Internet content regulation in liberal democracies.

A literature review.

Yana Breindl
(Institute of Political Science,
Georg-August-Universität Göttingen)

DH Forschungsverbund – Working Papers zu Digital Humanities 2

Gefördert von

Niedersächsisches Ministerium für Wissenschaft und Kultur

VolkswagenStiftung

Digital Humanities Forschungsverbund - DHFV

Goettingen Research Campus

Die Working Papers zu den Digital Humanities werden erstellt von Verbundpartnern des Göttingen Research Campus aus dem „Digital Humanities Forschungsverbund“, einem vom Niedersächsischen Ministerium für Wissenschaft und Kultur (MWK) und der VW-Stiftung geförderten und vom Göttingen Centre for Digital Humanities (GCDH) geleiteten Verbundprojekt (Laufzeit: Jan. 2012 – März 2015).

Erschienen März 2013

Online:
http://www.gcdh.de/en/publications/

GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Institut für Politikwissenschaft der Georg-August-Universität Göttingen
yana.breindl@sowi.uni-goettingen.de

Abstract:

This paper presents an overview of the literature on Internet content regulation in general and Internet blocking in particular as part of the research project on "Internet blocking in liberal democracies" of the Digital Humanities Research Collaboration at the Göttingen Centre for Digital Humanities. It starts by presenting the main debates about Internet regulation and governance of the last twenty years. Scholars of Internet governance remain divided about the role played by the nation-state in the digital realm as well as the disruptive potential of the Internet for society and politics in general. There is however broad consensus that new forms of regulation (e.g. "code as law") have emerged and that private actors play an important part in Internet regulation. The report then assesses the challenges and opportunities presented by digital content for policy-makers before reviewing various points and techniques of control that have been implemented to deal with problematic content. This includes in particular technical blocking, removal of search results and take-down procedures. The final section of the review then assesses recent legal and empirical scholarship pertaining to Internet blocking before discussing future research steps.

Inhalt

Introduction

Since the introduction of the World Wide Web and browsers in the early 1990s, there has been an explosion of content available across state boundaries, in easily duplicable format through the Internet. This development has first been interpreted as a formidable chance for democracy and civil liberties. The Internet has and continues to be perceived as the infrastructure and tool of global free speech (Mueller, 2010). Many optimists hoped that, free from state intervention or mainstream media intermediaries, citizens would be better informed about politics, at lower costs and more efficiently. The need for content control was however discussed as soon as the Internet became accessible to the greater public. Similarly to the emergence of previous communication and media technologies, pressure rapidly built up to demand more control of what type of content is accessible to whom (Murray, 2007). The regulation of content is linked to a broader discussion about the regulability of the Internet that is the focus of section 1 before turning to content regulation *per se* in section 2.

1 Internet regulation and governance

One of the characteristics of the literature on Internet regulation in general and content regulation in particular is the use of often vague terminologies and concepts that are not clearly distinguishable and lack direct connections to empirical foundations (Hofmann, 2012). Authors writing on Internet regulation do so from a given perspective. In particular, they diverge on two central aspects: the role of the nation-state and the disruptive potential of the Internet.

The role of the nation-state in regulating the digital realm in comparison with other actors such as corporations or civil society remains disputed. For some scholars, the nation-state is the main actor capable of directly or indirectly regulating social behaviour. For others, the state is one among a variety of competing actors and has lost its dominance. Their perspective is generally reflected in the terminology used, focusing on "governance" instead of "regulation" when taking into account a broader set of actors and processes than interactions centred around the state.

