulation is a controversial area, particularly, because it is difficult to assess the impact of such regulatory measures to online child pornography industry as a whole. Generally, to assess the success of a regulatory policy it is necessary to identify its aims in advance. Whether it is to limit access to, to minimise the chance of inadvertent access to, or to have a deterrent effect on potential viewers of child pornographic websites; these are indicators to measure its success. There are however other indicators of success or failure. For example, whether the regulatory measure is able to achieve a balance between increased surveillance powers given to state

---

[919] See Section 8 below.

[920] See Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008).

[921] In the sense that a number of checks and balances have to be implemented, and compromises have to be made to protect civil liberties and accommodate demands from a wide range of interest groups.

[922] See *e.g.* Becker, G., 'Crime and Punishment: An Economic Approach', in George Stigler (ed.), *Chicago Studies in Political Economy* (London: The University of Chicago Press, 1988), 537-92.

regulators and safeguarding civil liberties, or whether employing automated architecture-based regulatory technologies avoids restricting the creative and lawful use of the Internet.

Successful regulatory measures to limit access to child pornographic material available on the Internet are not only those which fulfil primary regulatory aims. For the regulatory policy to be successful it should also identify the potential negative implications and have safeguards to minimise the threats posed to free speech, privacy protection and democracy online. This is relatively easy to state in theory, but finding an effective and efficient optimal policy mix in practice is not so straightforward, because the possible combinations are context dependent, may be counterproductive or incompatible.[923]

In short, the success of an anti-online child pornography regulatory intervention can be assessed not only by the extent to which it fulfils its aims and objectives, but if it limits the potential for free speech and privacy violations and employs a scheme of safeguards that works in practice: it should articulate efficiently, effectively and fairly the practicalities of protecting both children and civil liberties in the online environment.

Interestingly, the more states enacted anti-child pornography criminal laws over the years to cope with the perceived threats posed to children on the Internet, the more opportunities for crime commission, enforcement problems, and regulatory failure are created (creating ineffective laws that undermines the individuals' belief on the authority of the state). It seems that the regulatory enterprise is not only creating more problems than solutions, but also making it difficult to achieve regulatory success.

Against this background, how should success be measured when the Internet and the wide range of anti-online child pornography laws produced numerous venues of regulatory action? Should the police use all their resources to investigate everything that is reported, or focus on the most exemplary cases? Should the police and other regulators use a managerial or a moral approach? These questions remain open, but this thesis exposed the conflict between a zero-tolerance moral approach of both political and media discourses, and the managerial stance of law enforcement authorities amongst other regulators.

The role of the regulatory culture cannot be overlooked in relation to a cross-national evaluative criteria. For example, the wider scope of the Australian online censorship regime which included in the regulatory remit not only criminal material such as child pornography but legal adult pornography, made evident the importance that protection of children from online material considered inappropriate had for agenda setting in that jurisdiction. Of course this was also a

---

[923] Gunningham, N. and Grabosky, P., *Smart Regulations: Designing Environmental Policy* (Oxford: OUP, 1998), p 423.

concern in both Brazil and the UK, but in these countries it has been generally left to parents and the Internet industry to resolve things on their own via self-regulation.[924]

For Hood and Margetts, regulatory '[…] applications and effects vary with culture'.[925] And this is a similar point made by Reed who argues that '[…] different societies have different views on such fundamental values as privacy and free speech'.[926] Indeed, the importance given to each category within the evaluative model varied across the jurisdictions and therefore it has to take the cultural variations into account if it is to be employed cross-nationally. The grand-concepts of free speech, privacy protection and democratic values may mean different things in different contexts. For example, the acceptability of more surveillance powers given to law enforcement authorities could be stronger on jurisdictions already subject to terrorist attacks; some jurisdictions could be more sensitive to free speech restrictions than others; and some bureaucracies could be more prepared than others to safeguard and promote democratic values. The success of a regulatory measure could be strongly influenced by the transparency and protection of free speech in some jurisdictions, whereas legitimacy and efficiency could be more relevant in others.

The importance given to particular issues was a result of different agendas and interests driving the regulatory actors. Whenever there were well-established civil rights and anti-censorship groups, the protection of free speech and privacy of individuals were emphasised in the agenda and discussions. These groups were only recently active in Brazil and they mainly focused on the debate around the *Marco Civil* and Cybercrime legislative proposals, not anti-child pornography regulation. The anti-censorship and protection of online privacy discourses were only used by the Brazilian online intermediaries to avoid the burden of regulation.

In Australia and the UK, for example, the protection of free speech in relation to anti-child pornography measures was emphasised not only in the relevant academic literature but the empirical evidence, such as policy documents, campaigning groups and the general public. This may be a result of the blocking mechanisms being employed voluntarily at the ISP-level. The free speech concerns were less evident in the Brazilian case study, partially because of little academic literature available, and because of no blocking mechanism in place. The absence of a content blocking scheme might had been a result of telcos' opposition in relation to the operational costs involved but also a result of a national aversion against censorship policies

---

[924] There were developments from the UK government to force ISPs to employ an 'opt in' policy in relation to access to adult pornography available on the Internet. This meant that UK ISPs may block access to adult material websites as a default option for customers. See Halliday, J., 'Pornography online: David Cameron to consider 'opt in' plan', *The Guardian,* 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/may/04/pornography-online-cameron-opt-in-plan?newsfeed=true>, accessed 05 May 2012.

[925] Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007), p 192.

[926] Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012), p 243.

usually associated with the authoritarian military government that ruled the country from March 1964 to March 1985.[927]

Overall, the evaluative criteria developed in Chapter 2 proved to be a robust tool for an impact assessment mechanism to evaluate the anti-online child pornography regulations, and also to explore the problematic relationships between state and private regulatory actors. It showed that hybrid regulation of online child pornographic material was problematic in all three jurisdictions irrespective of the regulatory mechanics employed. Nevertheless, improvements can be made.

Evaluative criteria to assess and compare internationally the impact of anti-child pornography regulatory interventions for free speech, privacy protection and good regulation involves therefore: (1) free speech - involving issues of unchecked private censorship, scope creep, lack of focus and excessive use of architecture-based regulatory tools; (2) privacy protection - involving issues of increased unchecked and more invasive surveillance powers given to law enforcement authorities; and (3) general democratic values and good regulation - involving issues around the lack of transparency, accountability, legitimacy, proper oversight, and citizen involvement as well as inefficiency and ineffectiveness of regulatory intervention which includes difficulties in evaluating hybrid regulation, crime displacement, unchecked regulatory powers and insufficient safeguards. In addition to this, the economics around the regulation of online child pornography (for example, the sharing of costs to implement the regulatory measures), how each jurisdiction evaluates the success of the regulatory polices employed, the constitutional framework and mechanics of the international interfaces associated with the regulatory arrangements, and the cross-national differences in terms of the importance given to each criteria are issues that should be aggregated to the cross-national criteria for future comparisons.

4 The adjudication of apparent illegality of online content by private actors

The adjudication of apparent illegality of material available online by private actors was relevant to all case studies, and it is an issue that deserves special attention. This theme raises the question of whether the perception of illegality, the determination of potential illegality, or even the determination of illegality are inherently judicial responsibility, or whether it can also be performed by private actors.

These concerns were minimised in Australia, because of the statutory nature of ACMA, but even in that jurisdiction, there was a voluntary ISP-level blocking scheme in place that used Interpol's blocklist; the judgment about the potential illegality was transferred to an international institution. In Brazil, any institution or individual could report any suspected

[927] For an overview about the Brazilian military dictatorship, see Gaspari, E., *A Ditadura Envergonhada* (vol. 1; São Paulo-SP: Companhia da Letras, 2002); Gaspari, E., *A Ditadura Escancarada* (vol. 2; São Paulo-SP: Companhia da Letras, 2002); Gaspari, E., *A Ditadura Derrotada* (vol. 3; São Paulo-SP: Companhia da Letras, 2003); Gaspari, E., *A Ditadura Encurralada* (vol. 4; São Paulo-SP: Companhia da Letras, 2004).

criminal activity to a law enforcement authority, which is required by law to act. Nevertheless, a few institutions such as Safernet Brasil performed most of the reporting activities, and this relieved the courts and law enforcement authorities from most of the burden of assessing the potential illegality of the reported material. The proposed 2010 *Marco Civil* Bill made any online content removal of a reported material by online intermediaries dependent on a judicial order, but this has been criticised as excessive dependence on judicial orders[928] and it is likely to be withdrawn during parliamentary discussions. In the United Kingdom, the problem of assessing the potential illegality of online material was highlighted in the aftermath of the Wikipedia incident discussed in the UK case study material. Although the 'incorrect' judgement of IWF's staff was not exempt from future judicial redress, there were no incentives for free speech activists or UK online intermediaries to challenge IWF's decisions in courts in relation to alleged child pornographic content being blocked.

Such adjudication processes are not limited to cyberspace. Indeed, they are performed by different social actors, on a daily basis, in a number of different areas. For example, members of the public often notify the relevant authority if they suspect that a criminal act was committed; police agents use their discretion to decide whether to investigate or not, based on their own judgment about the evidence presented; and prosecutors take the decision to pursue a criminal prosecution if they believe this serves the public interest. Moreover, in all these events the judicial authority may still decide whether the reported 'crime' has not been committed after all. Generally, a limited judicial oversight could manage these situations reasonably well.

Nevertheless, the online environment has a number of features that render these traditional adjudication processes problematic. Controversial material and reporting mechanisms are easily available to a larger public and therefore an immense volume of alleged criminal material can be reported to law enforcement authorities. Unfair accusations can be made anonymously and in great numbers, authorities are unable to assess the immense volume of reports received, online intermediaries undertake unchecked private censorship, perfectly legal material may be taken down and such decisions stay unchallenged, wrongful accusations can have a devastating effect on an individual's reputation before any judicial remedy is put in place (for example, when defamatory information is made available online), and courts are unable to undertake proper judicial oversight *vis-à-vis* the great volume of requests in relation to controversial online material.

The traditional judicial oversight is unable to cope with such demand, but on the other hand, the excessive judicialisation of online content regulation is also undesirable. Indeed, if on the one hand, regulators need to address the material available online that may put individual's life at risk or facilitate sexual abuse committed against children without delays, on the other hand,

---

[928] See Thompson, M., 'Problemas Fundamentais do Marco - Marcelo Thompson @ Cultura Digital', (Brasília-DF, Brasil, 2010) at <http://culturadigital.br/marcelothompson/>, accessed 13 March 2012; and also Carr, J., 'Getting it wrong', *Desiderata* (2012) at <http://johnc1912.wordpress.com/2012/07/15/getting-it-wrong/> Accessed 16 July 2012.

proper judicial oversight is also needed to prevent illegal taking down of material and unchecked private censorship. The challenge here is to find a balance between an excessive dependence on courts' decisions and a total absence of judicial oversight around the operation of private actors controlling online content.

The great volume of potentially controversial material available on the Internet and the operational cost of monitoring all this material in different platforms and applications would largely extrapolate the capacity of the judicial system. The courts are arguably not needed in all situations; its operation is costly and demands time. As such, automated regulatory technologies employed by non-judicial actors are welcome if used judiciously. Such use is expected to rise because of the more sophisticated technologies available for content regulation.

The problem is perhaps that the digital communication technologies enabled private actors to employ these processes (in relation to the perception and determination of illegality) in an automated manner, in larger scale, and therefore with wider implications. Again, these tools are becoming more precise because of the developments computational semantic analysis and artificial intelligence that inform automated content analysis systems. Although the fast assessment of apparent illegality of content is welcome to cope with the regulatory demands, minimum judicial standards and safeguards should be in place.

5 Increasing publicness of hybrid arrangements and the need of legislative safeguards

Chapter 5 shows that all regulatory models explored in the case study material are problematic in relation to the evaluative criteria irrespective of the level of state involvement. This is in line with the claim that accounts on the greater accountability, transparency and legitimacy of a state regulator may be exaggerated and it is no guarantee that free speech and privacy are protected nor are good regulation practices followed.[929]

The need to incorporate public values and safeguards around the operation of self-regulatory bodies were a constant concern in the case of both Internet hotlines: IWF in the UK, and Safernet in Brazil. These safeguards were to strengthen the judicial oversight, legislative scrutiny, citizen involvement, external audits and overall transparency. Given that these organisations were exercising arguably public functions, there should be mechanisms to increase their accountability to the public at large (a publicisation process to make them look more like a statutory body) and minimise the influence of private interests that might capture these institutions. Nevertheless, the existence of a statutory regulatory body is no automatic guarantee that concerns about transparency, accountability and legitimacy of regulation are addressed properly. For example, the ACMA blocklist could not be made public via FOI requests, was not independently audited, nor could the people responsible for creating it be

[929] Stenning, P., 'Powers and Accountability of Private Police', *European Journal on Criminal Policy and Research,* 8 (2000), 325-52.

named. In addition, the ACMA's reports about the blocklist's operation ceased to be made to the Commonwealth Parliament. Overall, in all three jurisdictions, increased regulation meant the need to establish safeguards to prevent potential abuses.

The need to increase publicness of public-private arrangements is discussed in Chapter 2 but one important question to ask in relation to online child pornography regulation is how such aim is to be implemented in practice. One way forward may be via legislated safeguards which establish general principles and permanent monitoring of such principles around the operation of the domestic public-private regulatory arrangements and their international interfaces.

Indeed, the assessment of the case studies identified a number of threats to free speech. One of them was the proliferation of unchecked private censorship. Both the use of legislation and the threat of legislation forced online intermediaries in the jurisdictions studied to adopt regulatory measures of their own, whether be they automated or via human-based analysis. This is expected to increase as architecture-based regulatory technologies get cheaper and more sophisticated, and with developments in terms of semantic analysis of image content. Furthermore, the availability of cheaper regulatory tools may minimise the financially motivated opposition of Brazilian intermediaries against the regulatory will of state regulators and pave the way for further unchecked regulation. The evidence from Australia and the UK suggested that the online intermediaries were more willing to automatically take down or block alleged child pornographic content reported by IWF or ACMA rather than considering these requests carefully, or challenging them in courts. Once the regulatory platform was up and running, it was more cost effective to automatically enforce the requests made and avoid the risk of criminal liability. Safeguards in this regard include the use of regular independent audits and reports to the Parliament, increased judicial review, detailed and comprehensive appeal and put back procedures, and checking regularly the architecture-based regulatory tools employed by the private actors.

Concerns about scope creep[930] found in the literature were also an issue in the case study material. In Australia, the voluntary ISP-level blocking scheme was reported to target child pornography only, but there were governmental plans to block access to the wide range of RC-rated content via legislation. In Brazil, although the agreements were settled following a moral crusade against online child pornography by politicians and the media, the regulatory system was used to target other criminal content, *e.g.* incitement to racial hatred and religious intolerance. In the United Kingdom, the IWF reported that the voluntary ISP-level blocking scheme limited access to overseas child pornographic URLs only. Nevertheless, recent developments, for example court orders to block access to copyright infringement via filesharing applications and the ISPs 'opt in' policy to access adult pornography showed that using the existing IWF blocking platform to block access to other material was possible to occur despite the alleged opposition from the UK Internet industry. Safeguards in this regard include

[930] Once the regulatory platform is in place, it can be used to censor other types of material available on the Internet.

restricting the use of more invasive regulatory measures only to criminal content of more violent nature, *e.g.* child pornography and terrorist-related, leaving copyright infringement via filesharing and adult pornography, for example, outside the scope of such measures.

The low level of citizen involvement in policymaking was highlighted in both the Australian and Brazilian case studies. In the United Kingdom, although the IWF drew its Board members of different sectors of society, it was unclear how civil society at large, including free speech and civil rights's groups, could influence IWF's operation. Safeguards in this regard include the participation of citizens in the policymaking process and encouragement of free-speech and civil rights' protection organised groups.

Although privacy implications of regulatory measures were only peripherally addressed in the case studies, regulatory developments in relation to disclosure of information about Internet users by online intermediaries to law enforcement authorities should be closely scrutinised and carefully discussed by society at large. This is particularly important at this stage of online regulatory development when more invasive surveillance powers and less privacy protection are considered the natural antidotes to the resilient nature of the Internet,[931] which represents a move from a 'fire-alarms' towards a 'police-patrol' regulatory approach.[932] Perhaps these measures are not the only answers, and they may be wasting valuable resources and displacing crime. Safeguards in this regard include more judicial oversight, punishment of abuses committed by state regulators, and compensation of victims of improper privacy violation.

Regulation of online content is increasing across the world, and the question is no longer whether the Internet should be regulated or not, but rather which type of regulation should be implemented and which safeguards ought to be put in place to deter abuses. [933] Accordingly, after the relevant threats posed by regulatory measures were identified and explained, safeguards can be designed and employed. The academic literature discussed in Chapter 2 (Section 4) suggests a number of safeguards to minimise the risk of free speech and privacy violations as well as to tackle the democratic deficit vis-à-vis the use of hybrid regulation. These include measures of extended accountability, enhanced democratic governance, stronger judicial and legislative oversight, more citizen involvement, and improved transparency. Designing safeguards in advance is needed to avoid the problems of the 'implementation game', meaning that the process of organising the administrative machine and making it work as intended.[934]

---

[931] See *e.g.* the US National Security Agency project and the UK governmental plans to increase surveillance over online activities. Bamford, J., 'The Black Box', *Wired Magazine*, April (2012) at <http://www.wired.com> accessed 03 April 2012. And also, Booth, R., 'Government plans increased email and social network surveillance', *The Guardian,* 01 April 2012, sec. World News at <http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance>, accessed 01 May 2012.

[932] See McCubbins, M. and Schwartz, T., 'Oversight Overlooked: Police Patrols versus Fire Alarms', *American Journal of Political Science,* 28(1) (1984), 165-79.

[933] For Walden, censorship is a feature of all states. See Walden, I., 'Porn, Pipes and the State: Censoring Internet Content', *The Barrister*, (2010) at <http://www.barristermagazine.com/archive-articles/issue-46/porn,-pipes-and-the-state:-censoring-internet-content.html> accessed 24 May 2012.

[934] See Bardach, E., *The Implementation Game: What Happens After a Bill Becomes a Law* (Cambridge, MA: MIT Press, 1977), p 250.

A permanent scheme of safeguards to minimise violations of free speech and privacy as well as to secure transparency, legitimacy and accountability should be preferable enforced via legislation, which considers the public function that regulatory actors (whether public or private) have as information gatekeepers, and include mechanisms that: (1) strengthen the citizen involvement (from relevant sectors of society) in formulating, management and monitoring of regulatory policies; (2) secure the transparency about all aspects of the regulatory model both in relation to its domestic and international interfaces; (3) provide sufficient channels for accountability, independent audits, reports to Parliament, detailed and comprehensive appeal and put-back procedures to avoid abuses and compensate victims of wrongful decisions; (4) deliver permanent and adequate judicial oversight; (5) assess the invasive level of regulatory policies in relation to privacy protection; and (6) assess the adequacy of architecture-based regulatory tools.

Generally, the general principles of such safeguards may be established via legislation whilst specific details around its actual implementation can be established via self-enforced mechanisms that includes escalation of sanctions by the state. Of course, these mechanisms may not be the same as they derive from political bargaining, regulatory and cultural agendas as well as financial interests that depends on a particular jurisdiction. As such, it is an open question whether such scheme can be replicated in other countries. It is also worth noting that such scheme of safeguards should be enforced not only against the main regulator but all actors involved in a regulatory environment where the policing powers are dispersed.[935] This adds another layer of complexity because it involves enforcing such safeguards at the international level.