The transformative or disruptive impact digital technologies may have on politics and society in general divides scholars. Early Internet policy debates have fuelled utopian and dystopian scenarios. The Internet has been perceived as the instrument of global free speech on the one side and as a tool leading to a new type of sophisticated surveillance state on the other side. If nuances run through both the optimistic and the pessimistic strands of the literature, a recurrent criticism is that they are based on either social or technological determinism. They are emblematic of the emergence of any new technology and not particular to the case of the Internet. Similar narratives surrounded the emergence of previous technologies such as the telegraph, the radio or television (Flichy, 2001; Vanobberghen, 2007). Technologies are socially constructed. They do nonetheless generate "social affordances", a term largely used in human-computer interaction studies, and defined as "the possibilities that technological changes afford for social relations and social structure" (Wellman, 2001, 228). They hold certain potentialities that can be positive – new forms of sociability, rapid information transmission, spaces for open collaboration – as well as negative – lack of control or oversight, reduced privacy, increased surveillance and cyberattacks. However, in terms of regulation, the literature remains divided between authors who consider that there is (or should be) something distinctly different about Internet politics, compared to other policy fields, and those who consider that Internet regulation is maturing and resembling more traditional policy fields, similar to the emergence of environment issues as a new policy field at the end of the twentieth century.

The discussion about the regulation of the Internet has shifted from whether the Internet can be regulated at all to *how* it is regulated and by *whom*. The question opposed the so-called cyber-libertarians who contested any exterior assertion of power, be it by states or other actors (section 1.1), to legal and political scholars arguing that the Internet was in fact regulated, although through different regulatory modalities (section 1.2). For some authors, states continue to play a significant role in these regulatory arrangements (section 1.3) while there is widespread agreement that the Internet has become an object of political struggle for states and various other actors alike (section 1.4). However, the narrowly defined state-centric perspective on Internet regulation has more recently been criticised as "cyber-conservatism" (Mueller, 2010; DeNardis, 2010) by a third set of scholars interested in the institutional innovations and broader power dynamics at play in Internet governance (section 1.5).

1.1 Cyberlibertarians

Because of the Internet's decentralised and global architecture, early Internet enthusiasts and cyber-libertarian scholars perceived "cyberspace" as a social space beyond territorially-based regulation that should remain free from governmental or corporate intervention (see for instance Johnson and Post, 1996 and Barlow's famous *Declaration of Independence of Cyberspace*).[1] Internet freedom was thought to be hardwired into its technological infrastructure as exemplified by the often-quoted phrase "the Net interprets censorship as damage and routes around it".[2] Nation-states in particular were perceived as illegitimate and powerless actors with no means to enforce state sovereignty in cyberspace. The only legitimate form of decision-making for cyberspace would have to be "developed organically with the consent of the majority of the citizens of cyberspace" (Murray, 2007, 7).

Much has been written about the Internet's open, minimalist and decentralised architecture that allowed for its rapid success, integration with any other computer network and the rapid development of new applications such as the World Wide Web or email programs. The Internet has been built upon the "end-to-end principle", which stipulates that application-specific functions are hosted at the endpoints of the network (e.g. servers or personal

[1] Barlow, J.-P. (8 February 1996). A Declaration of the Independence of Cyberspace. Available at: https://projects.eff.org/~barlow/Declaration-Final.html. See also *Cyberspace and the American Dream: A Magna Carta for the Knowledge Ag*e (Dyson *et al.*, 1996) and *Birth of a Digital Nation* (Katz, 1997).

[2] Quote attributed to the civil liberties advocate and co-founder, together with J.P. Barlow, of the digital rights platform Electronic Frontier Foundation (EFF), John Gilmore.

computers) instead of intermediary nodes (e.g. routers). Similarly to postal mail delivery agents, intermediaries route data packages from one endpoint to another endpoint, without needing to know what the datagram will be used for or contains in terms of content. The “end-to-end” principle is central to current “net neutrality” debates (see below) that focus on new technological possibilities for intermediaries to perform certain application-specific functions (e.g. distinguishing between peer-to-peer file-sharing and video streaming).

The protocols and standards developed during the 1960-70s by the so-called “Internet founders”, academics and government engineers, funded by the U.S. Department of Defense, are still the basis of today’s Internet. To protect their achievements, the founders established a series of institutions, in particular the Internet Engineering Task Force (IETF) in 1986 to regulate and develop new standards. These institutions were perceived by cyber-libertarians and many of the founders as new and better forms of governance under the leitmotiv of “rough consensus and running code” (Dave Clark, Internet founder, quoted in Goldsmith and Wu, 2006, 24). Although the cyber-libertarian perspective was rapidly criticised as technologically deterministic and contrary to empirical evidence of increased state and corporate control of the Internets’ infrastructure and content, its main tenets and values continue to inform current policy discussions and self-regulatory practices that proliferate online.

1.2 Code as law and other “cyberspace” regulations

The cyber-libertarian perspective was rapidly challenged, notably by Joel Reidenberg (1998) who argued that despite the challenge to territorial borders posed by global networking, new models and rules would emerge in which the state continues to be involved. If governments would not necessarily be able to directly regulate “cyberspace”, they would at least be able to influence two distinct regulatory borders: contractual agreements between Internet Service Providers (ISPs) and the network architecture, in particular technical standards. He referred to *Lex Informatica* as the possibility to regulate user behaviour through influencing the Internet's underlying technological infrastructure and system design choices. The concept would influence the cyber-paternalist position and the future debate about Internet regulation (Klang, 2005).

The argument that the Internet is not unregulable but in fact regulated by its architecture was expanded upon in the 1999 publication of U.S. law professor Lawrence Lessig's seminal book "Code and other laws of Cyber-space". Lessig argued that the Internet is not a space free from state intervention and that computer code, the Internet's underlying infrastructure, provides a powerful tool for regulating behaviour online (Lessig, 1999, 2006). For Lessig, code is one of the four modalities of regulation next to law, social norms and markets. The latter are institutional constraints, which do not allow for immediate control over human behaviour and are considered by a large majority of observers as insufficient to effectively regulate global Internet traffic. Lawsuits are time and cost intensive, often ineffective when dealing with the scale change brought through the Internet, whilst generating broad negative publicity (see for instance Brown, 2010). Social norms are easily violated, and can be manipulated. Market constraints can be circumvented in many ways, and commercial entities are dependent on effective protection by social norms and the legal system for enforcement (Boas, 2006). Whether Internet design choices are a regulatory modality in itself or not remains debated (McIntyre and Scott, 2008). Murray and Scott (2001) have for instance criticised Lessig's modalities as over- or under-inclusive. They propose to speak instead of "hierarchical" (law), "community-based" (norms), "competition-based" (market) or "design-based" controls.

Nonetheless, it is widely acknowledged that code plays a central role in controlling user behaviour, often in support of legal arrangements. This focus on "code as law" or the control of user behaviour through technical design features has been widely taken up by scholars who point to the inherent political dimension of the Internet's infrastructure, made of hardware, cables, standards and protocols (see for instance DeNardis, 2009, 2012). As we will see, this aspect is also highly relevant for content control. Contrary to the cyber-libertarian position, which postulates that freedom was inscribed in the architecture of the Internet and thus beyond state control, Lessig's position asserted that who controlled the code controlled user behaviour. In practice, this means that private actors, the owners of the Internet's infrastructure made of hardware and software, play an increasingly important role in regulating the digital realm while the state in which they operate can indirectly control the infrastructure by regulating the intermediaries.

With the turn of the millennium, the discussion has thus clearly shifted from whether the Internet can be regulated at all to how and by whom it is and whether there is anything explicitly new about the phenomenon. Here, scholars remain divided by those insisting on the dominant role of nation-states in Internet regulation, pointing to the increasing number of state legislation directed towards the digital realm (e.g. Goldsmith and Wu, 2006), and those who argue that more attention should be paid to new processes and institutions that are emerging at the international level and the key role played by private actors in Internet politics (e.g. DeNardis, 2009; Mueller, 2010).