6 Broad lessons of online child pornography regulation

The second part of Chapter 2 shows the existence of an international consensus about the criminal nature of and the need to tackle the child pornographic material available on the Internet. For example, there were numerous anti-child pornography laws, cross-national police operations and conferences, substantial visibility of the topic in the media, and a range of regulatory measures intended to target the production and distribution of, and the access to online child pornography both nationally and internationally. It also suggested that there were a number of regulatory rationales driving this regulatory expansion: (1) the exaggerated dimension of perceived harms; (2) the new venues where child abuse could be performed; and (3) institutional agendas geared by symbolic politics, moral entrepreneurs, media-made criminality, the prospects of financial gain and survival, and a legitimate interest in protecting children against sexual abuse.

Generally all these factors were present in all three jurisdictions, and they provided a basis on which to support and justify the expansion of anti-online child pornography laws and

[935] Loader, I., 'Plural Policing and Democratic Governance', *Social & Legal Studies,* 9(3) (2000), 323-45.

regulations domestically. Nevertheless, some of the reasons driving the regulatory expansion were emphasised more than others depending on the jurisdiction observed.

For example, in Australia the development of anti-online child pornography regulations was part of the movement to apply the current censorship scheme of Tv broadcasting to the online environment. There was a statutory Commonwealth censorship body operating the scheme that made the online intermediaries come into line with the regulations established. The established, and for some time supported, filtering scheme provided commercial opportunities for software and hardware manufacturers. Moreover, the Commonwealth government's intention to create a mandatory website blocking scheme at the ISP-level faced parliamentary opposition, but was employed voluntarily by major Australian ISPs.

In Brazil, the role of moral entrepreneurs was evident. Some political figures and institutions, such as the MPF-SP and Safernet Brasil jointly conducted a moral crusade against the problem with interests of their own, whether to increase political capital, centralise investigatory powers or secure financial survival. The focus on a big player (for example, the SNS Orkut owned by Google Inc.) to drive media attention, a self-regulation discourse that was never implemented in practice by the online intermediaries, and sensationalist media portrayal of the problem were also reasons to push these regulations forward. The Brazilian regulators made online intermediaries come into line under threat of criminal liability.

In the UK, the media demonisation of some Internet entrepreneurs who opposed the state call for removal of alleged child pornographic content hosted in newsgroups in 1996, and an environment prone to self-regulatory practices provided the conditions for the creation of IWF. The government forced the UK Internet industry to create a solution of its own under threat of legislation.

Overall, online child pornography regulation provided rich material to explore the implications of hybrid regulation. First, the consensus about its criminal nature and the will to regulate were common grounds to explore regulatory differences and similarities of the jurisdictions chosen. Second, this investigation not only covered most implications from the academic literature but also covered other issues from the documentary evidence. Third, it explored a number of regulatory measures (for example comprehensive systems of website and blocklist for search engines) that remained politically sensitive and inappropriate to be employed against other types of material available online in modern industrialised democracies. Furthermore, the subject matter made evident the regulatory appeal of both child pornographic material and the convincing discourse of child protection as a justifying basis for increased regulation of both content and users' activities on the Internet generally.

Although there were a number of other applications and platforms to exchange and access child pornographic content, the regulatory measures in place targeted only the WWW environment; this made the measures only partially effective. For some, the web-based regulatory policies are

entirely ineffective to limit access because much of the pornographic material moved from public websites to more resilient online platforms and applications. Such situation not only motivated and justified the use of mandatory and increasingly invasive regulatory policies, but put in place a regulatory infrastructure that could be used to target other types of material. This suggests that child pornography was used as a means to increase the regulation of the online environment generally. Of course, other types of material (such as terrorism-related and material containing incitement to racial hatred) and behaviour (for example, online attacks to national infrastructure) contributed to this regulatory expansion, but anti-child pornography discourse was widely used as a regulatory justification in all jurisdictions observed.

Nevertheless, the resilience of the Internet to evade regulation and enhance crime displacement is no reason to eliminate the prospects of a successful regulatory policy. After all, resilience to regulation and crime displacement are also features of 'offline' crimes or other regulated activities, for example drug trafficking, tax evasion and prostitution. These are all subject to crime displacement after regulation is employed, but this condition does not eliminate the possibility of assessing how successful the regulatory policies employed are.

Another important point concerns whether anti-child pornography policies are converging or diverging internationally, in other words, whether these domestic public-private regulatory arrangements are experiencing increased homogenisation (a type of 'institutional isomorphism)[936] or whether regulatory arrangements are following different paths. The nature of such institutional arrangement is of interest here, whether it is: (1) domain orientated - punctual experiences from one country are used to formulate policy proposals in another jurisdiction; or (2) paradigm orientated - transformations in one jurisdiction aims to achieve overall congruence with a wider policy concept in place in another country.[937]

Taking into account the case study material, developments in this area seems to be not only domain orientated (particularly in relation to the use of the blocking scheme that was implemented in 2004 in the UK and has influenced other countries to follow suit; it is at the moment spreading around the EU) but also policy orientated (for example in relation to the NTD scheme implemented domestically by some countries in Europe after the enactment of the 2000 EU Directive on Electronic Commerce). Furthermore, other factors seem to be in favour of such overall congruence around a wider policy project: the economic interests of online intermediaries to avoid regulatory costs and operate under minimum restrictions worldwide, the need to have a cross-national harmonised response to the problem of child pornography, and the development of uniform regulations in some areas are some of these converging forces.

---

[936] Isomorphism as 'constraining processes that forces one unit in a population to resemble other units that face the same set of environmental conditions'. See DiMaggio, P. and Powell, W., 'The Iron Cage Revisited: institutional Isomorphism and Collective Rationality in Organizational Fields', *American Sociological Review,* 48(2) (1983), 147-60.

[937] These two sources of isomorphism are explored in Lodge, M., *On Different Tracks: Designing Railway Regulation in Britain and Germany* (London: Praeger, 2002), p 22-23.

Finally, another point worth stressing is the selection of priorities after anti-child pornography are enacted and regulation is implemented. Although anti-child pornography discourse pushes online regulation forward, other regulatory targets are prioritised in reality and many other areas are left unchallenged. For example, the daily practice of policing of online crimes showed that much more human and financial resources were employed to target online financial crimes in Brazil when compared to online child pornography.[938] There is therefore a gap between anti-child pornography discourse and regulatory practice that needs further investigation.

7 Concluding comments

This investigation employs evaluative criteria to assess the anti-child pornography laws and regulations in place in Australia, Brazil and the United Kingdom in regards to free speech and privacy protection as well as democracy and principles of good regulation in the online environment. This aimed to explore different features of public-private regulatory configurations found in these jurisdictions, to learn from current policymaking in the area, and also to advance the debate over a number of issues raised in the literature review chapter. This research is therefore important to regulatory and governance theorists as well as criminologists.

First, this investigation makes a number of contributions for the comparative research of regulatory models tackling online child pornographic material domestically and internationally. It designed and employed a typology of regulatory models to conduct comparative research and also discussed the option of comparing such regulatory configurations in terms of public-private arrangements and functional equivalents. It shows that the existing models in all three jurisdictions are much more complex than the state, self and hybrid categories and that, although the state played a significant role,[939] there is fragmentation of power and authority in the regulatory environment. As such, it suggests a comparative classification based not on 'pure' regulatory models but on the function that such public-private arrangements play. In addition, it improves the cross-national evaluative criteria for anti-online child pornography regulations designed in Chapter 2 taking into account the contributions from fieldwork. These are all important tools and discussions to undertake cross-national comparative studies in the area of child pornography regulation and may represent a starting point where further research is developed such as an international comparative impact assessment tool.

Second, it suggests a number of improvements to current policymaking: (1) minimising violations of free speech and privacy as well as securing that the principles of good regulation are met via legislated safeguards and their permanent monitoring; (2) strengthening international interfaces of domestic regulatory arrangements so as to tackle the challenges posed by the multi-jurisdictional nature of the Internet; and (3) achieving a balance to adjudicate the

---

[938] See the annual reports by the Brazilian Federal Police. From 1999 to 2008, they conducted 22 police operations and investigated 958 cases related to online child pornography. DPF, 'Relatórios Anuais de Atividades', (Brasília-DF, Brasil: Departamento de Polícia Federal, 2009) at <http://www.dpf.gov.br/institucional/relatorio-anual-pf/>, accessed 28 May 2012.

[939] A regulatory compromise would not follow organically from within the environment.

apparent illegality of online material. These serve as guide to policymaking in the area and also advance current knowledge about judicial oversight within the online environment.

This investigation shows that the existence of a state regulator is no guarantee that accountability, transparency and legitimacy are met, and thus a legislative scheme of safeguards, establishing general principles and the permanent monitoring of such principles, is needed. It also shows that the multi-jurisdictional challenge of the Internet is not only legal but regulatory and whilst international law may establish general terms for action, international protocols and standards can be established in a more flexible and creative manner, for example, taking into account that the public-private arrangements can operate as regulatory nodes. Furthermore, it stresses that automated regulatory technologies employed by non-judicial actors are welcome if used judiciously.

Third, it shows the relevance of the local regulatory environment and culture for child pornography regulation and their implications for cross-national comparison and international regulatory interfaces: there are cultural variations despite the international consensus about the problem that reflect both domestically and internationally. In addition, it makes evident how the resilient and multi-jurisdictional nature of the Internet contributes to crime displacement, and that the problem of online child pornography provided rich material to explore the implications of hybrid regulation and to enrich the dialogue amongst regulation and governance theorists, and criminologists.

The next chapter reflects on the research process, explores the contribution made to knowledge, the originality and limitations of this research, and also a number of avenues for future investigation about the topic.

CHAPTER 7: LIMITATIONS AND FUTURE RESEARCH

This investigation employs evaluative criteria against the laws and regulations limiting access to child pornography available on the Internet in Australia, Brazil and the United Kingdom to address the implications of hybrid regulation. It designs evaluative criteria for anti-online child pornography regulations and a scheme of safeguards to minimise violations of free speech and privacy protection as well as to strengthen democratic values and secure good regulation. It also discusses the broad lessons associated with online child pornography regulation, the use of decentred and polycentric theories of regulation to approach the child pornography problem, the problematic international interfaces of domestic regulatory arrangements, the adjudication of apparent illegality of online material by private actors, and explores the way forward for the regulatory intervention in this area.

This final chapter reflects on the research process and explores the contribution made to knowledge, the originality and limitations of this study, and a number of avenues for future investigation about the topic

1 Originality and contribution to knowledge

This investigation identifies and explains anti-child pornography laws and regulations in place in three jurisdictions and maps out a number of negative consequences of hybrid regulation for free speech, privacy protection and democracy on the Internet. The findings from such diverse regulatory environments may help improving current policymaking in the area.

Although cultural issues are not entirely excluded from the analysis, this investigation is not intended to explain the regulatory differences in terms of their cultural and institutional dissimilarities. Such a research question would demand other methods in addition to the documentary analysis. In short, the documentary analysis undertaken here does not allow to explore in detail the reasons why a configuration was in place, or which political struggles were that led to such configuration in one jurisdiction or another; such approach would demand a review of the relevant literature, further *in loco* unstructured interviews and perhaps also participant observation for a longer period.

Chapter 3 argues that this research is important for three key reasons: (1) policymaking; (2) legal, criminological and regulatory scholarship; (3) and new case study evidence of how regulation works. Indeed, these are the key contributions made.

First, the comparative analysis identifies a range of potential threats from anti-online child pornography regulation, develops cross-national evaluative criteria, and suggests a scheme of safeguards. In addition, it explores a number of ways by which policymakers can tackle the multi-jurisdictional challenge of the Internet. These have further practical utility as a guide for

policymaking in relation to regulation designed to limit access to child pornographic material available online.

Second, the academic literature about Internet regulation and governance are explored and tested out against the evidence from case studies. The topics discussed include the implications of hybrid regulation, the use of decentred and polycentric theories of regulation to explain child pornography regulation, the problematic assessment of apparent illegality of online material by private actors, the models of regulation applied to online pornography and the cross-national similarities and differences of public-private regulatory arrangements, and the call for increased publicness of such arrangements.

Third, this investigation addresses a number of issues of interest to criminologists such as the evolution of anti-online child pornography laws, the resilient nature of the Internet and displacement of cybercrime, and the regulatory rationales used to criminalise a number of conducts and material associated with child pornography. Furthermore, it critically analyses the the problematic enforcement of existing legal frameworks (for example, in relation to criminal content regulation) on the Internet and whether simpler and more flexible legal approaches may solve most of the enforcement problems identified.

Finally, this research also explores the evolution of anti-child pornography laws and regulations in Brazil, where little academic information was available. It provides therefore a starting point for further research in the field.

It is also worth stressing the role of the experts' consultation exercise. This is innovative in the sense that the experts' feedback about the case study material is part of the overall research methodology, instead of a mere peer-review activity, similar to those used in journal publications. The consultation exercise is used as a validation method, and helps to explore issues neglected during the documentary analysis. It hints at other relevant questions that can be explored in future research.[940]

2 Strengths and limitations

This investigation provides detailed and through data about laws and regulations to limit access to child pornography available on the Internet in three jurisdictions and explores the Brazilian regulatory landscape where little information was available about the topic. In addition, the case study material is validated by local experts from each jurisdiction.

The research also lays out the basis for the development of an international evaluative model, and a scheme of safeguards needed to protect free speech, privacy and democracy online. In addition, it tests out a number of assumptions from the academic literature against documentary evidence, and provides data where further research on the topic can be pursued.

---

[940] See Sections 2 and 3 below.

The problem of online child pornography regulation is addressed in a multidisciplinary manner taking into account the regulation, criminological and legal academic literature. The contributions from different areas of knowledge provides varied perspectives about the topic and enhances the overall analysis. Concepts, ideas and debates from each of these areas are used to explore the problem of online child pornography regulation.

Finally, this investigation helps developing a number of skills such as accessing people, convincing experts to participate, giving papers in conferences, accepting criticisms, and understanding that research can be a never-ending process.

Nevertheless, this study has a few limitations that may indicate further research trajectories. Although the evaluative criteria developed in this investigation helped comparing and analysing the case study material and thus achieving the aims proposed at the outset of this research project, this topic needs a more detailed and robust critical appraisal about its derivation in order to improve current limitations, increase cultural adaptability and be used in future comparative work. Indeed, this is a key research area worth exploring further.

In addition, confidence in the evaluative criteria and scheme of safeguards proposed here can be made more robust if the regulation of access to other types of material available on the Internet such as copyrights protected, defamatory, and state classified information are included in future analysis.

This investigation can also benefit from including other jurisdictions (such as the US, Russia and China) as case studies to enlarge the sample and achieve more generalising power. The US is important as it illustrates a different approach of imposing criminal liability on online intermediaries; Russia, because it has been accused of being a worldwide repository of child pornographic material available on public websites, and because it has recently experienced the operation of an Internet hotline domestically;[941] and China for its extensive regulatory approach in relation to online content.

Other issues such as the political struggles that led to the regulatory choices made domestically, the institutional agendas, the cultural variables that shaped regulation are all relevant topics that should be explored further. These 'why' questions are not easily addressed via documentary analysis, but need *in loco* unstructured interviews and participant observation. Although the documentary analysis is able to fulfil the aims and objectives set out for this investigation,[942] this research is unable to explain in detail why the regulatory landscape is the way it is. Nevertheless, this is another area that deserves attention. The process of agenda setting and the reasons why certain policy alternatives are chosen, and others not, vary cross-nationally and

---

[941] 'Friendly Runet Foundation', at <http://hotline.friendlyrunet.ru/?l=en>, accessed 28 May 2012.

[942] Section 1 stressed that this investigation was not intended to explain the regulatory differences in terms of the cultural and institutional dissimilarities, mainly because of limited time and financial resources.

have to do with the cultural contexts where these decisions are taken.[943] These questions are important in explaining the cross-national differences, the economics of anti-online child pornography regulation, the regulatory history, and to justify future regulatory intervention.

Another area that needs further exploration is the negative implications of anti-child pornography regulatory measures for privacy protection. The laws and regulation in regards to investigatory and surveillance powers given to law enforcement authorities are only peripherally addressed in each jurisdiction and it deserves an investigation of its own, particularly in relation to police investigations and relationships established with online intermediaries for the disclosure of information about Internet users.

Finally, this investigation does not intend to explore in depth other aspects around the problem of online child pornography, for example its production and distribution, the police investigations, criminal prosecutions, and the operation of the courts. Further research on this topic is important to provide the wider context where the anti-online child pornography laws and regulations operate. Further research about the convicted offenders, victims, and other Internet applications and platforms may provide important information to guide policymaking in this area. One thing that this author would do differently would be to conduct *in loco* unstructured interviews and participant observation as well as to add other jurisdictions as case studies.

3 Future research

Although this research covers only part of the problem and has its own limitations, it provides a number of avenues for future research on the topic. They are: (1) to explore further and enhance both the evaluative criteria and scheme of safeguards so as to develop an international comparative model, and an impact assessment tool in relation to free speech and privacy protection as well as good regulation on the Internet; (2) to employ the evaluative model against other types of criminal material available on the Internet; (3) to include other jurisdictions's regulatory measures to limit access to child pornographic content available on the Internet; (4) to address the regulatory measures tackling the production and distribution of online child pornography; (5) to explore the developments in relation to multi-state regulation, such as international treaties, standardised legal definitions, liability and responsibilities of online intermediaries, and improvements around the international interfaces of these public-private regulatory arrangements; (6) to explore possible uses of complex network theory to the regulation of criminal online material; (7) to assess the impact of the liability placed on online intermediaries in the USA in relation to child pornographic material; (8) to explore the economy or regulation in relation to child pornographic material, the impact of regulatory measures for

[943] Kingdon provides a conceptual framework on which to explore these issues further. See Kingdon, J., *Agendas, Alternatives, and Public Policies* (Updated 2nd edn.; London: Longman, 2011).

the digital economy and for the creativity in the Internet industry; and (9) to conduct research about assessing successful anti-online child pornography regulatory policies.

This study shows that regulation of the Internet is increasing not only in relation to issues of infrastructure, but also in relation to the controversial material available online. There are increased legal liabilities placed on online intermediaries, more invasive surveillance powers given to law enforcement authorities, and widespread use of sophisticated and automated architecture-based regulatory tools. The question is no longer whether the Internet should or should not be regulated but which forms of regulation are appropriate. This is the reason why the discussion developed here concerned the potential negative implications of current policies for the protection of free speech, privacy and principles of good regulation online.

Another important research topic is however whether the escalation of laws and regulations in relation to online criminal content is creating more problems than solving them. Indeed, such legislative proliferation may undermine the judicial process (for example, creating legal inconsistencies, making the process of reaching judicial decisions more costly and problematic, and putting too great a demand on the criminal justice system) and also the implementation of online content regulatory measures such as ineffective and inefficient policies, unattainable expectations, violation of civil liberties, and limit the digital economy's growth. It is perhaps about time to explore new theoretical legal models, less punitive criminal laws, and flexible regulatory approaches towards the criminal content available online.

Of course, there is much more to do but this research matters because it describes and compares the anti online child pornography policies in place in three different jurisdictions; it assesses the implications of these policies for online democracy in general; it may serve as a guide for future cross-national comparisons and policymaking in the field; and explores the broader lessons of online child pornography regulation such as that the evaluation of 'success' should not follow an economicist approach only, that the existing regulatory culture plays a crucial role in the regulatory dynamics, and that the excessive judicialisation on online content regulation may pose more dangers than guarantee proper protection. In addition, this research tests out some key assumptions found in the academic literature, particularly that a statutory regulator may guarantee transparency, legitimacy and accountability of regulatory intervention; also, it critically reviews the practicalities and costs involved in implementing children and civil liberties protection principles as well as crime control and economic development strategies in the online environment. It is expected that these contributions will help advancing existing knowledge in the field and also open new avenues for academic enquiry.