1.3 Cyberpaternalism or the return of the nation-state

In their 2006 book "Who controls the Internet? Illusions of a borderless world", Goldsmith and Wu (2006) recognise that the Internet challenges state power but argue that since the 1990s, governments across the world have increasingly asserted their power to make the global Internet more "bordered" and subject to national legislations. They provide numerous examples of interactions where the nation-state resorted as the dominant actor, starting with the *LICRA v. Yahoo! Inc.* (2000) case in France that led Yahoo to remove Nazi memorabilia on its auction website worldwide to comply with French law,[3] the long interactions between the Internet's

[3] In the 2000 ruling *LICRA v. Yahoo! Inc.*, the Tribunal de Grande Instance of Paris exercised territorial jurisdiction on the grounds that the prejudice of the content hosted abroad took place on French territory. The Court required Yahoo! to prevent French users from accessing Nazi memorabilia on its auction website. The company complied to the judgement even though a U.S. District Court judge considered in 2001 that Yahoo! could not be forced to comply to the French laws, which were contrary to the First Amendment. The ruling was reversed in 2006 by a U.S. Court of Appeals. For Goldsmith and Wu (2006), the French state could exert pressure upon Yahoo! because the company held several assets for its operation in France that the French state could have acted upon should Yahoo! have refused to comply to the French court order.

founding fathers and the U.S. government over the Internet's domain name system (referred to as "the root", see Mueller, 2002) that eventually led to the establishment of ICANN and, of course, the establishment of the Chinese great firewall as an illustration of "what a government that really wants to control Internet communications can accomplish" (Goldsmith and Wu, 2006, 89). In sum, "[a] government's failure to crack down on certain types of Internet communication ultimately reflects a failure of interest or will, not a failure of power" (*ibid.*). Similarly, for Deibert and Crete-Nishihata (2012), it was a conscious decision by the US and other Western states to not directly regulate the Internet in the early 1990s, leaving operating decisions to the Internet's engineering community that functioned on a basis of consensus building and requests for comments. This was to foster innovation and economic growth at a time where one could only speculate as to how precisely the Internet would develop over time.

In fact, the first motivation for Internet regulation was to situate Internet exchanges into existing legal categories (e.g. is the Internet similar to the telephone or broadcasting media?) or to create new categories, and in rare cases, new institutions. However, in the early to mid-1990s, states largely maintained the *status quo ante*, either to protect emerging business models or established governmental practices (Froomkin, 2011, 5).

1.4 The Internet as an object of political struggle

Although the state-centric and cyberlibertarian perspective are still present in Internet governance discussions, the dominant perspective nowadays is that the state is one, albeit important, actor among a variety of stakeholders that are interested in shaping the Internet's future. Those stakeholders hold different interests, norms and values as to how the Internet should develop in the future. The technical community, that was instrumental in developing the Internet in the first place, aims to protect the open and decentralised architecture of the Internet from governmental or corporate encroachments.[4]

[4] Internet engineers remain the principal decision-makers over the Internet's "critical resources", most notably the domain name system through ICANN but also in the domain of standards setting (e.g. the IETF). Those resources are heavily contested but, notably due to the protection of the U.S.

Private actors are increasingly important in shaping the Internet's development. Some corporations have based their business model on the relatively unregulated environment of the 1990s and early 2000s, with limited intermediary liability (e.g. for Internet service providers (ISPs) or online content providers (OCPs)), and succeeded to monetize their Internet activities principally through paid, and increasingly targeted, advertisement (e.g. Google or Facebook). Other actors, for instance the entertainment industry, have been severely challenged by new practices developing online such as widespread sharing of copyrighted material. Attempts to roll back "piracy" have generally led to further technological developments such as peer-to-peer technologies (Musiani, 2011). Other actors increasingly converge their activities to the Internet bringing with them different norms and interests than those of the early Internet communities (Deibert and Crete-Nishihata, 2012; Rasmussen, 2007; Castells, 2001). States, which are driven by security and public order concerns, are by no means in agreement over who should control the Internet albeit all recognise the fundamental importance of the network as a global communication infrastructure and business opportunity. Finally, a broad transnational movement of NGOs, associations, information groups and individuals has emerged over the years in response largely to regulatory attempts to introduce more control of the network of networks but also, at times, to demand governments to intervene in business practices that are considered as harming the end-to-end principle at the basis of the Internet (Mueller *et al.*, 2004; Breindl and Briatte, 2013; Haunss, 2011; Löblich and Wendelin, 2012).

Through digital convergence, most information and communication activities have shifted to the Internet. The separate legal and regulatory instruments that governed entertainment consumption, print and broadcasted media, libraries, public information delivery etc. are now converging on the Internet, encompassing the "entirety of communication and information policy" (Mueller, 2010, 10). States alone are not able to

government, a far-reaching reform of the U.S.-centred domain name system has until now been avoided, although concessions have been made to other governments and private actors (Mueller, 2002).

regulate the Internet without at least relying on private actors to assist them. Many Internet issues extent beyond national borders, making coordinated action necessary.

1.5 Institutional change and multi-stakeholderism

Authors such as Milton Mueller (2010) consider that the only solution to current Internet issues such as intellectual property rights, cybersecurity, content regulation and critical Internet resources, that would preserve the open and disruptive character of the Internet, is institutional change in the way communication and information technology has been regulated so far. He therefore speaks about Internet *governance* at the international level to highlight “the coordination and regulation of interdependent actors in the *absence* of an overarching political authority” (Mueller, 2010, 8, emphasis in original). For Mueller (2010, 4) the Internet challenges the nation-state because communication takes place at a global scope, at unprecedented scale while control is distributed, meaning that “decision-making units over network operations are no longer closely aligned with political units”; new institutions have emerged to manage the Internet’s critical resources (e.g. domain names, standards and protocols) beyond the established nation-state system, while dramatically lowering the costs for collective action thus allowing new transnational networks of actors and forms of activism to emerge. Similarly, for Braman (2009) the increasing importance of information policy manifest and trigger profound changes in the nature of how the state and governance functions. Old categories need therefore to be reassessed in light of Internet governance and more fluid forms of decision-making.

To deal with Internet issues at an international level, the United Nations launched the World Summit on the Information Society in 2002, which opposed proponents of a state-centric regulatory regime to supporters of a more “open, pluralistic, and transnational policy-making framework” (Mueller, 2010, 10). Especially civil society and private businesses demanded to be integrated into the discussion asking for more “multi-stakeholder participation” (Mueller, 2010). The Summit held in Geneva in 2002 and

Tunis in 2005 resulted in a series of declarations, action plans and agendas.[5] The WSIS opposed the United States' defending their unilateral control of ICANN, "one of the few globally centralised points of control on the Internet" (Mueller, 2010, 61) to Europe, on the one side, and emergent countries, on the other side, both demanding more influence over the domain name system and Internet governance in general. The Tunis Agenda explicitly praised the role of the private sector in the Internet's daily operating decisions, but also paved the way for a long-term reform of ICANN (for more information see Mueller, 2010) and mandated the creation of a non-binding, multi-stakeholder forum to discuss Internet governance issues on an annual basis. Since then seven Internet Governance Forums (IGFs) have taken place in various locations, offering a unique, yet not binding, platform for discussion and dialogue about Internet related issues by a broad range of stakeholders. However, IGFs, in which any actor can participate, are repeatedly criticised for not resulting in concrete outcomes with several critics turning to other forums, reserved to member states such as the International Telecommunications Union (ITU), a UN agency, to defend their interests in global Internet politics, notably in the domain of Internet content regulation.