REFERENCES

1 CASES

1.1 France

LICRA et UEJF v Yahoo! Inc. and Yahoo France, Tribunal de Grande Instance de Paris, Superior Court of Paris

1.2 United Kingdom

R. v Hicklin [1868] LR 3 QB 360

R. v Penguin Books [1961]

R. v Stanley [1965] 1 All ER 1035; [1965] 2 QB 327; [1965] 2 WLR 917; 129 JP 279; 109 Sol Jo 193; 49 Cr App Rep 175, CCA

DPP v Whyte [1972] AC 849

R. v Buttler [1992] 1 S.C.R. 452

R. v Fellows and Arnold [1997] 2 All ER 548

Atkins v DPP; Goodland v DPP [2000] 2 All ER 425; [2000] 1 WLR 1427 (QBD)

R. v Bowden [2000] 2 All ER 418

R. v Goldman [2001] Crim LR 822

R v Oliver and others [2002] EWCA Crim 2766; [2003] 2 Cr App R (S) 64; [2003] 1 Cr. App. R. 28; [2003] 2 Cr. App. R. (S.) 15; [2003] Crim. L.R. 127

R. v Perrin [2002] EWCA Crim 747

R. v Smith and R. v Jayson [2002] EWCA Crim 683; [2003] 1 Cr App R 13

R. v Collier [2005] EWCA Crim 1411

R. v Dooley [2006] 1 WLR 775, [2005] EWCA Crim 3093

R. v Porter [2006] EWCA Crim 560; [2006] All ER (D) 236 (Mar)

Twentieth Century Fox et al v BT [2011] EWHC 1981 (Ch)

1.3 United States

Ashcroft v ACLU, 535 US 564 (2002)

Ashcroft v Free Speech Coalition, 535 US 234 (2002)

Bernstein v United States (1996)

FCC v Pacifica Foundation, 438 US 726 (1978)

Ginsberg v New York, 390 US 629 (1968)

Miller v California, 413 U.S. 15 (1973)

New York v Ferber, 458 US 747 (1982)

Osborne v Ohio, 495 US 103 (1990)

Reno v ACLU, 521 US 844 (1997)

Roth v. United States, 354 U.S. 476 (1957)

United States et al. v American Library Association et al., 539 US 194 (2003)

2 LEGISLATION AND LEGISLATIVE PROPOSALS

2.1 United Nations

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002)

UN Convention on the Rights of the Child. Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989. Entry into force 2 September 1990, in accordance with article 49. 1989 (United Nations)

Worst Forms of Child Labour Convention 1999 (International Labour Organization (ILO) in 1999 as ILO Convention No 182) (ILO)

UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2000 (adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002) (United Nations)

2.2 Europe

EU Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14. 1950 (04 Nov 1950) (European Union)

The Data Retention (EC Directive) Regulations 2009 (European Union)

European Data Protection Directive (Directive 95/46/EC), 24 October 1995 (European Union)

EU Directive on Electronic Commerce. DIRECTIVE 2000/31/EC, 08 June 2000 (European Union)

Council of Europe Convention on Cybercrime 2001 (opened for signature on 23/11/2001, entered into force on 01/07/2004, CETS No. 185, Budapest) (Council of Europe)

Additional Protocol to the Convention of Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems 2003 (opened for signature on 28/01/2003, entered into force on 01/03/2006, CETS No. 189, Strasbourg) (European Union)

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 (COM(2010)94 final), 29 March 2010 (Brussels)

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA 2011 (European Union)

2.3 Australia

Customs Act 1901 (Cth Australia)

Telecommunications (Interception and Access) Act 1979 (Cth Australia)

Freedom of Information Act 1982 (Cth Australia)

Broadcasting Services Act 1992 (Cth Australia)

Classification (Publications, Films and Computer Games) Act 1995 (Cth Australia)

Criminal Code Act 1995 (Cth Australia)

Telecommunications Act 1997 (Cth Australia)

Broadcasting Services Amendment (Online Services) Act 1999 (Cth Australia)

Commonwealth of Australia Constitution Act 2003 as amended (Australia)

Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth Australia)

Surveillance Devices Act 2004 (Cth Australia)

Australian Communications and Media Authority Act 2005 (Cth Australia)

National Classification Code 2005 (Cth Australia)

Communications Legislation Amendment (Content Services) Act 2007 (Cth Australia)

Telecommunications (Interception and Access) Amendment Act 2007 (Cth Australia)

Guidelines for the Classification of Films and Computer Games 2008 (Cth Australia)

2.4 Brazil

Código Penal. Decreto-Lei No. 2.848, de 07/12/40. 1940 (Brasil)

Código de Processo Penal. Decreto-Lei No. 3.689, de 03/10/41. 1941 (Brazil)

Constituição da República Federativa do Brasil 1988 (Brazil)

Lei No. 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente 1990 (Brazil)

Projeto de Lei No. 84 de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. (1999). at <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>, accessed 18 April 2011

Lei No. 10.764, de 12 de novembro de 2003. Altera a Lei No. 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. 2003 (Brazil)

Decreto No. 5.007 de 08 de março de 2004. Promulga o Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil. 2004 (entered into force on 08 March 2004) (Brasil)

Lei No. 11.829, de 25 de novembro de 2008. Altera a Lei No. 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008 (Brazil)

Projeto de Lei do Senado, No. 494 de 2008 - Disciplina a forma, os prazos e os meios de preservação e transferência de dados informáticos mantidos por fornecedores de serviço a autoridades públicas, para fins de investigação de crimes praticados contra crianças e adolescentes, e dá outras providências. (2008). at <http://www.senado.gor.br>, accessed 26 April 2011

Marco Civil da Internet (2010). at <http://culturadigital.br/marcocivil/>, accessed 26 April 2011

Projeto de Lei do Senado No. 100 de 2010 - Altera a Lei No. 8.069 de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes da polícia

na Internet com o fim de investigar crimes contra a liberdade sexual de crianças ou adolescentes (2010). at <http://www.senado.gov.br>, accessed 13 May 2011

2.5 United Kingdom

Obscene Publications Act (20 & 21 Vict. c.83) 1857 (England and Wales)

Obscene Publications Act (c.66) 1959 (England and Wales)

Obscene Publications Act (c.74) 1964 (England and Wales)

Protection of Children Act (c.37) 1978 (England and Wales)

Copyright, Design and Patents Act 1988 (England and Wales)

Criminal Justice Act (c.33) 1988 (England and Wales)

Criminal Justice and Public Order Act (c.33) 1994 (England and Wales)

Criminal Justice and Court Services Act (c.43) 2000 (England and Wales)

Regulation of Investigatory Powers Act (c.23) 2000 (England and Wales)

Sexual Offences Act (c.42) 2003 (England and Wales)

Charities Act (c. 50) 2006 (England and Wales)

The Criminal Justice and Immigration Act (c.4) 2008 (England and Wales)

Coroners and Justice Act (c.18) 2009 (England and Wales)

Digital Economy Act (c. 24) 2010 (England and Wales)

2.6 United States

'18 U.S.C. § 2702 US Code - Section 2702: Voluntary disclosure of customer communications or records', (USA, at <http://codes.lp.findlaw.com/uscode/18/I/121/2702>, accessed 20 March 2012

Child Protection Act 1984 (Pub. L. No. 98-292, 98 Stat. 204) (USA)

Child Sexual Abuse and Pornography Act 1986 (Pub. L. No. 99-628, 100 Stat. 3510) (USA)

Child Protection and Obscenity Enforcement Act 1988 (Pub. L. No. 100-690, 102 Stat. 4486) (USA)

Digital Millennium Copyright Act 1988 (17 USC § 512 (g)) (USA)

Child Pornography Prevention Act 1996 (United States, Pub. L. No. 104-208, 110 Stat. 3009) (USA)

Communication Decency Act 1996 § 502, 110 Stat. (United States of America)

Child Online Protection Act 1998 (United States of America)

Child Internet Protection Act 2000 (47 USC §§ 254 (h)) (USA)

Protect Act 'Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today' 2003 (Pub.L. 108-21, Title V, 30 April 2003, 117 Stat. 650, S. 151) (USA)

Enhancing the Effective Prosecution of Child Pornography Act 2007 (P.L. 110-358) (sanctioned 08 October 2008) (USA)

PROTECT Our Children Act 2008 (Pub.L. 110−401, 122 Stat. 4229) (enacted 13 October 2008) (USA)

3 REGULATIONS, POLICYMAKING DOCUMENTS AND AGREEMENTS

3.1 Europe

Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services. Brussels, 16.10.1996, COM(96) 483 final. (1996)

Illegal and Harmful Content on the Internet. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Brussels, 16.10.1996, COM (96) 487 final. (1996). at <http://aei.pitt.edu/5895/01/001527_1.pdf> accessed 12 July 2010

Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (1999)

Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. (1999)

'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions concerning the evaluation of the Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors. Brussels, 03.11.2003. COM(2003) 653 final.', 2003)

Decision No. 1151/2003/EC of the European Parliament and of the Council, of 16 June 2003, amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. (2003)

'The Evaluation of the Safer Internet Action Plan 1999-2002. Executive Summary.', (Luxembourg: European Commission, 2003)

Decision No. 854/2005/EC of the European Parliament and of the Council, of 11 May 2005, establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies. (2005)

'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Final evaluation of the implementation of the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Brussels, 06.11.2006, COM(2006) 663 final.', 2006)

Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies. (2008). Strasbourg at <http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm>

Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA. 2009 (Brussels)

Safer Internet: A multi-annual Community programme on protecting children using the Internet and other communication technologies. Work Programme (2009). Brusselsat <http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm> accessed 07 July 2011

CDT, 'Yahoo France case', at <http://www.cdt.org/grandchild/yahoo-france-case>, accessed 04 June 2010

EDRI, 'Internet Blocking Booklet', (Brussels: European Digital Rights, 2010) at <http://www.edri.org/files/blocking_booklet.pdf>, accessed 04 June 2010

INTERPOL, 'Criteria for inclusion in the "Worst of"-list', (Interpol, 2011) at <http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list> Accessed 06 March 2012

3.2 Australia

'Classification Website, Australian Commonwealth Government', at <http://www.classification.gov.au/>, accessed 07 September 2011

'BBS Task-force Report', (Australia, 1994) at <http://web.archive.org/web/20020906144005/http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&pathid=/pubs/bulletin_board/report.htm>, accessed 05 March 2012

Agreement between [Commonwealth, States & Territories] relating to a revised co-operative legislative scheme for censorship in Australia (1995). at <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~30000intergovernmental+agreement.pdf/$file/30000intergovernmental+agreement.pdf> accessed 06 March 2012

'Principles for a Regulatory Framework for On-line Services in the Broadcasting Services Act 1992', (Australia: Ministry for Communications and the Arts and the Attorney-General, 1997) at <http://web.archive.org/web/20000226172048/http://www.dcita.gov.au/nsapi-text/?MIval=dca_dispdoc&pathid=/policy/framework.html>, accessed 05 March 2012

'Report of the 'Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies', (Australia, 1997) at <http://www.aph.gov.au/senate/committee/comstand_ctte/online3/index.htm>, accessed 05 March 2012

'Broadcasting Services Amendment (Online Services) Bill 1999: Explanatory Memorandum', The Parliament of the Commonwealth of Australia: The Senate, 1999) at <http://www.comlaw.gov.au/Details/C2004B00465/Explanatory%20Memorandum/Text>, accessed 05 March 2012

Restricted Access Systems Declaration (No 1) (1999). Australian Broadcasting Authority, ABA

'Six Month Report on Co-Regulatory Scheme for Internet Content Regulation', (Australia: Minister for Communications, Information Technology and the Arts, 2000) at <http://www.archive.dbcde.gov.au/__data/assets/file/0013/11560/Six-month_report_on_co-regulatory_scheme_for_internet_content_regulation_January_to_June_2001.rtf>

'NetAlert Protecting Australian Families Online', (Australian Government, 2007) at <http://www.dbcde.gov.au/__data/assets/pdf_file/0011/72956/Protecting-Australian-Families-Online-booklet.pdf> Accessed 25 September 2011

Restricted Access Systems Declaration (2007). Australian Communications and Media Authority, ACMA

'Proposed Reforms to Commonwealth Child Sex-Related Offences', (Attorney-General's Department, Australian Government, 2009) at <http://www.ag.gov.au> Accessed 25 September 2011

'Chapter 6 of the Joint Parliamentary Committee report on their inquiry into the Cybercrime Legislation Amendment Bill 2011', (Australia, 2011) at <http://www.aph.gov.au/house/committee/jscc/cybercrime_bill/report/chapter6.pdf>, accessed 05 March 2012

'Official Committee Hansard - SENATE - ENVIRONMENT AND COMMUNICATIONS LEGISLATION COMMITTEE: Estimates', (Canberra, 2011) at <http://www.aph.gov.au/hansard/senate/commttee/s380.pdf>, accessed 06 March 2012

The AAT decision in Electronic Frontiers Australia Incorporated and Australian Broadcasting Authority Q2000/979 (2002). Adminstrative Appeals Tribunal, at <http://www.efa.org.au/FOI/AAT2000-979_dec.pdf> accessed 01 September 2011

ABA, 'Investigation into the Content of On-line Services', (Australia: Australian Broadcasting Authority, 1996) at <http://web.archive.org/web/20060827020412/http://www.acma.gov.au/acmainterwr/aba/about/recruitment/olsfinal.pdf>, accessed 05 March 2012

ACMA, 'Restricted Access Systems Declaration 2007 - Explanatory Statement', (Australian Communications and Media Authority, 2007) at <http://www.comlaw.gov.au/> Accessed 22 August 2011

ACMA, 'Closed Environment Testing of ISP-Level Internet Content Filtering: Report to the Minister for Broadband, Communications and the Digital Economy', ACMA, 2008) at <http://www.acma.gov.au>, accessed 28 August 2011

ACMA, 'ACMA hotline – Frequently asked questions: 25. What is the relationship between the ACMA and law enforcement?', (updated 02 September 2011) at <http://www.acma.gov.au/WEB/STANDARD/pc=PC_310147#25>

ALRC, 'National Classification Scheme Review', (Sydney, Australia: Australian Law Reform Commission, 2011) at <http://www.alrc.gov.au/inquiries/national-classification-review> Accessed 06 March 2012

Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Main Report', Internet Industry Association - IIA Australia, 2008) at <http://sydney.edu.au/engineering/it/~bjornl/Main_Report_-_Final.pdf>, accessed 07 September 2011

Collins, L., et al., 'Feasibility Study: ISP Level Content Filtering - Part 2', Internet Industry Association - IIA Australia, 2008) at <http://www.dbcde.gov.au/__data/assets/pdf_file/0019/95311/Part_2_-_Attachments_Final.pdf>, accessed 07 September 2011

Conroy, S., 'Media Release: Outcome of consultations on Transparency and Accountability for ISP Filtering of RC content', (2010) at <http://www.minister.dbcde.gov.au/media/media_releases/2010/068> Accessed 06 March 2012

Coonan, H., 'NetAlert: Protecting Australian Families Online - Media Release', (Ministry for Communications, Information Technology and the Arts, 2007) at <http://www.minister.dbcde.gov.au/coonan/media/media_releases/netalert_-_protecting_australian_families_online> Accessed 25 September 2011

EFA, 'History of Internet Regulatory Proposals/Activity in Australia', (updated January 2000) at <http://www.efa.org.au/Issues/Censor/censhistory.html>, accessed 19 September

Graham, I., 'Blinded by Smoke: The Hidden Agenda of the Net Censorship Bill 1999', *Libertus.net*, (1999) at <http://libertus.net/censor/rdocs/blinded.html> accessed 01 September 2011

Graham, I., 'The Net Censorship Dilemma: Liberty or Tyranny', (updated 06 June 2009) at <http://libertus.net/liberty/>, accessed 01 September 2011

Graham, I., 'Overview / Summary: AU Gov't Mandatory ISP Blocking/Censorship Plan', at <http://libertus.net/censor/isp-blocking/au-govplan-overview.html>, accessed 01 September 2011

Graham, I., 'Australia's Internet Censorship System', (updated 11 April 2010) at <http://libertus.net/censor/netcensor.html>, accessed 01 September 2011

Graham, I., 'Detailed information and examples of "RC" material', at <http://libertus.net/censor/isp-blocking/au-govplan-refusedclassif.html#RCexamples>, accessed 06 March

Graham, I., 'Outline of "RC" material', at <http://libertus.net/censor/isp-blocking/au-govplan-refusedclassif.html#RClist>, accessed 06 March

Graham, I., 'Australian ISPs Voluntary Filtering/Blocking', at <http://libertus.net/censor/isp-blocking/au-ispfiltering-voluntary.html>, accessed 06 March 2012

Graham, I., 'Libertus.net: about censorship and freedom of expression, in Australia and elsewhere', at <http://libertus.net/>, accessed 22 August 2011

IIA, 'Codes for Industry Co-Regulation in Areas of Internet and Mobile Content (Pursuant to the Requirements of the Broadcasting Services Act 1992). May 2005 (includes provisions affecting mobile services). Version 10.4. As Registered by the Australian Broadcasting Authority.', (Internet Industry Association, 2005) at <http://www.iia.net.au> Accessed 26 September 2011

IIA, 'Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992 as amended). Registration Version 1.0 - Current and in Force. As approved by Australian Communications and Media Authority on 10 July 2008', (Internet Industry Association, 2008) at <http://www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/content_services_code_2008.pdf> Accessed 07 September 2011

3.3 Brazil

Termo de Compromisso de integração operacional celebrado entre o MPF-SP e os principais provedores de acesso de São Paulo. (2005). MPF-SP, São Pauloat <http://www.prsp.mpf.gov.br/prdc/area-de-atuacao/direitos-humanos/dhumint/Crimes%20contra%20Direitos%20Humanos%20-%20Termo%20de%20Compromisso%20celebr.pdf> accessed 31 August 2010

'Notas taquigráficas da audiência pública realizada no dia 26 de abril de 2006 sobre utilização da Internet como instrumento para a prática de crimes', (Brasília-DF: Comissão de Direitos Humanos e Minorias da Câmara dos Deputados, 2006) at <http://www2.camara.gov.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/notas-taquigraficas/nt26042006.pdf> Accessed 20 April 2011

Termo de Mútua Cooperação Técnica, Científica e Operacional que entre si Celebram a Procuradoria da República no Estado de São Paulo e a Safernet Brasil. 29 de março de 2006. (2006). São Paulo-SP, Brasilat <http://www.safernet.org.br/site/sites/default/files/mpsp.pdf> accessed 17 March 2012

'Ata da 21a Reunião da Comissão de Constituição, Justiça e Cidadania em conjunto com a 19a Reunião da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal, 04 de julho de 2007', (Brasília-DF, Brasil: Senado Federal, 2007) at <http://www.senado.gov.br> Accessed 13 March 2012

'Comissão Parlamentar de Inquérito do Senado Federal para apurar a utilização da internet na prática de crimes de "pedofilia", bem como a relação desses crimes com o crime organizado', (Brasília-DF, Brasil, 2008) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 March 2012

Term of Adjustment of Conduct settled between the MPF and Google Brasil (2008). CPI da Pedoflia, Brasília-DF at <http://www.prsp.mpf.gov.br/crimes-ciberneticos/GoogleTAC_english_version.pdf/at_download/file> accessed 27 August 2010

Termo de Cooperação celebrado entre a Safernet Brasil e a Google Brasil Internet Ltda. (2008). SAFERNET, São Paulo-SP, Brasil at <http://www.safernet.org.br/site/institucional/parcerias/google> accessed 31 August 2010

Termo de Cooperação Técnica, Científica e Operacional celebrado entre a SEDH-MJ e a Safernet Brasil e outros (2008). SEDH-MJ, Brasília-DF, Brasil at <http://www.safernet.org.br/site/sites/default/files/SEDHDPF.pdf> accessed 31 August 2010

'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, “com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de ‘pedofilia’, bem como a relação desses crimes com o crime

organizado”', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011

CGI, 'Reunião de 09 de abril de 1999', (Porto Alegre-RS, Brasil: Comitê Gestor da Internet no Brasil, 1999) at <http://www.cgi.br/acoes/1999/rea-1999-04.htm>, accessed 13 March 2012

Termo de Mútua Cooperação celebrado entre as empresas associadas da ABECS, a CPI da Pedofilia e outros. (2008). CPI da Pedofilia, Brasília-DF, Brasil at <http://www.safernet.org.br/site/sites/default/files/abecs.pdf> accessed 31 August 2010

Termo de Mútua Cooperação celebrado entre as prestadoras de serviços de telecomunicações, de provimento de acesso à Internet, a CPI da Pedofilia e outros. (2008). CPI da Pedofilia, Brasília-DF, Brasil at <http://www.safernet.org.br/site/sites/default/files/Teles.pdf> accessed 31 August 2010

CPI, 'Relatório Final da Comissão Parlamentar de Inquérito. Criada por meio do Requerimento nº 2, de 2005-CN, “com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de ‘pedofilia’, bem como a relação desses crimes com o crime organizado”', (Brasília-DF: Senado Federal do Brasil, 2011) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85380&tp=1>, accessed 20 April 2011

CPMI, 'Relatório Final da Comissão Parlamentar Mista de Inquérito da Exploração Sexual de Crianças e Adolescentes', (Brasília-DF, Brasil: Senado Federal, 2004) at <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=56335&tp=1> Accessed 14 March 2012

DPF, 'Relatórios Anuais de Atividades', (Brasília-DF, Brasil: Departamento de Polícia Federal, 2009) at <http://www.dpf.gov.br/institucional/relatorio-anual-pf/>, accessed 28 May 2012

MPF-SP, 'Nota Pública: MPF rescinde Termo de Cooperação com Safernet', (São Paulo-SP: MPF-SP, 2010) at <http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/12-11-10-nota-publica-mpf-rescinde-termo-de-cooperacao-com-safernet/> Accessed 29 April 2011

SAFERNET, 'Parceria com a Google Brasil', at <http://www.safernet.org.br/site/institucional/parcerias/google>, accessed 17 March 2012

SAFERNET, 'Ofício n. 0017/2010/SAFERNET Brasil referente ao cumprimento do termo de cooperação firmado entre a SaferNet e a PR/SP', (São Paulo-SP, Brasil: Safernet Brasil, 2010) at <http://www.safernet.org.br>, accessed 13 March 2012

Suiama, S., 'Nota Técnica GCCC/PR/SP', (São Paulo: MPF-SP, 2010) at <http://www.prsp.mpf.gov.br/sala-de-imprensa/pdfs-das-noticias/crimes-ciberneticos> Accessed 19 April 2011

Sundfeld, C. A., 'Parecer jurídico redigido a pedido das companhias Empresa Brasileira de Telecomunicações S.A. (Embratel), Telecomunicações de São Paulo S.A. (Telesp), Claro S.A., Vivo S.A. e Terra Networks Brasil S.A.', (São Paulo-SP, 2009) at <http://www.senado.gov.br/atividade/comissoes/comissao.asp?origem=SF&com=1422>, accessed 20 April 2011

3.4 United Kingdom

'Report of the Committee on Obscenity and Film Censorship', (London: HMSO, 1979)

'Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003', (2004) at <http://www.cps.gov.uk/publications/docs/mousexoffences.pdf> Accessed 07 June 2011

'Regulation - Less is More Reducing Burdens, Improving Outcomes. A BRTF report to the Prime Minister', Better Regulation Task Force. Department for Business, Enterprise and Regulatory Reform, 2005) at <http://www.bis.gov.uk/files/file22967.pdf>, accessed 03 January 2012

'Consultation on Possession of Non-Photographic Visual Depictions of Child Sexual Abuse', Home Office, 2007) at <http://scotland.gov.uk/Resource/Doc/1099/0048474.pdf>, accessed 12 July 2010

Sexual Offences Act 2003: Definitive Guideline (2007). Sentencing Guidelines Council, at <http://sentencingcouncil.judiciary.gov.uk/docs/web_SexualOffencesAct_2003.pdf> accessed 10 July 2011

'Parliamentary records. Answer given by Home Office Minister Alan Campbell on 02 November 2009', (London: UK Parliament - House of Commons, 2009) at <http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091102/text/91102w0017.htm#09110238001607> Accessed 26 May 2012

'UK code of practice for the self-regulation of new forms of content on mobiles. Version 2 published on 10 June 2009', (2009) at <http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf> Accessed 07 September 2011

'The Grim RIPA: Cataloguing the ways in which local authorities have abused their covert surveillance powers', (London: Big Brother Watch, 2010) at <http://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf>, accessed 12 March 2012

'Indecent photographs of children', *The Crown Prosecution Service* at <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/#a06>, accessed 08 July 2011

Service Level Agreement between the Association of Chief Police Officers and the Internet Watch Foundation (2010). IWF and ACPO, at <http://www.acpo.police.uk/documents/crime/2010/201010CRIIW01.pdf> accessed 14 June 2010

'Privacy and injunctions: Session 2012-12', *Joint Committee on Privacy and Injunctions* (London: House of Lords and House of Commons, 2012) at <http://www.publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/273.pdf>, accessed 01 May 2012

Byron, T., 'Safer Children in a Digital World: The Report of the Byron Review', 2008) at <http://www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf>, accessed 30 June 2010

Coaker, V., 'House of Commons Written Answer from the Home Office Minister, Hansard, 15 May 2006, col 716W', (2006)

Coaker, V., 'House of Commons Written Answer from the Home Office Minister, Hansard, 16 June 2008, col 684W', (London: House of Commons, 2008) at <http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080616/text/80616w0011.htm#08061620000413>, accessed 02 March 2012

CPS, 'Indecent photographs of children: legal guidance', (London: The Crown Prosecution Service, 2012) at <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/>, accessed 03 March 2012

DBCDE, 'ISP filtering - frequently asked questions', (updated 27 May 2011) at <http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering_-_frequently_asked_questions>, accessed 28 August 2011

ISPA, 'ISPA Code of Practice', at <http://www.ispa.org.uk/about_us/page_16.html>, accessed 10 July 2011

IWF, 'Internet Watch Foundation Annual Report 2003', (Cambridge, UK: IWF, 2004) at <http://www.iwf.org.uk>, accessed 07 June 2011

IWF, 'Internet Watch Foundation Annual Report 2004', (Cambridge, UK: IWF, 2005) at <http://www.iwf.org.uk>, accessed 07 June 2011

IWF, 'Annual and Charity Report 2005', (Cambridge, UK: IWF, 2006) at <http://www.iwf.org.uk>, accessed 07 June 2011

IWF, 'Annual and Charity Report 2006', (Cambridge, UK: IWF, 2007) at <http://www.iwf.org.uk>, accessed 07 June 2011

IWF, 'IWF statement regarding Wikipedia webpage' (2008); <http://www.iwf.org.uk/media/news.archive-2009.251.htm> accessed 13 July 2010

IWF, '2008 - Annual and Charity Report ', (Cambridge, UK: IWF, 2009) at <http://www.iwf.org.uk>, accessed 07 June 2011

IWF, 'Annual and Charity Report 2008', (Cambridge, UK: IWF, 2009) at <http://www.iwf.org.uk>, accessed 07 June 2011

IWF, 'Annual and Charity Report 2010', (Cambridge, UK: IWF, 2011) at <http://www.iwf.org.uk>, accessed 02 March 2012

IWF, 'Content Assessment Appeal Process', at <http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process>, accessed 09 July 2011

Marwick, P. and Hall, D., 'Review of the IWF', (London: KPMG, 1999)

OGC, 'Procurement Policy Note – Blocking access to web pages depicting child sexual abuse. Action Note 05/10', (The Office of Government Commerce, 2010) at <http://www.ogc.gov.uk/documents/PPN_05_10_Blocking_illegal_sites.pdf> Accessed 09 July 2011

Sexual Offences Act 2003: Definitive Guideline (2007). Sentencing Guidelines Council, at <http://sentencingcouncil.judiciary.gov.uk/docs/web_SexualOffencesAct_2003.pdf> accessed 10 July 2011

3.5 United States

'Summary and Highlights of the Philadelphia Federal District Court's Decision: CDT v. Pappert, Case No. 03-5051 (E.D. Pa. Sept. 10 2004)', (Washington, DC: Center for Democracy and Technology, 2004) at <http://www.cdt.org/speech/pennwebblock/20040915highlights.pdf>, accessed 11 April 2011

'Attorney General Cuomo and Facebook Announce New Model to Protect Children Online', (New York: Office of the Attorney General, 2007) at <http://www.ag.ny.gov/media_center/2007/oct/oct16a_07.html> Accessed 29 April 2011

'Attorney General Cuomo takes legal action against social networking site that ignores proliferation of child pornography', (New York, NY: Office of the Attorney General, 2008) at <http://www.ag.ny.gov/media_center/2010/june10b_10.html> Accessed 11 April 2011

'Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States (Executive Summary)', (Cambridge, MA: The Berkman Center for Internet & Society at Harvard University, 2008) at <http://cyber.law.harvard.edu/pubrelease/isttf/>, accessed 07 June 2010

APPLE, 'Registered Apple Developer Agreement', (2010)

Barlow, J., 'A Declaration of the Independence of Cyberspace ' (1996); <http://homes.eff.org/~barlow/Declaration-Final.html> accessed 04 June 2010

ICMEC, 'Child Pornography: Model Legislation & Global Review ', International Centre for Missing & Exploited Children, 2008) at <http://www.icmec.org/en_X1/English__5th_Edition_.pdf>, accessed 08 June 2010

4 ACADEMIC LITERATURE

Aarnio, A., *Essays on the Doctrinal Study of Law* (London: Springer, 2011)

Ahlert, C., Marsden, C., and Yung, C., 'How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation', (Oxford: Oxford Institute, 2004) at <http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf>, accessed 01 July 2010

Akdeniz, Y., 'Governance of Pornography and Child Pornography on the Global Internet: a multi-layered approach', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: regulating cyberspace* (Oxford: Hart Publications, 1997), p. 223-41

Akdeniz, Y., 'The Regulation of Pornography and Child Pornography on the Internet' *The Journal of Information, Law and Technology* 1(1997); <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1> accessed 08 June 2010

Akdeniz, Y., 'Who Watches the Watchmen - Part I: Internet Content Rating Systems, and Privatised Censorship', Cyber-Rights & Cyber-Liberties UK, 1997) at <http://www.cyber-rights.org/watchmen.htm>, accessed 06 June 2011

Akdeniz, Y., 'Who Watches the Watchmen - Part II: Accountability & Effective Self-Regulation in the Information Age', Cyber-Rights & Cyber-Liberties UK, 1998) at <http://www.cyber-rights.org/watchmen-ii.htm>, accessed 06 June 2011

Akdeniz, Y., 'Who Watches the Watchmen - Part III: ISP Capabilities for the Provision of Personal Information to the Police', Cyber-Rights & Cyber-Liberties UK, 1999) at <http://www.cyber-rights.org/privacy/watchmen-iii.htm>, accessed 06 June 2011

Akdeniz, Y., 'Controlling Illegal and Harmful Content on the Internet', in David Wall (ed.), *Crime and the Internet* (London: Routledge, 2001), 113-39

Akdeniz, Y., 'Governing Pornography and Child Pornography on the Internet: The UK Approach', *UWLALR,* 32 (2001), 247

Akdeniz , Y., 'Possession and Dispossession: A Critical Assessment of Defences in Possession of Indecent Photographs of Children Cases', *Criminal Law Review,* (2007), 274-88

Akdeniz, Y., *Internet child pornography and the law: national and international responses* (Surrey: Ashgate, 2008)

Akdeniz, Y., 'To block or not to block: European approaches to content regulation, and implications for freedom of expression', *Computer Law & Security Review,* 26 (2010), 260-72

Alston, R., 'The Government's Regulatory Framework for Internet Content', *University of New South Wales Law Journal,* 23(1) (2000), 192-97

Atkinson, P. and Coffey, A., 'Analysing Documentary Realities', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 45-62

Atkinson, P. and Silverman, D., 'Kundera's Immortality: The Interview Society and the Invention of the Self', *Qualitative Inquiry,* 3(3) (1997), 303-25

Baldwin, R., *Rules and government* (Oxford socio-legal studies; Oxford: OUP, 1995)

Baldwin, R. and Cave, M., *Understanding regulation: theory, strategy, and practice* (Oxford: OUP, 1999)

Baldwin, R., Cave, M., and Lodge, M., *Understanding Regulation: theory, strategy and practice* (2nd edn.; Oxford: OUP, 2012)

Baldwin, R., Scott, C., and Hood, C., 'Introduction', in Robert Baldwin, Colin Scott, and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: OUP, 1998), 1-55

Bambauer, D., 'Filtering in Oz: Australia's Foray into Internet Censorship', *Brooklyn Law School, Legal Studies Paper No. 125,* (2008)

Bambauer, D., 'Guiding the Censor's Scissors: A Framework to Assess Internet Filtering', *ExpressO,* at http://works.bepress.com/derek_bambauer/25 (2008)

Bambauer, D., 'Cybersieves', *Duke Law Journal,* 59(3) (2009), 377-446

Bambauer, D., 'The Widening Gyre', *Information, Law, and the Law of Information* (2011) at <http://blogs.law.harvard.edu/infolaw/2011/06/20/the-widening-gyre/> Accessed 29 December 2011

Bambauer, D., et al., 'Internet Filtering in China in 2004-2005: A Country Study', *Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2005-10*, 2005) at <http://ssrn.com/paper=706681>

Banakar, R. and Travers, M., 'Law, Sociology and Method', in R. Banakar and M. Travers (eds.), *Theory and Method in Socio-Legal Research* (Oxford: Hart, 2005)

Bardach, E., *The Implementation Game: What Happens After a Bill Becomes a Law* (Cambridge, MA: MIT Press, 1977)

Bauer, J., 'Internet governance: theory and first principles', in Ravi Kumar Jain Bandamutha (ed.), *Internet governance: an introduction* (Hyderabad, India: The Icfai University, 2007), 40-59

Bauer, M. W., 'Analytic Approaches for Text, Image and Sound', in Martin W. Bauer and George Gaskell (eds.), *Qualitative Researching with Text, Image and Sound: a practical handbook* (London: Sage Publications, 2000), 131-51

Becker, G., 'Crime and Punishment: An Economic Approach', in George Stigler (ed.), *Chicago Studies in Political Economy* (London: The University of Chicago Press, 1988), 537-92

Becker, H. S., *Outsiders: Studies in the Sociology of Deviance* (New York, NY.: The Free Press, 1966)

Becker, H. S. and Geer, B., 'Participant Observation: The Analysis of Qualitative Data', in Robert G. Burgess (ed.), *Field Research: a sourcebook and field manual* (London: Unwin Hyman, 1982), 239-50

Benkler, Y., The Wealth of Networks: How Social Production Transforms Markets and Freedom (London: Yale University Press, 2006)

Benkler, Y., *'Fear of a Networked Fourth Estate',* (2011) (Audio, Radio Berkman #182, 29 April 2011), at <http://blogs.law.harvard.edu/mediaberkman/2011/04/29/radio-berkman-182-was-wikileaks-unprecedented/>, accessed 07 June 2011

Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: The MIT Press, 2006)

Berg-Schlosser, D. and De Meur, G., 'Comparative Research Design: Case and Variable Selection', in Rihoux Benoît and Charles Regin (eds.), *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques* (London: Sage, 2009)

Biegel, S., *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, MA: MIT Press, 2001)

Bing, J., 'Building Cyberspace: a brief history of the Internet', in John Bing and Lee A. Bygrave (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 8-47

Black, J., 'Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world', *Current Legal Problems,* 54 (2001), 103-46

Black, J., 'Critical reflections on regulation', *Australian Journal of Legal Philosophy,* 27 (2002), 1-35

Black, J., 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Law Society Economy Legal Studies Working Paper No. 2/2008* (London: London School of Economics and Political Science, Law Department, 2008)

Bottomley, K. and Pease, K., *Crime and Punishment: interpreting data* (Buckingham: Open University Press, 1986)

Braithwaite, J., 'The New Regulatory State and the Transformation of Criminology', *The British Journal of Criminology* 40 (2000), 222-38

Braithwaite, J. and Ayres, I., *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992)

Brown, I., 'Internet Censorship - Be Careful What You Ask for', in S. Kirca and L. Hanson (eds.), *Freedom and Prejudice: Approaches to Media and Culture* (Istanbul: Bahcesehir University Press, 2007)

Brownsword, R., 'Neither East Nor West: Is Mid-West Best?', *SCRIPT-ed,* 15(3:1) (2006)

Brownsword, R., *Rights, regulation, and the technological revolution* (Oxford: OUP, 2008)

Bryman, A., *Social Research Methods* (3rd edn.; Oxford: OUP, 2008)

Bulmer, R., 'Why the Cassowary is not a bird', in Mary Douglas (ed.), *Rules and Meanings: the anthropology of everyday knowledge* (Harmondsworth: Penguin Books, 1967), 163-67

Callanan, C., et al., 'Internet blocking: balancing cybercrime responses in democratic societies', Open Society Institute, 2009)

Carr, A., 'The social dimension of the online trade of child sexual exploitation material', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010

Carr, J. and Hilton, Z., 'Combating child abuse images on the internet – international perspectives. [Unpublished]', (2010)

Castells, M., *Communication Power* (Oxford: OUP, 2009)

Cave, J., Marsden, C., and Simmons, S., 'Options for and Effectiveness of Internet Self- and Co-Regulation. Summary prepared for the European Commission', (Cambridge: RAND Europe, 2008) at <http://www.rand.org/pubs/technical_reports/2008/RAND_TR566.pdf>, accessed 04 June 2010

Charlesworth, A., 'Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: A Framework for Electronic Commerce.* (2nd edn.; Oxford: Hart Publishing, 2000)

Clayton, R., 'Anonymity and traceability in cyberspace', *Technical Report Number 653* (Cambridge: University of Cambridge, 2005) at <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html>, accessed 20 June 2011

Clayton, R., 'Failures in a Hybrid Content Blocking System', *Workshop on Privacy Enhancing Technologies* (Dubrovnik, Croatia, 2005) at <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf> Accessed 05 July 2010

Clough, J., 'Now you see it, now you don't: Digital images and the meaning of 'possession'', *Criminal Law Forum,* 19 (2008), 205-39

Cohen, S., *Folk devils and moral panics: the creation of the Mods and Rockers* (3rd edn.; London: Routledge, 2002)

Curran, J., 'Reinterpreting Internet history', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 17-37

De Hert, P. and Raab, C., 'Tools for Technology Regulation: Seeking Analytical Approaches', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008)

Deibert, R. and Rohozinski, R., 'Beyond Denial: Introducing Next Generation Information Access Controls', in Ronald J. Deibert, et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010), 3-13

Deibert, R. J., et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010)

DiMaggio, P. and Powell, W., 'The Iron Cage Revisited: institutional Isomorphism and Collective Rationality in Organizational Fields', *American Sociological Review,* 48(2) (1983), 147-60

Duffy, J., 'Toothless Tiger, Sleeping Dragon: Implied Freedoms, Internet Filters and the Growing Culture of Internet Censorship in Australia.', *Murdoch University Electronic Journal of Law,* 16(2) (2009), 91-105

Dupont, B., 'Security in the Age of Networks', *Policing & Society,* 14(1) (2004), 76-91

Dutton, W. and Peltu, M., 'The Emerging Internet Governance Mosaic: Connecting the Pieces', *Forum Discussion Paper No. 5* Oxford Internet Institute, University of Oxford, 2005)

Easton, S., *The Problem of Pornography: regulators and their right to free speech* (London: Routledge, 1994)

Edwards, L., 'Editorial: From child porn to China, in one Cleanfeed ', *Script-ed,* 3(3) (2006), 174-5

Edwards, L., 'The Fall and Rise of Intermediary Liability Online', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 47-88

Edwards, L., 'The Internet is for Porn? Content Filtering and the New Censorship', (2009)