Governments attempted at several occasions to use the established intergovernmental process of the ITU to gain more influence over the U.S. dominated "critical Internet resources", in particular the domain name system, and more recently by attempting to extend the ITU's competencies to Internet policy at the World Conference on International Telecommunications (WCIT) in December 2012. The 1988 ITU's telecommunication regulations (ITRs) were debated by all member states. The negotiations were heavily criticised for being closed to non-governmental stakeholders, non-transparent and could lead to more restrictive Internet policies, especially by authoritarian regimes. The most contentious amendments were vaguely formulated, leaving space for various interpretations in national law that

[5] The Geneva meeting adopted the *Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium* (2003); The Tunis meeting led to the *Tunis Agenda for the Information Society* (2005).

could be used as a legitimation by authoritarian states to filter political content and crack down on opponents. Several Western and African states refused to sign the final declaration, the U.S. being the most vocal defender of Internet freedom stating that:

> ”The Internet has given the world unimaginable economic and social benefit during these past 24 years. All without UN regulation. We candidly cannot support an ITU Treaty that is inconsistent with the multi-stakeholder model of Internet governance.”[6]

The controversial negotiations resulted in a split between Western states who refused to sign the treaty and emerging economies, in particular Russia and China who demanded more state control over Internet regulation and signed the final treaty. If the present system is far from ideal, it is perceived nonetheless by most Western states as the best possible solution to protect their interests (and the interests of their IT industries) and prevent authoritarian states from gaining direct interference in Internet regulation. Nonetheless, various commentators have rejected the apparent opposition between the freedom-protecting West compared to the authoritarian and repressive East by pointing to the fact that maintaining the *status quo* perpetuates the dominance of the U.S. and U.S. business interests (e.g. Google accompanied the WCIT by a particularly vocal campaign to defend Internet freedom) in Internet governance. Poorer countries can only voice their positions at intergovernmental conventions such as the ITU. As it is, they are in effect excluded from gaining any weight in Internet regulation, with some countries even arguing that the U.S. uses denial of Internet services, among other forms of sanctions, for policy leverage. Also, the U.S. defence of “Internet freedoms” at the international level stands in sharp contrast to a series of domestic policies adopted in the name of security that increases control over networks by possibly reducing citizens’ freedoms.[7] Not surprisingly, many of these policies deal with Internet content regulation.

[6] Terry Kramer, head of the US delegation to WCIT, quoted in Arthur, Charles (14 December 2012). “Internet remains unregulated after UN treaty blocked”, *The Guardian*, available at: http://www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-Internet-unregulated?INTCMP=SRCH

[7] See for instance: Powell, Alison (20 December 2012). “A sticky WCIT and the battle for control of the Internet”, *Free Speech Debate*, available at: http://freespeechdebate.com/en/discuss/a-sticky-wcit-and-the-battle-for-control-of-the-Internet/; Mueller, Milton (13 December 2012). “What really

2 Digital content as a new policy problem

The early literature on Internet content regulation has primarily focused on the tension between online content regulation and human rights, in particular freedom of expression and privacy, and constitutional principles such as the rule of law. Especially state-led initiatives were interpreted as censorship and critically analysed by freedom of expression advocates, computer scientists and legal scholars. A second wave of literature focused essentially on authoritarian states to document how countries such as China or Iran started to build national firewalls and sophisticated filtering systems (Deibert *et al.*, 2008; Clayton *et al.*, 2006; Wright *et al.*, 2011). The spread of information control systems throughout the world, including in Western democracies – Deibert and Crete-Nishihata (2012, 341) speak about a "norm regression" to designate the transition from the belief in the Internet as a "freedom" technology to the increasing demands for more information controls – has more recently led to the emergence of a more empirical, sometimes apolitical, literature that views Internet blocking not as the exception but rather as a "global norm" in emergence (Deibert *et al.*, 2010, 2011a; McIntyre, 2012).