Edwards, L., 'Pornography, Censorship and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet* (3rd edn.; Oxford: Hart Publishing, 2009), 623-69

Edwards, L., 'Anti-social Networking: Inaugural Lecture', (Sheffield: University of Sheffield, 2010)

Edwards, L., 'Law and sausages: How Not to Legislate for the Digital Economy', at <http://blogscript.blogspot.com/>, accessed 03 May 2010

Edwards, L., 'Newzbin 2: Landmark or Laughing Stock?', *Pangloss* (2011) at <http://blogscript.blogspot.com/2011/07/newzbin-2-landmark-or-laughing-stock.html> Accessed 28 December 2011

Edwards, L., 'Role and Responsibility of Internet Intermediaires in the Field of Copyright and Related Rights', (Geneve: WIPO, 2011) at <http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf>, accessed 28 December 2011

Edwards, L., Rauhofer, J., and Yar, M., 'Recent developments in UK cybercrime law', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 413-36

Eneman, M., 'A Critical Study of ISP Filtering of Child Pornography' *European Conference on Information Systems. Paper 209* (2006); <http://is2.lse.ac.uk/asp/aspecis/20060154.pdf> accessed 29 December 2011

Faris, R., Roberts, H., and Wang, S., 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', *The OpenNet Initiative Bulletin* The OpenNet Initiative, 2009)

Faris, R. and Villeneuve, N., 'Measuring Global Internet Filtering', in Ronald Deibert, et al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), 5-28

Feick, J. and Werle, R., 'Regulation of Cyberspace', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2010), 523-47

Feinberg, J., *The Moral Limits of the Criminal Law: Harm to Self* (Volume 3; New York: OUP, 1986)

Filho, D. R., 'O crime de divulgação de pornografia infantil pela Internet: breves comentários à Lei No. 10.764/03' *Infojus* (2003); <http://www.advogado.adv.br/artigos/2003/democritoreinaldofilho/crimepornografiainfantil.htm> accessed 20 April 2011

Fox, M. and Bell, C., *Learning Legal Skills* (3rd edn.; London: Blackstone Press Ltd., 1999)

Gaspari, E., *A Ditadura Envergonhada* (vol. 1; São Paulo-SP: Companhia da Letras, 2002)

Gaspari, E., *A Ditadura Escancarada* (vol. 2; São Paulo-SP: Companhia da Letras, 2002)

Gaspari, E., *A Ditadura Derrotada* (vol. 3; São Paulo-SP: Companhia da Letras, 2003)

Gaspari, E., *A Ditadura Encurralada* (vol. 4; São Paulo-SP: Companhia da Letras, 2004)

Gerson, K. and Horowitz, R., 'Observation and Interviewing', in Tim May (ed.), *Qualitative Research in Action* (London: Sage Publications, 2002), 199-224

Gillespie, A., 'Indecent Images of Children: the ever-changing law', *Child Abuse Review,* 14 (2005), 430-43

Gillespie, A., 'Tackling Child Pornography: The Approach in England and Wales', in Max Taylor and Ethel Quayle (eds.), *Viewing child pornography on the Internet* (Dorset: Russel House Publishing, 2005)

Gillespie, A., 'Defining Child Pornography: Challenges for the Law', *Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children* (University of North Carolina, NC, USA, 2009) at <http://www.iprc.unc.edu/symposium.shtml> Accessed 24 June 2010

Gillespie, A., *Child Pornography: law and policy* (Oxon: Routledge, 2011)

Glebstein, E. and Kurbalija, J., 'Internet Governance: issues, actors and divides', *DIPLO Report* DIPLO / GKP, 2005) at <http://www.diplomacy.edu/ISL/IG/>

Goldsmith, J., 'Regulation of the Internet: Three Persistent Fallacies', Chicago-Kent Law Review, 73 (1998), 1119-31

Goldsmith, J. and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World* (New York, NY: OUP, 2006)

Grabosky, P., 'Discussion Paper: Inside the Pyramid: Towards a Conceptual Framework for the Analysis of Regulatory Systems', *International Journal of Sociology of Law,* 25 (1997), 195-201

Grabosky, P., 'The Global Dimension of Cybercrime', *Global Crime,* 6(1) (2004), 146-57

Grabosky, P., *Electronic Crime* (Master Series in Criminology; Upper Saddle River, NJ: Pearson Prentice Hall, 2007)

Grabosky, P., 'Security in the 21st Century', *Security Journal,* 20 (2007), 9-11

Grabosky, P. and Smith, R., *Crime in the Digital Age: controlling telecommunications and cyberspace illegalities* (New Brunswick-NJ and Sydney: Transaction Publishers and Federation Press, 1998)

Griffith, G., 'Censorship in Australia: Regulating the Internet and other recent developments', NSW Parliamentary Library Research Service, 2002) at <http://www.parliament.nsw.gov.au>, accessed 25 September 2011

Griffith, G. and Simon, K., 'Child Pornography Law', New South Wales Parliament, 2008) at <http://www.parliament.nsw.gov.au/prod/parlment/publications/>, accessed 12 July 2010

Guadamuz, A., *Networks, Complexity and Internet Regulation: Scale-Free Law* (Cheltenham, UK: Edward Elgar, 2011)

Gunningham, N., 'Enforcement and Compliance Strategies', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2012), 120-45

Gunningham, N. and Grabosky, P., *Smart Regulations: Designing Environmental Policy* (Oxford: OUP, 1998)

Hafner, K. and Lyon, M., *Where Wizards Stay Up Late* (New York: Simon & Schuster, 1998)

Harley, B., 'A Global Convention on Cybercrime?' *The Columbia Science and Technology Law Review* (2010); <http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/> accessed 29 August 2010

Hirst, P., 'Democracy and Governance', in Jon Pierre (ed.), *Debating governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000), 13-35

Holstein, J. A. and Gubrium, J. F., *The active interview* (Qualitative research methods; Thousand Oaks, Calif. ; London: Sage, 1995)

Holstein, J. A. and Gubrium, J. F., 'Active Interviewing', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 113-29

Hood, C., *Administrative Analysis: an introduction to rules, enforcement and organizations* (Brighton, Sussex: Wheatsheaf Books Limited, 1986)

Hood, C., 'Assessing the Dangerous Dogs Act: when does a regulatory law fail?', *Public Law,* Summer (2000), 282-305

Hood, C. and Margetts, H., *The Tools of Government in the Digital Age* (2nd revised edn.: Palgrave Macmillan, 2007)

Hunter, P., 'BT Site Block: BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns', *Computer Fraud and Security,* (9) (2004), 4-5

Jenkins, P., *Beyond Tolerance: Child Pornography on the Internet* (New York: New York University Press, 2001)

Jenkins, P., 'Failure to launch: Why do some social issues fail to detonate moral panics?', *British Journal of Criminology,* 49 (2009), 35-47

Jewkes, Y., 'Public policing and Internet crime', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 525-45

Jewkes, Y. and Andrews, C., 'Internet Child Pornography: international responses', in Yvonne Jewkes (ed.), *Crime Online* (Devon: Willan Publishing, 2007), 60-80

Jewkes, Y. and Yar, M., 'Introduction: the Internet, cybercrime and the challenges of the twenty-first century', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 1-8

Johnson, D., Crawford, S., and Palfrey, J., 'The Accountable Net: Peer Production of Internet Governance', *Berkman Center for Internet & Society at Harvard Law School Virginia Journal of Law and Technology,* 9(9) (2004)

Karstedt, S., 'Comparing cultures, comparing crime: Challenges, prospects and problems for a global criminology', *Crime, Law and Social Change,* 36(3) (2001), 285-308

Kingdon, J., *Agendas, Alternatives, and Public Policies* (Updated 2nd edn.; London: Longman, 2011)

Klang, M., 'Controlling Online Information: Censorship and Cultural Protection', *The World Summit on the Information Society: A Summit of Solutions?* (Uppsala, Sweden and Kampala, Uganda: Collegium for Development Studies, 2005), 43-50

Klang, M., 'Disruptive Technology: effects of technology regulation on democracy', (Göteborg University, 2006),

Koops, B.-J., 'Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008)

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

Krone, T., 'Combating Online Child Pornography in Australia', in Max Taylor and Ethel Quayle (eds.), *Viewing child pornography on the Internet* (Dorset: Russel House Publishing, 2005)

Laidlaw, E., 'Private Power, Public Interest: An Examination of Search Engine Accountability', *International Journal of Law and Information Technology,* 17(1) (2008), 113-45

Lakoff, G. and Johnsson, M., *Metaphors We Live By* (Chicago: Chicago University Press, 1980)

Landau, M., 'Rationality, and the Problem of Duplication and Overlap', *Public Administration Review,* 29(4) (1969), 346-58

Latapy, M., 'Measurement and Analysis of P2P Activity Against Paedophile Content', at <http://antipaedo.lip6.fr/>, accessed 14 March 2012

Leavitt, G. C., 'Relativism and Cross-Cultural Criminology: A Critical Analysis', *Journal of Research in Crime and Delinquency,* 27(1) (1990), 5-29

Leigh, D. and Harding, L., *WikiLeaks: Inside Julian Assange's War on Secrecy* (London: Guardian Books, 2011)

Leiner, B., et al., 'A Brief History of the Internet' *Internet Society* (2003); < http://www.isoc.org/internet/history/brief.shtml> accessed 02 December 2011

Lemos, R., *Direito, Tecnologia e Cultura* (Rio de Janeiro-RJ, Brasil: Ed. FGV, 2005)

Leonardi, M., *Responsabilidade Civil dos Provedores de Serviços de Internet* (São Paulo: Juarez de Oliveira, 2005)

Leonardi, M., 'Controle de conteúdos na Internet: filtros, censura, bloqueio e tutela', in Newton de Lucca and Adalberto Simão Filho (eds.), *Direito & Internet: aspectos jurídicos relevantes* (vol. II; São Paulo: Quartier Latin, 2008), 377-401

Lessig, L., 'What Things Regulate Speech: CDA 2.0 vs. Filtering', *Jurimetrics,* 38 (Summer 1998 1998), 629-70

Lessig, L., Free Culture: The Nature and Future of Creativity (New York: Penguin Books, 2004)

Lessig, L., *Code: version 2.0* (New York, NY: Basic Books, 2006)

Loader, I., 'Plural Policing and Democratic Governance', *Social & Legal Studies,* 9(3) (2000), 323-45

Loader, I. and Sparks, R., 'Contemporary Landscapes of Crime, Order, and Control: governance, risk, and globalization', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (4rd edn.; Oxford: OUP, 2007), 78-101

Lodge, M., *On Different Tracks: Designing Railway Regulation in Britain and Germany* (London: Praeger, 2002)

Lodge, M. and Hood, C., 'Pavlovian Policy Responses to Media Feeding Frenzies? Dangerous Dogs Regulation in Comparative Perspective', *Journal of Contingencies and Crisis Management,* 10(1) (2002), 1-13

Lodge, M. and Stirton, L., 'Accountability in the Regulatory State', in Martin Lodge, Martin Cave, and Robert Baldwin (eds.), *The Oxford Handbook of Regulation* (Oxford: OUP, 2010), 349-70

Maguire, M., 'Crime data and statistics', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (4th edn.; Oxford: OUP, 2007)

Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution* (London: Bloomsbury Academic, 2009)

Marsden, C., Tambini, D., and Leonardi, D., *Codifying cyberspace: communications self-regulation in the age of internet convergence* (New York: Routledge, 2007)

Mason, J., 'Qualitative Interviewing: asking, listening and interpreting', in Tim May (ed.), *Qualitative Research in Action* (London: Sage Publications, 2002), 225-41

McCubbins, M. and Schwartz, T., 'Oversight Overlooked: Police Patrols versus Fire Alarms', *American Journal of Political Science,* 28(1) (1984), 165-79

McGuire, M., *Hypercrime: The New Geometry of Harm* (Oxon: Routledge-Cavendish, 2007)

McIntyre, T., 'Blocking child pornography on the Internet: European Union developments', *International Review of Law, Computers and Technology,* 24(3) (2010), 209-21

McIntyre, T., 'Internet Filtering: Implications of the "Cleanfeed" System', *Third Year PhD Presentation Series* (Edinburgh: School of Law, University of Edinburgh, 2010) at <http://www.law.ed.ac.uk/file_download/communities/245_tj%20macintyre%20-%20internet%20filtering-%20implications%20of%20the%20cleanfeed%20system.pdf>, accessed 29 February 2012

Moore, T. and Clayton, R., 'The Impact of Incentives on Notice and Take Down', (Cambridge: University of Cambridge, 2008) at <http://www.cl.cam.ac.uk/~rnc1/takedown.pdf>, accessed 05 July 2010

Morgan, B. and Yeung, K., *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007)

Moyser, G., 'Non-Standardized Interviewing in Elite Research', in Robert G. Burgess (ed.), *Studies in Qualitative Methodology: conducting qualitative research* (1; London: Jai Press, 1988), 109-36

Mueller, M., *Rulling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, MA: MIT Press, 2002)

Murray, A., *The regulation of cyberspace*: control in the online environment (1st edn.; Milton Park, Abingdon, UK ; New York, NY: Routledge-Cavendish, 2006)

Murray, A., 'Symbiotic Regulation', *The John Marshall Journal of Computer & Information Law,* XXVI(2) (2008), 208-28

Murray, A., *Information Technology Law: the law and society* (Oxford: OUP, 2010)

Murray, A., 'Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers', in Antonio Cassese (ed.), *Realizing Utopia: The Future of Internacional Law* (Oxford: OUP, 2012), 496-507

Murray, A. and Scott, C., 'Controlling the New Media: Hybrid Responses to New Forms of Power', *Modern Law Review,* 65 (2002), 491

Nelken, D., 'Whom can you trust? The Future of Comparative Criminology', in David Nelken (ed.), *The Futures of Criminology* (London: Sage Publications, 1994), 220-43

Nelken, D., 'Comparing Criminal Justice', in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology* (3rd edn.; Oxford: OUP, 2007), 139-57

Newburn, T., *Permission and Regulation: law and morals in post-war Britain* (London: Routledge, 1992)

Newey, A., 'Freedom of expression: censorship in private hands', in Liberty (ed.), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (London: Pluto Press, 1999)

Newland, E., et al., 'Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users', (Cambridge, MA: The Berkman Center for Internet & Society and The Center for Democracy & Technology, 2011) at <http://cyber.law.harvard.edu/node/7080>, accessed 28 December 2011

Noman, H. and York, J., 'West Censoring East: The Use of Western Technologies by Middle East Censors 2010-2011', (Toronto, Otawa and Stanford: Opennet Initiative, 2011)

Nunziato, D., *Virtual freedom: net neutrality and free speech in the Internet age* (Stanford: Stanford University Press, 2009)

O'Donnell, I. and Milner, C., *Child pornography: crime, computers and society* (Devon: Willan Publishing, 2007)

Ogus, A., 'Rethinking Self-Regulation', *Oxford Journal of Legal Studies,* 15(1) (1995), 97-108

Oliveira, T. and Reis, F., *Pornografia Infantil na Internet: o enfrentamento no Brasil (unpublished)* (Salvador-BA, Brasil: CEDECA-BA, 2006) 104p

ONI, 'Internet Filtering in China', OpenNet Initiative, 2009) at <http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf>, accessed 04 June 2010

Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press, 2009)

Oswell, D., 'When Images Matter: Internet Child Pornography, Forms of Observation and an Ethics of the Virtual', *Information, Communication and Society,* 9(2) (2006), 244-65

Oswell, D., 'Media and Communications Regulation and Child Protection: An Overview of the Field', in Sonia Livingstone and Kirsten Drotner (eds.), *International Handbook of Children, Media and Culture* (London: Sage, 2008), 469-86

Parry, J., et al., 'Internet content filtering A Report to the Department of Communications, IT and the Arts. Version 1.0', Ovum, 2003) at <http://www.dbcde.gov.au/__data/assets/file/0016/10915/Ovum_Report_-_Internet_content_filtering.rtf.>, accessed 07 September 2011

Penfold, C., 'Village Idiot, or Wisest Person in Town? Internet Content Regulation in Australia', *University of Ottawa Law and Technology Journal,* 3(2) (2006), 333-52

Perritt Jr., H. H., 'Towards a hybrid regulatory scheme for the Internet', *University of Chicago Legal Forum,* (2001), 215-332

Petit, J., 'Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the sale of children, child prostitution and child pornography. E/CN.4/2005/78, 23 December 2004.', (New York: United Nations, 2004) at <http://www.unhcr.org/refworld/category,REFERENCE,UNCHR,,,42d66e480,0.html>, accessed 30 June 2010

Petley, J., 'Web Control', *Index on Censorship,* 38(1) (2009), 78-90

Pierre, J., 'Introduction: Understanding Governance', in Jon Pierre (ed.), *Debating Governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000)

Post, D., *In search of Jefferson's moose: notes on the state of cyberspace* (Oxford: OUP, 2009)

Post, D. and Johnson, D., 'Law and borders: the rise of law in cyberspace', *Stanford Law Review,* 48 (1996), 1367-75

Post, D. and Johnson, D., 'The New 'Civic Virtue' of the Internet: A Complex Systems Model for the Governance of Cyberspace', in C. Firestone (ed.), *The Emerging Internet (1998 Annual Review of the Institute for Information Studies)* (1998)

Price, M. and Verhulst, S., 'In the search of the self: Charting the course of self-regulation on the Internet in a global environment', in Chris Marsden (ed.), *Regulating the Global Information Society* (London: Routledge, 2000), 57-78

Price, M. and Verhulst, S., *Self Regulation and the Internet* (The Hage, The Netherlands: Kluwer Law International, 2005)

Prior, L., 'Following Foucault's Footsteps: text and context in qualitative research', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 63-77

Przeworski, A. and Teune, H., *The Logic of Comparative Social Inquiry* (London: Wiley-Interscience, 1970)

Quayle, E., Loof, L., and Palmer, T., 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the III World Congress against Sexual Exploitation of Children and Adolescents', (Bangkok: ECPAT International, 2008) at <http://www.childcentre.info/public/Thematic_Paper_ICTPsy_ENG.pdf>, accessed 09 June 2010

Raab, C. and De Hert, P., 'The Regulation of Technology: Policy Tools and Policy Actors', *Tilburg University Legal Studies Working Paper No. 004/2007; TILT Law & Technology Working Paper Series No. 003/2007* (The Nederlands: Tilburg University, 2007)

Reed, C., *Internet Law: Text and Materials* (2nd edn.; Cambridge: Cambridge University Press, 2004)

Reed, C., *Making Laws for Cyberspace* (Oxford: OUP, 2012)

Reifschneider, E. and Reis, A., 'Pesquisa sobre Pornografia Infantil na Internet – Brasil. Proyecto sobre Tráfico de Niños, Pornografia Infantil en Internet y Marcos Normativos en el Mercosur, Bolívia e Chile', (Montevideo-Uruguay: Instituto Interamericano Del Niño, 2004) at <http://www.iintpi.net/informes/index.php>, accessed 25 May 2005

Reiner, R., *The Politics of the Police* (3rd edn.; Oxford: OUP, 2000)

Reis, F., 'Internet Hotlines Fighting Online Child Pornography: a comparative study between Brazil and England.', (The University Of Sheffield, 2003), at <http:// www.fabiorei.com> accessed 07 June 2010

Rhodes, R. A. W., *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Buckingham: Open University Press, 1997)

Rhodes, R. A. W., 'Governance and Public Administration', in Jon Pierre (ed.), *Debating Governance: Authority, Steering, and Democracy* (Oxford: OUP, 2000)

Roberts, H., Zuckerman, E., and Palfrey, J., '2007 Circumvention Landscape Report: Methods, Uses, and Tools', The Berkman Center for Internet & Society at Harvard University, 2009) at <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ 2007_Circumvention_Landscape.pdf>, accessed 04 June 2010

Roland, G., 'The Political Economy of Transition', *Journal of Economic Perspectives,* 16(1) (2002), 29-50