Internet content regulation is one of the drivers of Internet governance (Mueller, 2010). As various authors have noted, making available content such as pornography or copyrighted material has in fact significantly contributed to driving Internet growth and, in response, led to increasing efforts to control and regulate the Internet (Johnson, 1997; Zittrain, 2003; Murray, 2007). It has indeed been this type of content that was the object of early concern, notably because of the characteristics of digital content and its intrinsic relationship to freedom of expression. We will therefore first examine the particularities of digital content (section 2.1) before presenting the evolution of content controls through different points and techniques of control (section 2.2) to finally assess recent empirical research (section 2.3).

happened in Dubai?", *Internet Governance Project*, available at: http://www.Internetgovernance.org/2012/12/13/what-really-happened-in-dubai/.

2.1 Characteristics of digital content

The Internet's role in providing access to information and facilitating global free expression has been repeatedly underlined by commentators, politicians (e.g. Clinton's "Freedom to connect") and institutional reports (e.g. Dutton *et al.*, 2011; La Rue, 2011; OECD, 2011). However, the borderless nature of information exchanges conflicts with the body of pre-existing regimes on information and content regulation that have been established at the national level. Attempts to harmonise these regulatory bodies lead often to conflicts, especially since information, and the control thereof, gains in strategic and economic importance (Busch, 2012).

Although all democratic countries protect freedom of expression through a series of national and international legal instruments, each country holds a margin of appreciation to introduce speech-based restrictions to its laws (Akdeniz, 2010). Countries have "differing human rights approaches" (Brown and Marsden, 2013, 204). Especially in Europe, freedom of expression has never been an inalienable right but is balanced against other rights, such as the respect of privacy or public order (Akdeniz, 2010; Zeno-Zencovich, 2009). If freedom of expression was longtime associated with freedom of the press and the mass media in general, resulting in a series of regulations of these sectors, the convergence of broadcasting and telecommunication and the emergence of the Internet have fundamentally altered the situation. The Internet has in effect "resurrected the notion of freedom of expression as an individual liberty" (Zeno-Zencovich, 2009, 100), meaning that any actor can express himself freely on the Internet and potentially reach a broad audience. The question remains thus "whether and to what extent any regulation might be desirable or necessary" (Zeno-Zencovich, 2009, 103). Furthermore, scholars wonder whether technology-based forms of content control are proportionate with and respectful of human rights protection, in particular freedom of expression and privacy.

Online content differs from previous types of content in its digital nature. danah boyd (2008, 2009) distinguishes five "by default" properties of digitised content: digital content is persistent, replicable, scalable, searchable and (de)locatable. Online messages are automatically recorded and archived. Once content is placed online, it is not easy to remove. Digital content can be easily duplicated, e.g. over thousand mirror sites emerged within a week after WikiLeaks' web hosting contract was terminated by Amazon Cloud Services after the publication of U.S. diplomatic cables in 2010 (Brown and Marsden, 2013; Benkler, 2011, see below). Digital copies are perfect copies of the original, contrary to the products of previous recording technologies such as the tape recorder. The potential visibility of digital content is high. Digital content can be easily transferred to almost anywhere on the globe in a matter of seconds. The emergence of search engines allows users to access content but also provides a new opportunity to filter what type of content depending on the algorithm used. Finally, mobile technologies dislocate us from physical boundaries while at the same time locating us in geographical spaces. Content is accessible in ever more places yet technologies are increasingly constructed to locate us in space and propose location-based content. These properties are not only socially significant, as shown in boyds research, but also politically in that they introduce new social practices and policy responses that may or may not challenge existing economic, legal and political arrangements.