Ruggiero, V. and et al., 'Towards a European Criminological Community', in Ruggiero and et al. (eds.), *The New European Criminology: Crime and Social Order in Europe* (London: Routledge, 1998), 1-15

Russell, A. L., "Rough Consensus and Running Code' and the Internet-OSI Standards War', *IEEE Annals of the History of Computing,* 28(3) (2006), 48-61

Samuelson, P., 'Five Challenges for Regulating the Global Information Society', in Chris Marsden (ed.), *Regulating the Global Information Society* (London: Routledge, 2000)

Scott, C. and McIntyre, T., 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008)

Scott, J., *A matter of record: documentary sources in social research* (Cambridge: Polity, 1990)

Shapiro, A., *The control revolution: how the Internet is putting individuals in charge and changing the world we know* (New York: PublicAffairs, 1999)

Smelser, N. J., 'The Methodology of Comparative Analysis', in Donald P. and Osherson Warwick, Samuel (ed.), *Comparative Research Methods* (Englewood Cliffs, N.J.: Prentice-Hall, 1973), 3-41

Solum, L. B., 'Models of Internet Governance', in Lee A. Bygrave and John Bing (eds.), *Internet Governance: Infrastructure and Institution* (Oxford: OUP, 2009), 48-91

Spar, D., *Ruling the Waves: From the Compass to the Internet, a History of Business and Politics along the Technological Frontier* (New York: Harcourt, 2001)

Spinello, R., *Regulating cyberspace: the policies and technologies of control* (Westport, Conn.: Quorum Books, 2002)

Stalla-Bourdillon, S., 'Chilling ISPs... when private regulators act without adequate public framework...', *Computer Law & Security Review,* 26 (2010), 290-7

Star, A. (ed.), *Open Secrets: Wikileaks, War, and American Diplomacy (The New York Times)* (Grove Press, 2011)

Stenning, P., 'Powers and Accountability of Private Police', *European Journal on Criminal Policy and Research,* 8 (2000), 325-52

Stirton, L. and Lodge, M., 'Transparency Mechanisms: Building Publicness into Public Services', *Journal of Law and Society,* 28(4) (2001), 471-89

Stol, W., et al., 'Governmental filtering of websites: The Dutch case', *Computer Law & Security Review,* 25 (2009), 251-62

Sunstein, C., *Republic.com* (Princeton and Oxford: Princeton University Press, 2001)

Taylor, M. and Quayle, E., *Child Pornography: an Internet Crime* (New York, NY: Brunner-Routledge, 2003)

Thomas, D. and Loader, B., 'Introduction - Cybercrime: law enforcement, security, and surveillance in the information age', in Douglas Thomas and Brian Loader (eds.), *Cybercrime: law enforcement, secutiry, and surveillance in the information age* (London: Routledge, 2000), 1-13

Thompson, M., 'The Insensitive Internet – Brazil and the Judicialization of Pain', *unpublished,* (2010)

Thompson, M., 'Problemas Fundamentais do Marco - Marcelo Thompson @ Cultura Digital', (Brasília-DF, Brasil, 2010) at <http://culturadigital.br/marcelothompson/>, accessed 13 March 2012

Trebilcock, M., et al., 'The Choice of Governing Instrument', (Ottawa: Canadian Government Pub. Centre, 1982) at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997355>, accessed 12 July 2012

UNESCO (ed.), *Inocência em Perigo: abuso sexual de crianças, pornografia infantil e pedofilia na Internet* (São Paulo: UNESCO, Garamound and ABRANET, 1999)

UNODC, 'The Globalization of Crime: a transnational organized crime threat assessment', (Vienna: United Nations Office on Drugs and Crime, 2010) at <http://www.unodc.org/

documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf>, accessed 13 March 2012

Vagg, J., 'Context and Linkage: Reflections on Comparative Research and Internationalism in Criminology', *British Journal of Criminology,* 33(4) (1993), 541-54

Villeneuve, N., 'Barriers to cooperation: An analysis of the origins of international efforts to protect children online', in Ronald J. Deibert, et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010), 59-70

Walden, I., 'Criminal Content and Control', in David Goldberg, Gavin Sutter, and Ian Walden (eds.), *Media Law and Practice* (Oxford: Oxford University Press, 2009), 427-62

Walden, I., 'Porn, Pipes and the State: Censoring Internet Content', *The Barrister*, (2010) at <http://www.barristermagazine.com/archive-articles/issue-46/porn,-pipes-and-the-state:-censoring-internet-content.html> accessed 24 May 2012

Wall, D., 'Policing and the Regulation of the Internet', *Criminal Law Review. December Special Edition: Crime, Criminal Justice and the Internet,* (1998)

Wall, D., *Cyberspace crime* (Aldershot: Ashgate Dartmouth, 2003)

Wall, D., *Cybercrime: the transformation of crime in the information age* (Cambridge: Polity Press, 2007)

Wall, D., 'Cybercrime and the Culture of Fear: social science fiction and the production of knowledge about cybercrime', *Information, Communication and Society,* 11(6) (2008), 861-84

Wall, D., 'Criminalising cyberspace: the rise of the Internet as a 'crime problem'', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 88-103

Watson, R., 'Ethnomethodology and Textual Analysis', in David Silverman (ed.), *Qualitative Research: Theory, Method and Practice* (London: Sage Publications, 1997), 80-97

Weber, R., *Regulatory models for the online world* (New York: Kluwer Law International, 2002)

Weiser, P., 'The Future of Internet Regulation', *University of Colorado Law Legal Studies Research Paper No. 09-02,* (2009)

Williams, K., 'Transnational developments in Internet law', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 466-91

Wilson, M., 'Asking Questions', in Victor Jupp and Roger Sapsford (eds.), *Data Collection and Analysis* (London: Sage Publications, 1996), 94-120

Wolak, J., Mitchell, K., and Finkelhor, D., 'Child Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study', *National Center for Missing and Exploited Children*, 2005) at <http:// www.missingkids.com/en_US/publications/NC144.pdf>, accessed 07 June 2010

Wright, A., 'Australia: A Case Study on Internet Content Regulation', Australian Broadcasting Authority, 2002) at <http://www.acma.gov.au/webwr/aba/newspubs/speeches/ documents/aw_unesco_paper.pdf>, accessed 22 August 2011

Wu, T., *The Master Switch: The Rise and Fall of Information Empires* (Digital Kindle edn.; London: Atlantic Books, 2010)

Wykes, M. and Harcus, D., 'Cyber-terror: construction, criminalisation and control', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 214-27

Yar, M., 'The private policing of Internet crime', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (Devon: Willan Publishing, 2010), 546-61

Yeung, K., 'Towards an Understanding of Regulation by Design', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008)

Yin, R. K., *Case Study Research: Design and Methods* (4th Digital Kindle edn.; Los Angeles: Sage, 2009)

Zedner, L., 'Policing Before and After the Police: the historical antecedents of contemporary crime control', *British Journal of Criminology,* 46 (2006), 78-96

Zittrain, J., 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', in Adam Thierer and C. Wayne Crews Jr (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: CATO Institute, 2003), 13-31

Zittrain, J., 'A History of Online Gatekeeping', *Harvard Journal of Law & Technology,* 19(2) (2006), 253

Zittrain, J., 'Internet Filtering: The Politics and Mechanisms of Control', in Ronald Deibert, et al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), 29-56

Zittrain, J., 'Perfect Enforcement on Tomorrow's Internet', in Roger Brownsword and Karen Yeung (eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008)

Zittrain, J., *The future of the internet - and how to stop it* (New Haven, CT: Yale University Press, 2009)

Zittrain, J., 'The Personal Computer Is Dead', *The Future of the Internet and How to Stop It* (2011) at <http://futureoftheinternet.org/blog> Accessed 29 December 2011

Zittrain, J. and Edelman, B., 'Empirical Analysis of Internet Filtering in China', *IEEE Internet Computing,* (November 2002 2003)

Zittrain, J. and Palfrey, J., 'Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet', in Ronald Deibert, et al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), 103-22

Zuckerman, E., 'Intermediary censorship', in Ronald J. Deibert, et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010)

5 CONFERENCES

'1st World Congress against Commercial Sexual Exploitation of Children. Declaration and Agenda for Action.', (Stockholm: World Congress against CSEC, 1996) at <http://www.csecworldcongress.org/en/stockholm/index.htm>, accessed 18 April 2011

'2nd World Congress against Commercial Sexual Exploitation of Children. Yokohama Global Commitment', (Yokohama: World Congress against CSEC, 2001) at <http://www.csecworldcongress.org/en/yokohama/index.htm>, accessed 18 April 2011

CEDECA-BA, 'Pornografia Infanto-juvenil na Internet: Uma Violação aos Direitos Humanos', at <http://www.cedeca.org.br/publicacoes/conferencia.pdf>, accessed 18 April 2011

ECPAT, 'Child Pornography and the Internet Expert's Meeting. 28-29 May 1998.', (Lyon: ECPAT International, 1998) at <http://www.ecpat.net/eng/Ecpat_inter/projects/preventing_pornography/prevent.asp>, accessed 13 May 2005

Reis, F., 'Relatório sobre a Mesa-redonda contra a Pedofilia na Internet', (Salvador-BA: CEDECA-BA, 2000) at <http://www.fabiorei.com>, accessed 18 April 2011

UN, 'Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, 12-19 April 2010)', at <http://www.unodc.org/unodc/en/crime-congress/crime-congresses.html>, accessed 04 December 2011

UNESCO, 'Expert's Meeting. 18-19 Jan 1999.', (Paris: UNESCO, 1999) at <http://www.unesco.org/webworld/child_screen/conf_index.html>, accessed 13 May 2005

UNESCO, 'Fórum Brasileiro de Ética pela Infância e Adolescência na Internet: ForÉtica-BR', (Brasilia-DF: UNESCO BRASIL, 1999) at <http://www.dialdata.com.br/foretica>

WSIS, 'Working Group on Internet Governance: Report From the Working Group on Internet Governance', World Summit on the Information Society, at http://www.itu.int/wsis/docs2/pc3/html/off5/index.html, 2005) at <http://www.itu.int/wsis/index.html>

6 WEBSITES

'Meldpunt Kinderporno op internet', at <http://www.meldpunt-kinderporno.nl/EN/default.htm>, accessed 29 February 2012

'Portal Kids', at <http://www.portalkids.org.br/>, accessed 25 April 2011

'Virtual Globe Taskforce', at <http://www.virtualglobaltaskforce.com/>, accessed 09 August 2010

'Mobile Alliance Against Child Sexual Abuse Content', *GSM World,* 2008 at <http://www.gsmworld.com/newsroom/press-releases/2008/775.htm>, accessed 09 July 2011

'Friendly Runet Foundation', at <http://hotline.friendlyrunet.ru/?l=en>, accessed 28 May 2012

'Attorney-General's Department - Australian Government', at <http://www.ag.gov.au/>, accessed 19 September

'The European Financial Coalition against Commercial Sexual Exploitation of Children Online', at <http://www.ceop.police.uk/efc/>, accessed 26 May 2011

ABRANET, 'Associação Brasileira de Internet', at <http://www.abranet.org.br/>, accessed 30 August 2010

ABRAPIA, 'Do Marco Zero a Uma Política Pública Proteção à Criança e ao Adolescente', (Rio de Janeiro-RJ: ABRAPIA: Associação Brasileira Multiprofissional de Proteção à Infância e à Adolescência, 2003) at <http://www.abrapia.org.br>, accessed 12 June 2004

ACMA, 'Australian Communications and Media Authority - The ACMA is a statutory authority within the federal government portfolio of Broadband, Communications and the Digital Economy', at <http://www.acma.gov.au>, accessed 28 March 2010

ACMA, 'The ACMA Hotline: combating child sexual abuse', at <http://www.acma.gov.au/hotline>, accessed 01 September 2011

ACPO, 'AntiChildPorn.Org', at <http://www.antichildporn.org/overview.html>, accessed 29 June 2010

APL, 'The Anti-Pornography League', at <http://www.angelfire.com/art/antipornography/>, accessed 29 June 2010

CDHM, 'Comissão de Direitos Humanos e Minorias da Câmara dos Deputados', at <http://www2.camara.gov.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm>, accessed 27 April 2011

CEDECA-BA, 'HotlineBR CEDECA-BA', at <http://www.hotlinebr.org.br>, accessed 03 November 2005

CEDECA-BA, 'Centro de Defesa da Criança e do Adolescente da Bahia', at <http://www.cedeca.org.br>, accessed 31 August 2010

CEOP, 'Child Exploitation and Online Protection', at <http://www.ceop.gov.uk/>, accessed 29 February 2012

CGI, 'Comitê Gestor da Internet no Brasil', at <http://www.cgi.br/>, accessed 14 March 2012

CIRCAMP, 'Cospol Internet Related Child Abusive Material Project', at <http://circamp.eu>, accessed 30 June 2010

CONAR, 'Conselho Nacional de Autorregulamentação Publicitária', at <http://www.conar.org.br/>, accessed 30 August

Cyberangels, 'Cyberangels', at <http://www.cyberangels.org/about.php>, accessed 29 June 2010

DBCDE, 'Department of Broadband, Communications and the Digital Economy', at <http://www.dbcde.gov.au/>, accessed 11 September 2011

DPF, 'Polícia Federal', at <http://www.dpf.gov.br/>, accessed 25 April 2011

EFA, 'Electronic Frontiers Australia', at <http://www.efa.org.au/>, accessed 22 August 2011

EUROISPA, 'European Association of Internet Service Providers', at <http://www.euroispa.org/>, accessed 29 June 2010

EUROPOL, 'CIRCAMP - COSPOL Internet Related Child Abusive Material Project', at <http://www.europol.europa.eu/index.asp?page=InternetRelatedChildAbusiveMaterialProject>, accessed 05 August 2010

FCACP, 'Financial Coalition Against Child Pornography', at <http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703>, accessed 09 June 2010

ICANN, 'Internet Corporation for Assigned Names and Numbers', (updated 01 February 2008) at <http://www.icann.org/>

IIA, 'Internet Industry Association: policy, advocacy and representation for Australian business', at <http://www.iia.net.au/>, accessed 22 August 2011

INHOPE, 'International Association of Internet Hotlines', at <https://www.inhope.org/>, accessed 28 March 2010

INTERPOL, 'Interpol', at <http://www.interpol.int/>, accessed 09 August 2010

ISPA, 'Internet Service Providers' Association UK', at <http://www.ispa.org.uk/home/>, accessed 29 June 2010

IWF, 'Internet Watch Foundation - The UK Hotline for reporting illegal online content', at <http://www.iwf.org.uk/>, accessed 08 June 2011

ItXtreme, 'ItXtreme Family Internet', at <http://www.itxtreme.com.au/>, accessed 07 September 2011

Miranda, A. and Miranda, R., 'Campanha Censura.Com', at <http://www.censura.com.br/>, accessed 25 April 2011

MPF-SP, 'Grupo de Combate aos Crimes Cibernéticos', at <http://www.prsp.mpf.gov.br/noticias-prsp/crimes-ciberneticos>, accessed 18 April 2011

MPF-SP, 'Procuradoria da República em São Paulo. Grupo de Combate aos Crimes Cibernéticos', at <http://www.prsp.mpf.gov.br/noticias-prsp/crimes-ciberneticos>, accessed 27 April 2011

NCMEC, 'The CyberTipline', at <http://www.missingkids.com/cybertip/>, accessed 19 April 2011

ORKUT, 'A social networking system and discussion site operated by Google Inc.', at <http://www.orkut.com>, accessed 30 August 2010

Pedowatch, 'Pedowatch.Org', at <http://www.aboutus.org/PedoWatch.org>, accessed 29 June 2010

SAFERNET, 'Safernet Brasil', at <http://www.safernet.org.br/site/>, accessed 28 March

Wikipedia, 'Wikipedia: a multilingual, web-based, free-content encyclopedia project based on an openly editable model.', at <http://en.wikipedia.org/wiki/Main_Page>, accessed 09 July 2011

Webshield, 'Webshield: Australia's First Content Filtered Internet Service Provider', at <http://www.webshield.net.au/>, accessed 07 September 2011

7 OTHER REFERENCES

'A-Gs' media release', (Australia, 1997) at <http://web.archive.org/web/20070608032701/http://www.ag.gov.au/www/attorneygeneralHome.nsf/Alldocs/086E324FF9AA0947CA256B53000F1B19?OpenDocument> Accessed 05 March 2012

'Minister's media release', (1997) at <http://web.archive.org/web/20031124104143/http://www.dcita.gov.au/Article/0,,0_1-2_1-4_10366,00.html> Accessed 05 March 2012

'Minister's media release announcing the introduction of the 1999 Bill', (Australia, 1999) at <http://web.archive.org/web/20020821095852/http://www.dcita.gov.au/Article/0,,0_1-2_1-4_13762,00.html > Accessed 05 March 2012

'AFP successfully combats child sex exploitation', *Platypus Magazine*, (2009) at <http://www.afp.gov.au/~/media/afp/pdf/1/11-child-protection.ashx> accessed 07 March 2012

'Man cleared over Girls Aloud blog', *BBC News,* 29 June 2009 at <http://news.bbc.co.uk/1/hi/england/tyne/8124059.stm>, accessed 06 August 2010

'Orkut Continues to Lead Brazil's Social Networking Market, Facebook Audience Grows Fivefold', (São Paulo-SP: comScore, 2010) at <http://www.comscore.com/Press_Events/Press_Releases/2010/10/>, accessed 26 April 2011

'Cispa cybersecurity bill passed by House of Representatives', *The Guardian,* 27 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/27/cispa-cybersecurity-bill-passed-senate>, accessed 01 May 2012

Adetunji, J., 'Dog microchips expected to be made compulsory', *The Guardian,* 21 April 2012, sec. World News at <http://www.guardian.co.uk/world/2012/apr/21/dog-microchips-compulsory?newsfeed=true>, accessed 05 May 2012

Ahmed, M., 'Police warn over rise of teenage 'sexting' trend', *The Times,* 05 August 2009 at <http://technology.timesonline.co.uk/tol/news/tech_and_web/article6738532.ece>, accessed 14 May 2011

Arthur, C., 'I want the iPad porn-free, says Apple's Steve Jobs: Apps for the new iPad have had to self-censor ', *The Guardian,* Tuesday 25 May 2010 2010

Arthur, C., 'iPhone keeps record of everywhere you go', *Guardian News and Media Limited,* 20 April 2011 at <http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears>, accessed 21 April 2011

Arthur, C. and others, 'Google, Microsoft, Yahoo and AOL back US 'consumer privacy bill of rights'', *The Guardian,* 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/feb/23/google-microsoft-yahoo-aol-privacy>, accessed 22 March 2012

Ball, J., 'Me and my data: how much do the internet giants really know?', *The Guardian,* 22 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/22/me-and-my-data-internet-giants>, accessed 01 May 2012

Bamford, J., 'The Black Box', *Wired Magazine*, April (2012) at <http://www.wired.com> accessed 03 April 2012

Beaumont, P., 'US appoints first cyber warfare general', *The Observer,* 23 May 2010 at <http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general>, accessed 24 Aug 2010

Best, J., 'AU$189m govt porn blocking plan unveiled', *ZDNet,* 10 August 2007 at <http://www.zdnet.com.au/au189m-govt-porn-blocking-plan-unveiled_print-339281091.htm>, accessed 25 September 2011

Bingemann, M., 'ACMA blacklist leaked on the internet', *The Australian,* 19 March 2009, sec. Australian IT at <http://www.theaustralian.com.au/news/acma-blacklist-leaked-on-the-internet/story-e6frgb5x-1225700508594>, accessed 24 June 2011

Booth, R., 'Government plans increased email and social network surveillance', *The Guardian,* 01 April 2012, sec. World News at <http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance>, accessed 01 May 2012

Branigan, T., 'Facebook may 'block content' claim as speculation grows over entry into China', *Guardian News and Media Limited,* 20 April 2011 at <http://www.guardian.co.uk/technology/2011/apr/20/facebook-considers-censorship-claim-china>, accessed 21 April 2011

Carr, J., 'BlackBerry has some explaining to do', *Desiderata* (2011) at <https://johnc1912.wordpress.com/2011/12/09/blackberry-has-some-explaining-to-do/> Accessed 28 December 2011

Carr, J., 'Microsoft attacks online child pornography', *Desiderata* (2011) at <http://johnc1912.wordpress.com/2011/07/05/microsoft-attacks-online-child-pornography-3/> Accessed 28 December 2011

Carr, J., 'Hotlines and INHOPE: time to take stock?', *Desiderata* (2012) at <http://johnc1912.wordpress.com/2012/03/02/hotlines-and-inhope-time-to-take-stock-2/> Accessed 22 March 2012

Carr, J., 'Getting it wrong', *Desiderata* (2012) at <http://johnc1912.wordpress.com/2012/07/15/getting-it-wrong/> Accessed 16 July 2012

Collin, J., 'Leaked Government blacklist confirms worst fears' *Electronic Frontiers Australia*; <http://www.efa.org.au/2009/03/19/leaked-government-blacklist-confirms-worst-fears/> accessed 09 August 2010

Davies, C., 'The hidden censors of the internet', *Wired UK*, (2009) at <http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet?page=all> accessed 13 July 2010

Drummond, D., 'Greater transparency around government requests', *The Official Google Blog* (2010) at <http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html> Accessed 24 Aug 2010

Dredge, S., 'Apple bans satirical iPhone game Phone Story from its App Store', *The Guardian,* 2011, sec. Apps Blog at <http://www.guardian.co.uk/technology/appsblog/2011/sep/14/apple-phone-story-rejection>, accessed 28 December 2011

Elmer-DeWitt, P., 'Online Erotica: On a Screen Near You', *Time*, (1995) at <http://www.time.com/time/magazine/article/0,9171,983116,00.html> accessed 08 July 2010

Elmer-Dewitt, P., 'First Nation in Cyberspace', *Time Magazine*, 49 (1996) at <http://www.chemie.fu-berlin.de/outerspace/Internet-article.html> accessed 22 March 2012

Gallagher, R. and Syal, R., 'Met police using surveillance system to monitor mobile phones', *The Guardian,* 30 October 2011, sec. UK News at <http://www.guardian.co.uk/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance>, accessed 28 December 2011

Halliday, J., 'JailbreakMe released for Apple devices', *Guardian Technology Blog* (2010) at <http://www.guardian.co.uk/technology/blog/2010/aug/02/jailbreakme-released-apple-devices-legal> Accessed 12 August 2010

Halliday, J., 'BT and TalkTalk denied Digital Economy Act appeal', *The Guardian,* 12 June 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jun/21/bt-talk-talk-digital-economy-act>, accessed 21 June 2011

Halliday, J., 'Digital Economy Act will cost nearly £6m', *The Guardian,* 17 June 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jun/17/digital-economy-act-cost>, accessed 20 June 2011

Halliday, J., 'Google boss: anti-piracy laws would be disaster for free speech', *The Guardian,* 18 May 2011 at <http://www.guardian.co.uk/technology/2011/may/18/google-eric-schmidt-piracy>, accessed 07 June 2011

Halliday, J., 'Google faces pressure to block filesharing sites', *The Guardian,* 13 September 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/sep/13/google-block-filesharing-sites>, accessed 28 December 2011

Halliday, J., 'British ISPs will block The Pirate Bay within weeks', *The Guardian,* 30 April 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/apr/30/british-isps-block-pirate-bay>, accessed 01 May 2012

Halliday, J., 'BT and TalkTalk lose challenge against Digital Economy Act', *The Guardian,* 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/mar/06/internet-provider-lose-challenge-digital-economy-act>, accessed 22 March 2012

Halliday, J., 'Pornography online: David Cameron to consider 'opt in' plan', *The Guardian,* 2012, sec. Technology at <http://www.guardian.co.uk/technology/2012/may/04/pornography-online-cameron-opt-in-plan?newsfeed=true>, accessed 05 May 2012

Hogge, B., 'Lessons and questions for the IWF', at <http://www.openrightsgroup.org/blog/2008/lessons-and-questions-for-the-iwf>, accessed 07 June 2011

IIA, 'Internet industry moves on blocking child pornography', *Internet Industry Association Australia,* 2011 at <http://www.iia.net.au/index.php/all-members/892-internet-industry-moves-on-blocking-child-pornography.html>, accessed 07 September 2011

Jacobs, C., 'Conroy: Filter alive and kicking', *Electronic Frontiers Australia,* 27 May 2011 at <http://www.efa.org.au/2011/05/27/filter-alive-and-kicking/>, accessed 01 September 2011

Kaye, L., 'Blocking Newzbin2 paves the way for internet censorship', *The Guardian,* 29 July 2011, sec. Liberty Central at <http://www.guardian.co.uk/commentisfree/libertycentral/2011/jul/29/newzbin2-internet-censorship-bt>, accessed 28 December 2011

Kravets, D., 'Communications Decency Act Tipping Under Cuomo Kid-Porn Accord', *Wired,* 2008, sec. Threat Level at <http://www.wired.com/threatlevel/2008/06/analysis-commun/>, accessed 28 December 2011

LeMay, R., 'Filter delayed while RC is reviewed', *ZDNet,* 09 July 2010 at <http://www.zdnet.com.au/filter-delayed-while-rc-is-reviewed-339304437.htm>, accessed 22 August 2011

LeMay, R., '5 reasons to worry about the Interpol filter', *ZDNet,* 11 July 2011 at <http://www.zdnet.com.au/5-reasons-to-worry-about-the-interpol-filter-339318271.htm>, accessed 12 September 2011

LeMay, R., 'Does the filter breach user agreements?', *ZDNet,* 12 July 2011 at <http://www.zdnet.com.au/does-the-filter-breach-user-agreements-339318375.htm>, accessed 12 September 2011

LeMay, R., 'ISPs don't have to collect voluntary filter data', *Delimiter*, (2011) at <http://delimiter.com.au/2011/10/26/isps-dont-have-to-collect-voluntary-filter-data/> accessed 06 March 2012

LeMay, R., 'We'll filter when the law says: Internode', *ZDNet,* 05 July 2011 at <http://www.zdnet.com.au/well-filter-when-the-law-says-internode-339317922.htm>, accessed 12 September 2011

Marling, C., 'Interview with Sarah Robertson, director of communications for the Internet Watch Foundation', *Broadband Genie,* 08 April 2009 at <http://www.broadbandgenie.co.uk/blog/full-internet-watch-foundation-interview-20090408>, accessed 07 June 2011

Martins, R., 'Criminosos agem impunes no Orkut', *O Estado de São Paulo,* 06 February 2006

Moses, A., 'Leaked Australian blacklist reveals banned sites', *The Sydney Morning Herald,* 19 March 2009, sec. Technology at <http://www.smh.com.au/articles/2009/03/19/1237054961100.html>, accessed 24 June 2011

Moses, A., 'Web censorship plan heads towards a dead end', *The Sydney Morning Herald,* 26 February 2009, sec. Technology at <http://www.smh.com.au/articles/2009/02/26/1235237810486.html>, accessed 07 September 2011

Naughton, J., 'Smartphones can do everything – except safeguard the web', *The Guardian,* 17 July 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/jul/17/smartphones-internet-corporate-threat>, accessed 28 December 2011

Ozimek, J., 'Scorpions tale leaves IWF exposed: 'Look, that regulator isn't wearing any clothes'', *The Register,* 09 December 2008 at <http://www.theregister.co.uk/2008/12/09/iwf/>, accessed 20 June 2011

Ozimek, J., 'A censorship model', *The Guardian,* 02 August 2009, sec. Global at <http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/02/internet-censor>, accessed 20 June 2011

Ozimek, J., 'IWF chief: We don't need crusaders', *The Register,* 08 September 2009 at <http://www.theregister.co.uk/2009/09/08/iwf_peter_robbins_interview/>, accessed 07 June 2011

Ozimek, J., 'The IWF: Charity disparity?', *The Register,* 20 February 2009, sec. Law at <http://www.theregister.co.uk/2009/02/20/iwf_charity/>, accessed 02 March 2012

Ozimek, J., 'Aus gov, ISPs book seats for firewall demolition: new filters to catch nasty stuff ', *The Register,* 23 August 2010 at <http://www.theregister.co.uk/2010/08/23/aus_firewall_isp/ >, accessed 22 August 2011

Quinn, B., '.xxx adult entertainment domain approved by internet regulators', *The Guardian,* 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/mar/19/xxx-domain-suffix-adult-entertainment>, accessed 20 July 2012

Regalado, A. and Delaney, K., 'Google Under Fire Over a Controversial Site: Racist Speech, Porn Stir Battle in Brazil; A 'Pandora's Box'', *The Wall Street Journal*, (2007), A1 at <http://online.wsj.com/article/SB119273558149563775.html> accessed 30 August 2010

Rivlin, G., 'Hate Messages on Google Site Draw Concern', *The New York Times,* 07 February 2005 at <http://www.nytimes.com/2005/02/07/technology/07orkut.html>, accessed 26 April 2011

Rushe, D., 'Facebook reaches deal with FTC over 'unfair and deceptive' privacy claims', *The Guardian,* 2011, sec. Technology at <http://www.guardian.co.uk/technology/2011/nov/29/facebook-ftc-privacy-settlement>, accessed 28 December 2011

Stone, B., 'Amazon Erases Orwell Books From Kindle', *The New York Times,* 2009, sec. Technology at <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?adxnnl=1&adxnnlx=1325158251-ts7AYblRq6cBBmaPrJP1SQ>, accessed 29 December 2011

Syal, R., Halliday, J., and Siddique, H., 'Theresa May defends email surveilance plans', *The Gardian,* 04 Aprii 2012, sec. UK Police at <http://www.guardian.co.uk/uk/2012/apr/03/theresa-may-email-surveillance-plans>, accessed 04 April 2012

Syal, R., Halliday, J., and Siddique, H., 'Theresa May defends email surveillance plans', *The Gardian,* 04 April 2012, sec. UK Police at <http://www.guardian.co.uk/uk/2012/apr/03/theresa-may-email-surveillance-plans>, accessed 04 April 2012

Taggart, S., 'Down Under Smut Goes Up Over ', *Wired Magazine,* 02 February 2000, sec. Politics : Law at <http://www.wired.com/politics/law/news/2000/02/34043>, accessed 22 August 2011

Tay, L., 'ICT industry all nostalgic for NetAlert', *itNews - For Australian Business,* 08 July 2012 at <http://www.itnews.com.au/Tools/Print.aspx?CIID=219281>, accessed 25 September 2011

Thompson, B., 'Google censoring web content', *BBC News (the billblog),* 25 October 2002 at <http://news.bbc.co.uk/1/hi/technology/2360351.stm>, accessed 20 June 2011

Topping, A., 'G4S Olympic scandal: Ed Miliband calls for rethink of police outsourcing', *The Guardian,* 2012, sec. Politics at <http://www.guardian.co.uk/politics/2012/jul/19/g4s-olympic-ed-miliband-police>, accessed 20 July 2012

UNODC, 'Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime. Vienna, 17-21 January 2011', at <http://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html>, accessed 17 March 2012

Warden, P., 'iPhone Tracker', at <http://petewarden.github.com/iPhoneTracker/>, accessed 21 April 2011

Waters, D., 'Can Second Life regulate virtual sex?', *BBC News,* 2009 at <http://www.bbc.co.uk/blogs/technology/2009/04/can_second_life_regulate_virtu.html>, accessed 11 August 2010

Williams, C., 'Home Office backs down on net censorship laws', *The Register,* 16 October 2009 at <http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/>, accessed 20 June 2011

Williams, C., 'UK.gov to get power to force ISPs to block child porn ', *The Register,* 02 April 2009 at <http://www.theregister.co.uk/2009/04/02/eu_filtering_framework/>, accessed 20 June 2011

Williams, C., 'How Egypt shut down the internet', *The Telegraph,* 28 January 2011, sec. World News at <http://www.telegraph.co.uk/news/worldnews/africanandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html>, accessed 04 April 2012

Wintour, P., 'David Cameron to resist French plan for internet regulation: Nicolas Sarkozy calls for worldwide web controls at G8 summit, but Google chairman urges leaders to resist legislation', *The Guardian,* 24 May 2011 at <http://www.guardian.co.uk/technology/2011/may/24/david-cameron-resist-internet-regulation>, accessed 07 June 2011

Woods, J., 'Avatars and Second Life adultery: A tale of online cheating and real-world heartbreak', *Telegraph,* 2008 at <http://www.telegraph.co.uk/technology/3457828/Avatars-and-Second-Life-adultery-A-tale-of-online-cheating-and-real-world-heartbreak.html>, accessed 11 August 2010

Wyres, M., 'I'm dumping Telstra for the voluntary filter', *ZDNet Australia,* 24 June 2011 at <http://www.zdnet.com.au/im-dumping-telstra-for-the-voluntary-filter-339317382.htm>, accessed 12 September 2011

Zittrain, J., 'BlackBerry-22', *The Future of the Internet and How to Stop It* (2010) at <http://futureoftheinternet.org/blackberry-22> Accessed 12 August 2010

Zittrain, J., 'A fight over freedom at Apple's core', *Financial Times,* 03 February 2010 2010 at <http://www.ft.com/cms/s/2/fcabc720-10fb-11df-9a9e-00144feab49a.html?nclick_check=1>, accessed 14 December 2011

APPENDIX 1: COMPARATIVE TABLE OF CASE STUDIES

Comparative Table

			CASE STUDIES		
			Australia	*Brazil*	*United Kingdom (England and Wales)*
	PERIOD		*1990 - 2010*	*1990 - 2010*	*1978 - 2010*
LEGISLATION AND CASE LAW	***State-regulation***	Anti-child pornography criminal laws			
		definition of child porn	Generally the Cth has criminal jurisdictionover inter-state offences and States and territories over intra-state offence, but this is not so straighforward. The scope of the latter is broader. Section 473.1 of Criminal Code Act 1995 (Cth) amended in 2004, offences are in re to using or attempting to use a carrier service to be punishable at the Cth level (inter-state offences). There are variations across States and Territories	Sexually explicit or pornographic scenes depicting children or adolescents, ie any representation, by whatever means of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes (ECA art. 241-E). This is in line with the 2000 UN Optional Protocol. The criminal law is enforced uniformly across the country. The child depicted has to be real, non-fictitious and thus identifiable	POCA 1978: indecent photographs of a child, including films, copy os a photograph or film, negatives and positive versions, data stored in a computer,
		age of a child	A person under 18 (Cth) + variations across States and Territories	A person under the age of 18	A person under the age of 18 (after 2003, it was 16 before that)
		types of content	(States and Territories) photos, pseudo-photos, videos, cartoons, adult behaving as child, text and audio. The child can be real or computer-generated. (Cth) section 473.1 of the amended 1995 Code	Photos, pseudo-photos (ie modified or juxtaposed photos with real identifiable child), videos	Photographs, pseudo-photographs, adults conveying the impression of a child and non-photographic depictions (prohibited images of a child eg tracings, cartoons and drawings). The child can be real or computer-generated
		production	States and Territories. Cth if with the intention of using a carrier service to achieve this	Produce, reproduce, direct, photograph, film or register by any means child pornograhy	To take, permit to be taken, to make
		distribution	States and Territories. Cth if with the intention of using a carrier service to achieve this	Both the commercial (to sell or show with intent to sell) and non-commercial distribution (to offer, exchange, make available transmit, distribute, publish) are criminal offences	Both the commercial and non-commercial distribution are criminal offences: to distribute or show, to publish or cause to be publish any advertisement,
		intentional access	(Cth) to access or solicit	It is not criminalised, but 'to acquire' has been criminalised with the meaning of 'to buy'	Downloading or printing off can amount to a making or a possession offence. subject to mens rea. The 2011 EU Directive crimianlised the intentional access and promoted the website blocking measures
		possession	Qualified possession = with intention to distribute it via the carriage service (Cth) and mere possession (States and Territories)	The mere possession is a criminal offence since 2008	The mere possession was criminalised in 1988: prior to this only to have in possession with a view to being distributed
		penalties	Generally 15 years imprisonment (Cth)	From 01 to 08 years imprisonment depending on the offence	Harsher panalties were established in 2000
		extraterritorial	Yes to punish the Australian nationals and residents committing these offences abroad. Section 273.5 of the CCA 1995 as amended.	Not found	Not found
		liability of online intermediaries	Generally established via Cth law, which defines child pornography, hosting service and content service provider. See Criminal Code Act 1995 as amended in 2004. There are also provisions in the Broadcasting Services Act 1992 as amended	Established in the ECA as amended in 2008. These provisions only apply in re to child porn content. OIs exempt from criminal liability if unaware of the criminal content, but subject to criminal liability after notification (art. 241-A). No comprehensive legislative regulation of online intermediaires in relation to NTD (marco civil bil)	Established via the 2000 EU Commerce Directive. Safe harbour provisions (mere conduit, cache operations and content hosts). Crimina liability is subject to knowledge and control and no obligation to monitor or control content. The preservation of evidence is under the 2009 EU Data Retention Regulations

	Comparative Table			CASE STUDIES		
				Australia	***Brazil***	***United Kingdom (England and Wales)***
			defences	section 474.21 of CCA 1995 as amended: public benefit, law enforcemnt officer in duty, good faith	LEA and other organisations are not liable when they manipulate the child pornographic material for the purposes of notification	for possession: legitimate reason, unkown possession and unsolicited possession; the IWF is a relevant authority in 2003 following R. v Bowden
			investigatory powers of law enforcement bodies	Established by the Interception and Access Act 1979, and the Telecommunications Act 1997 both amended by the 2004 and 2007 Acts. a court order is needed to access the content of a communication. there is a memoranda of understanding settled between the ACMA and the Australian police forces	A court order is needed to access/intercept the contents of a communication but LEAs can obtain information about time, location, IP etc. upon request to the relevant OI	These are established via the Regulation of Investigatory Powers Act 2000. The RIPA 2000 allows the law enforcement bodies to request info from OIs about users without a court order; regulates the disclosure of electronic keys; fitting surveillance equipment onto OIs' networks. The gov has plans to review the law so as to extend these powers
	Multi-state regulation		2001 CoE Cybercrime Convention	No	No and there are no plans for that. The country is for the establishment of a new international UN-lead treaty that takes into account the views of a wider international community	Yes. It signed the treaty on 23 Nov 2001 and ratified it on 25 May 2011
			2000 UN Optional Protocol	Yes. It signed the treaty on 18 Dec 2001 and ratified it on 08 Jan 2007	Yes. It signed the treaty on 06 Sept 2000 and ratified it on 27 Jan 2004 without reservations	Yes. It signed the treaty on 07 Sep 2000 and ratified it on 20 Feb 2009
	PERIOD			*1990 - 2010*	*1999 - 2010*	*1990 - 2010*
	Key developments over time			BBS Task-force in 1994, ABA report 1996, Governmental proposal in 1997, Senate Select Committee in 1997, Proposal of regulatory framework by the Cth Gov, BSA 1992 amended in 1999 (applying the norms of Tv broadcast to the Internet), voluntary filtering scheme, call for a mandatory filtering scheme in 2007 (discussion is ongoing), anti-child porn criminal Cth laws amended in 2004, Operation Auxin in 2004, CoP registered in 2005, BSA 1992 amended again in 2007, CoP registered in 2008, voluntary ISP-level filtering implemented in 2011 by the IIA	International conferences after the late 1990s, establishment of Internet hotlines around early 2000s, self-regulation rhetoric never systematically implemented, criminal laws updated in 2003, creation of the Safernet in 2005, pressure from the MPF-SP and Safernet after 2005, a number of agreements with OIs are settled to take-down content hosted in the country, identify alleged offenders and preserve criminal evidence after 2005, Google has refused to cooperate, Senate Committee Inquiry launched in 2008, the Orkut case settled in 2008, criminal laws updated again in 2008, settlement with telcos in 2009, marco civil bill	Commercial Internet started to flourish in 1994, pseudo-photographs and making are outlawed in 1994, growing concerns over child porn available in newsgroups in 1996, police and gov put pressure on OIs to come up with a solution, Industry self-regulatory body (SafetyNet/IWF) was established in 1996, automated monitoring of newsgroups, websites grow in importance, EU Directive implemented in 2000 establishing safe harbour provisions and NTD framework. overseas URL blocking starts in 2004

	Comparative Table	CASE STUDIES		
		Australia	***Brazil***	***United Kingdom (England and Wales)***
REGULATORY FRAMEWORK	***Regulatory nature***	Co-regulation and complaint-based. The Cth government is the key actor: Cth statute (BSA 1992 as amended in 1999, 2004 and 2007) and Cth regulator ACMA, formerly ABA (state-regulation), self-regulation via CoP (voluntary filtering at the user and ISP-level) and memoranda of understanding (agreement) settled between the ACMA and the police forces. There are two key CoPs (2005 and 2008). The ACMA registers and monitors the CoP and can impose a standard of its own if necessary. It also operates a hotline that receives, investigates and forwards reports. The online intermediaires have no obligation to proactively monitor content	Middle-way between an incomplete state regulation of content and absent self-regulation. So the LEA settled agreements with online intermediaires. There is no comprehensive law to regulate the online intermediaires generally. NTD is based in law but only in relation to child pornography. The preservation of evidence and other measures have been established via agreements settled between the law enforcement authorities and ISPs - for identifying offenders and collecting evidence and IHPs/ICPs - for removing content, identifying offenders and collecting evidence with the help of the NGO Internet hotline and the Senate Committee Inquiry	Internet industry self-regulatory body IWF manages the take-down / blocking scheme / interface with OIs. Both the police and the government also play a role and established agreements with the IWF. The IWF has Board that have members or diferent society groups. The IWF acquired the status of relevant authority via legislation in 2003. The take-down of content hosted in the UK and the implementation of the URL blocking system is based on a voluntary agreement between the IWF and UK OIs that covers around 98% of the UK customer base. The 2011 EU Directive established rules for website blocking and intentional access. The blocking scheme is voluntary at the ISP-level - not legislated
	Scope: online material targeted	The online material is classified according to the categories applied to the film industry. See the 2005 Classification Code. Child pornography and other violent material are RC-rated. Other classifications include content considered inappropriate to minors (X18+, R18+, MA15+). These materials may be labelled prohibited or potential prohibited. RC and X18+ rated material are pot/prohibited material. R18+ and MA15+ may be also pot/prohibited material depending on RAS. Pot/prohibited content are included in the ACMA blocklist and the relevant online intermediary is notified according to the notification scheme. Child porn does not need to be classified prior to a notice being issued	Mainly child pornography but also incitement to racial hatred and religious intolerance either hosted in Brazil or hosted overseas but produced or distributed by a Brazilian resident	Child porn hosted anywhere, and both criminally obscene adult content and cartoon child porn hosted in the UK. Overseas URL Blocking only in re to child porn. Incetement to racial hatred was part of its remit only until 2011. The extreme pornographic content was included in its remit of obscene material in 2009 and cartoon child porn included in 2010. There has been pressure from the gov to include other types of contentin the blocklist
	Mechanics			
	Child pornography hosted domestically	Via notification to the Australian online intermediary and also the Australian police forces in the case of serious offences. Notifications are: final and interim take-down, service-cessation and link-deletion notices to Australian IHPs and ICPs. Police force notified according to the memoranda of understanding ie ACMA investigation is suspended whilst the police investigation takes place. Failure to take down the reported mterial is acriminal offence and may also result in heavy fees	Via notices of take-down issued mainly by the MPF-SP and the Safernet to the relevant ICPs and IHPs. Online payment systems are also notified about paid child pornography websites. These notifications lead to criminal investigation and further information is provided by the relevant OI to the LEAs	Notices of take-down and preservation of evidence request are issued by the IWF to relevant UK IHPs/ICPs - tougher measures (automated monitoring and take-down of entire newsgroups) were aplied to newsgroups in 2002; UK police force is notified by a request of investigation under the terms of an agreement; the relevant OI is contacted by phone; the website is monitored until content is removed. The IWF does not require the OI to do anything; it only puts them on notice and thus at risk of facing criminal liability

Comparative Table	CASE STUDIES		
	Australia	***Brazil***	***United Kingdom (England and Wales)***
Child pornography hosted overseas but accessed within the jurisdiction	Via notification to 'accredited' filter vendors and access-prevention notices to known ISPs. Website is included in the ACMA blocklist. Rules established by the 2005 CoP are: (notice to filter vendors, ISPs inform customers about the filters - voluntary filtering at the user-level). Notify a member of an Australian police force, and the INHOPE. More recently voluntary filtering of websites, not URLs, at the ISP-level using the Interpol blocklist (section 313 telco 1997 act?) but mandatory ISP-level filtering via legislation (?) is expected after the RC-rated content review but it is unclear how this scheme will be mplemented	Notifications are sent to partner-hotlines (if any) and to the Federal police via Interpol. Embassies are also notified. No evidence found about the use of blocklists (employed vountarily or otherwise) to block access to child pornographic content hosted overseas. Online payment systems also notified about paid websites hosted overseas	The partner hotline in that country, if any, is notified. The Interpol is also notified. The overseas hosts are notified as well. The URLs are added to the IWF blocklist which are passed on to member UK ISPs (inc. mobile operators and search engines) under the terms of a voluntary agreement (98% coverage). (A notification is sent to ICANN to unregister the relevant domain name. The online payment systems are also notified in the case of paid websites.) The URL is monitored until content is removed. The implementation of the blocklist is voluntary and at the discretion of the ISP which pay a membership montlhy fee to be part of the scheme
Is the pro-active content monitoring and disclosure of personal data by the OIs regulated to prevent abuses?	No. Access to the blocklisted websites are not traced back according to the police force	No	No
Complaints and content analysis (human or automated, ex ante or post) in re child porn	Complaint-based mechanism (by members of the public or the police to the ACMA or relevant OI) but there is also proactive content monitoring (human-based or automated) performed by the ACMA and OIs. Some OIs offer filtered access to the Internet commercially	Under the pressure of law enforcement agencies the OIs are performing proactive content monitoring via automated filtering and human analysis. There is neither legislative oversight nor are legislative safeguards to protect against abuses. Opaque private censorship	IWF work is generally reactive but there is indication of proactive monitoring. In addition, the IWF manages the blocklist but it is up to ISPs to implement or tinker with it at their own discretion
Internet applications targeted by the online intermediaries in re child porn	Public websites (ie the open Internet) and newsgroups hosted in Australia or overseas	Public websites and closed commercial websites (agreements with the online payment systems)	Newsgroups, public websites (inc unregistering domain names), paid websites via the financial coallition. Only public space Internetbut it can pass the reports received about closed platforms and suspect offenders on to the police
Appeal or put back procedures in re child porn	Apparently there are some in relation to the Interpol blocklist: info via Interpol website, appeal procedures managed by Interpol and AFP	None identified	There are appeal procedures established by the IWF
Who manages the blocking/removal lists/decides what to block?	Mainly the Cth regulator ACMA Hotline (domestically and overseas) together with the National Classification Board, but also the IHPs and ICPs (domestically) because the latter receive complaints from the public. The Internet industry is also a key actor	The Federal Public Prosecution Service (MPF-SP) and the Safernet notify the OIs about the content hosted in the country. Other institutions can also report the child pornographic content. In addition, some OIs operate monitoring strategies of their own and take-down alegedely child pornographic at their own discretion but are required to notify the LEA	The IWF receives and assess complaints from the public and manages the Blocklist of URLs which are passed on to the ISPs. These are responsible to implement the Blocklist against their custumers. The scheme is voluntarily based but have almost 100% membership. They allegedly target the most violent images of child porn
Online intermediaries targeted	Internet service, hosting and content providers (ISP - overseas; IHP and ICP - domestically). There are a number of Internet industry associations amongst which the IIA is the most important. There are high fees for non-compliance and this is also a criminal offence	ICPs and IHPs (eg Google, Orkut - to take-down the relevant content hosted in Brazil, preserve evidence and identify allegedely offenders), ISPs (eg telcos - info to help law enforcement bodies to identify allegedly offenders), payment systems	ISPs, ICPs/IHPs, online payment systems, search engines eg Yahoo! and Google (via implementation of the URL blocklist against the search results), mobile operators

		CASE STUDIES		
	Comparative Table	***Australia***	***Brazil***	***United Kingdom (England and Wales)***
	Key regulatory actors	Cth ACMA (it has a number of statutory powers to make the OIs come into line), Internet Industry Association, filter vendors, online intermediaries (ISPs, IHPs and ICHs), Internet users (installing filters but only as a protection against inadvertent access)	Federal Public Prosecution Service (MPF-SP) and other LEAs, OIs (ISPs, ICPs and IHPs), Internet hotline Safernet, Senate Committee Inquiry (no longer in operation), online payment systems	The IWF and the member ISPs. But both the government and the police play a key role in the scheme; mobile operators and oter OIs. The IWF is a member of the INHOPE Association
	Transparency	The ACMA Blocklist is exempt from disclosure under the FOI Act 1982 as amended. The use of the Interpol/IWF blocklists are also problematic. No independent audit performed and censors are unamed. Users are informed about blocked websites via the Interpol website	OIs are performing proactive monitoring of online content in non-transparent ways at their own discretion. The integrated national database of reports can be accessed by different actors	Some OIs provide the standard 403 message under the blocking scheme but no reason for this is given. ISPs implement the blocklist at their own discretion and may tinker with it
	Accountability	The ACMA is required to report to the Minister every six months about the Blocklist operation, but reports have been discontinued after 2005 and no explanation has been given. Similarly, the Minister is required to report to the Cth Parliament. Unamed staff classify the censored content and these decisons cannot be appealed	The Safernet Brasil has been criticised for not been accountable, for being a private institution assesssing the illegality of content, under no judicial oversight or external audit and its financial sources raise doubts about its true independency	For some, the heroic nature of the IWF has saved them from greater scrutiny
	Legitimacy	Blocklists generated by international companies (ie filter vendors), organisations (ie IWF) and police forces (ie Interpol). The responsibility for assessing and vetting content is delegated to overseas institutions. The regulatory scheme is defined via legislation	The NGO-based Internet hotline is performing a public function without a legislative mandade or proper public scrutiny. The Senate Committee Inquiry had a number of public sessions but sectors of society were outside the parliamentary discussions (eg judiciary, consumer rights, civil rights and children right's activists). Regulation via agreements can be illegitimate and have a democratic deficit. There is a bill on discussion (marco civil)	The IWF is an Internet industry regulatory body without a legislative mandate. It has however reformed its Board so as to include wider representation from different sectors of society. It is said to perform a public function (censorship) and judicial function (assessment of legality of online content), but it is not clear whether it is a public body or a private body undertaking public functions. Its charitable status has also been criticised. There are liaisons with the police. The dubious nature of the IWF: priavte org doing a a pub function? gov body of a charity? quasi-pub or quasi-priv? it is also said to lack citizen agency
	Judicial oversight	Interim notices can be used to bypass the National Classification Board decisions in re to potential prohibited content		It has been debated and referred by both Houses of the Parliament and in a number of court cases, and is also cited as an exemple of good practice by the government
	Legislative oversight		The Senate has actively participated in the regulatory endeavour legislating about criminal laws (substantive law and NTD scheme in re to child pornography) and forcing OIs to settle agreements in relation to the other regulations	It has been debated and referred by both Houses of the Parliament and in a number of court cases, and is also cited as an exemple of good practice by the government
IMPLICATIONS	***Citizen agency and public support***		Poor participation of civil rights and children rights activists, judiciary and consumers	

	Comparative Table	CASE STUDIES		
		Australia	***Brazil***	***United Kingdom (England and Wales)***
	Free speech: unchecked private censorship, scope creeep and narrowness	Legislated mandatory filtering scheme may be reduce the risk ot private censorship but a voluntary scheme is under operation at the ISP-level without a legislative mandate and without adequate safeguards. The filtering scheme is not narrow but targets a wide range of prohibited content (RC category is under revision). A few ISPs offer filtered access to the Internet commercially. Blocklists of websites are created and maintained by private companies and an overseas police organisation. The voluntary filtering scheme targets websites not URLs. Overall regulatory scheme is wide in scope. The proposed blocking of websites may include not only child pornography but the wider range of RC-rated material	OIs are employing monitoring of online content of their own in non-transparent ways (eg hashing checks, blocking uploads). No challenges were made in courts against the terms of the agreements. There is no comprehensive legislation to regulate the activities of OIs in Brazil neither are legislated safeguards to discourage/limit private censorship. OIs have more incentives to comply with the LEAs requests than challenge these requests in courts	The Wikipedia event: overblocking and assessing illegality without adequate judicial oversight. Scope creep has been alleged. The blocklist content is secretive, but it has been subject to independent audits. The blocklist is passed on to other institutions overseas. Ths OIs have more incentives to comply than challenge the requests. Non-legislated censorship performed by private actors? The ISPs may tinker with the blocklist. Some argue that the blocklist violates Article 10 of the ECHR because there are no adequate safeguards
	Privacy: unchecked and more invasive surveilance powers given to law enforcement authorities	Court orders are needed to obtain the contents of a communication	Access logs (not the contents of a communication) are disclosed without the need of a court order	
	Safeguards in place			Some have argued for the publicisation of the IWF
	Effectiveness	Arguably effective to remove child pornographic content hosted in Australia (there are limitations of a complaint-based strategy though). Filtering (voluntary or otherwise is unable to stop access to overseas content). Only websites are targeted. It offers only a false sense of secutiry	No evidence of blocklists implemented to limit access to child pornographic content hosted overseas. The current take-down regime targets only the websites hosted in the country and other platforms are a matter of police investigation, but a number of agreements have been settled on this regard to facilitate the identification of alleged offenders and the collection of criminal evidence. Material hosted in Brazil can go unreported and there are other platforms where child pornography is exchanged	Blocking and take-down notices only applied against the open Internet. The scheme is easily circumvented by persistent viewers, child porn is hardly found via public websites. A small number of ISPs do not take part in the blocking scheme. For some, URL blocking can undermine international cooperation
	Efficiency	The ACMA is a statutory body	Safernet mainly financed via public funds	The IWF is partially funded by the EU (75%) and OIs (25%) inc. membeship fees from the blocking scheme

APPENDIX 2: INVITATION LETTER

INVITATION LETTER

Participant's Contact Info

Fabio A. S. Reis
PhD Student, School of Law
The Sheffield Of University

Bartolomé House, Winter Street, Sheffield
S3 7ND, United Kingdom
e-mail: F.Reis@sheffield.ac.uk

Dear **Participant**, **15 November 2011**

This letter is asking for expert opinion in a doctoral research project that explores comparatively the Australian, Brazilian and British regulatory models designed to limit access to child pornographic content on the Internet. The documentary analysis developed so far has addressed each of the three regulatory models in detail and produced three draft chapters of around 8,000 words each. The next step is to validate the content of these three chapters by means of receiving written feedback from and, perhaps, conducting further interviews with experts in the three jurisdictions.

This research project is based at the School of Law of the University Of Sheffield and is partially funded by the Brazilian Government (State of Bahia). The project is under the supervision of Dr. Maggie Wykes (e-mail: M.Wykes@sheffield.ac.uk) and Dr. Lindsay Stirton (e-mail: L.Stirton@sheffield.ac.uk). In addition, the project was approved by the University Of Sheffield Research Ethics Committee and: (i) a consent form will be provided before the interview in order to inform participants about the validation process; (ii) responses will be kept confidential, unless explicit permission is given; and (iii) participants will be able to choose to be identified or not. Each participant is free to provide any feedback about the chapter from her/ his jurisdiction.

Given that this research is mostly funded at my own expense, I will not be able to provide any remuneration for this task but I will send a printed copy of the thesis to each participant once it is finally awarded as a sign of gratitude. The research timetable is heavily dependent on this validation process, so I do appreciate your prompt response about whether you are interested in taking part in this research.

If you have questions or need any further information about this, please do not hesitate to contact me (or my supervisors) via e-mail at F.Reis@sheffield.ac.uk.

Yours sincerely,
Fabio A. S. Reis

APPENDIX 3: PARTICIPANT CONSENT FORM

University of Sheffield

Participant Consent Form

Title of Research Project:

Regulating to Limit Access to Child pornography on the Internet: a multiple case study.

Name of Researcher:

Fabio Andre Silva Reis

1. I confirm that I have read and understand the information sheet dated 21 November 2011 explaining the above research project and I have had the opportunity to ask questions about the project.

2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason and without there being any negative consequences. In addition, should I not wish to answer any particular question or questions, I am free to decline. (Research supervisor: Dr. Maggie Wykes, e-mail: X.XXX@sheffield.ac.uk, phone: +44 XXX.XXX.XXXX).

3. I understand that my responses will be kept strictly confidential unless I have given written permission for them to be disclosed. I give permission for members of the research team to have access to my anonymised responses. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the report or reports that result from the research.

4. I agree for the data collected from me to be used in future research.

5. I agree/do not agree (delete as applicable) to be identified.

6. I agree to take part in the above research project.

_____	_____	_____
Name of Participant (*or legal representative*)	Date	Signature

FABIO ANDRE SILVA REIS	21/12/11	_____
Name of person taking consent (*if different from lead researcher*)	Date	Signature

To be signed and dated in presence of the participant

DR. MAGGIE WYKES	_____	_____
Lead Researcher	Date	Signature

To be signed and dated in presence of the participant

Copies:

Once this has been signed by all parties the participant should receive a copy of the signed and dated participant consent form, the letter/pre-written script/information sheet and any other written information provided to the participants. A copy of the signed and dated consent form should be placed in the project's main record (e.g. a site file), which must be kept in a secure location.

APPENDIX 4: CODING SCHEDULE

Coding Schedule				CASE STUDIES		
				Australia	*Brazil*	*United Kingdom (England and Wales)*
LEGISLATION AND CASE LAW	***State-regulation***	***PERIOD***		*1990 - 2010*	*1990 - 2010*	*1978 - 2010*
		Anti-child pornography criminal laws	definition of child porn			
			age of a child			
			types of content			
			production			
			distribution			
			intentional access			
			possession			
			penalties			
			extraterritorial			
			liability of online intermediaries			
			defences			
			investigatory powers of law enforcement bodies			
	Multi-state regulation	2001 CoE Cybercrime Convention				
		2000 UN Optional Protocol				
REGULATORY FRAMEWORK	***PERIOD***			*1990 - 2010*	*1990 - 2010*	*1990 - 2010*
	Key developments over time					
	Regulatory nature					
	Scope: online material targeted					
	Mechanics					
	Child pornography hosted domestically					
	Child pornography hosted overseas but accessed within the jurisdiction					
	Is the pro-active content monitoring and disclosure of personal data by the OIs regulated to prevent abuses?					
	Complaints and content analysis (human or automated, ex ante or post) in re child porn					
	Internet applications targeted by the online intermediaries in re child porn					
	Appeal or put back procedures in re child porn					
	Who manages the blocking/removal lists/decides what to block?					
	Online intermediaries targeted					
	Key regulatory actors					
IMPLICATIONS	***Transparency***					
	Accountability					
	Legitimacy					
	Judicial oversight					
	Legislative oversight					
	Citizen agency and public support					
	Free speech: unchecked private censorship, scope creep and narrowness					
	Privacy: unchecked and more invasive surveillance powers given to law enforcement authorities					
	Safeguards in place					
	Effectiveness					
	Efficiency					