Previous technologies would transmit content to more readily confined geographical areas (Akdeniz, 2010) often through more centralised institutions that could more easily be controlled by governments. On the contrary, the Internet's architecture is highly decentralised, in the hands of private actors, notably due to the liberalisation of the telecommunication industry in the 1980-90s in many liberal democracies (Mueller, 2010), and interconnected at the global level. For Brown and Marsden (2013, 176) "data packets can take a wide range of routes from sender to recipient, reducing the ability of intermediate points to block communications". In sum, the Internet's architecture empowers the periphery over the centre of the network (Froomkin, 2011). Nation states and content producers experience a loss of direct control over information flows (DeNardis, 2012).

If the Internet has challenged state sovereignty and oversight over content control, Internet technologies also *offer* new possibilities of control by automatising the monitoring, tracking, processing and filtering of large amounts of digital data. If the Internet has often been praised for its decentralised nature, removing the gatekeeping function of intermediaries, certain nodes (e.g. routers or servers) are increasingly taught to distinguish particular types of content be this for reasons of managing network congestion, dealing with security threats, developing for-profit services or restricting access to certain kinds of content (Bendrath and Mueller, 2011; Fuchs, 2012). In fact, much of the technologies used to block Internet content can be used for both valid and undemocratic purposes. They constitute so-called "dual use" technologies often produced by the cybersecurity industry of Western state. These have been rapidly adopted by authoritarian regimes (e.g. China built the great firewall using the U.S. company Cisco's technologies, see Goldsmith and Wu, 2006). Especially surveillance technologies used for law enforcement or traffic management purposes in Western democracies are invariably exported to authoritarian regimes where they are employed against activists and citizens in violation of human rights protections (Brown and Korff, 2012).

The Open Net Initiative (ONI), a consortium of universities and private institutions emerged in 2002 to map content restrictions across the world. Since 2006, they "mapped content-access control on the Internet in 70 states, probed 289 ISPs within those states, and tested Web access to 129 884 URLs" (Deibert *et al.*, 2011b, 6). ONI identifies four phases of Internet access and content regulation, three of which are the titles of ONI's *Access* books (Deibert *et al.*, 2008, 2010, 2011a):

THE OPEN COMMONS lasted from 1960s to 2000. "Cyberspace" was perceived as distinct from offline activities and either ignored or only slightly regulated. The period was marked by the belief in an open Internet that enabled global free speech.

THE ACCESS DENIED phase, from 2000 to 2005, was marked by states increasingly erecting filters to prevent their citizens from accessing certain types of content. China in particular emerged as the poster-child of content restrictions by building a highly sophisticated filtering regime that covers a wide range of contents. These controls are either based on existing regulations or new legal measures.

THE ACCESS CONTROLLED phase, from 2005 to 2010, saw states develop more sophisticated forms of filtering, designed to be more flexible and offensive (e.g. network attacks) to regulate user behaviour, including through registration, licensing and identity regulations to facilitate online monitoring and promote self-censorship. “The salient feature of this phase is the notion that there is a large series of mechanisms (including those that are non-technological) at various points of control that can be used to limit and shape access to knowledge and information” (Deibert *et al.*, 2011b, 10). Filtering techniques are situated at numerous points of the network, controls evolve over time and can be limited to particular periods such as elections or political turmoil. Egypt’s complete disconnection from the Internet in January 2011 represents the most extreme form and has triggered wide debates about state-controlled “kill switches” (see for instance Wu, 2010). To achieve more fine-grained controls, states need to rely on private actors through informal requests or stricter regulation.

ACCESS CONTESTED is the term used for the fourth phase from 2010 onwards, during which the Internet has emerged as a battlefield of competing interests for states, private companies, citizens and other groups. Democratic states are increasingly vocal in wanting to regulate the Internet. “The contest over access has burst into the open, both among advocates for an open Internet and those, mostly governments but also corporations, who feel it is now legitimate for them to exercise power openly in this domain”, write Deibert *et al.* (2011b, 14). A wide variety of groups recognise the growing ubiquity of the Internet in everyday life and the possible effects of access controls with some openly questioning the open standards and protocols that were thought to be achieved for good in the 1960-70s. The foundational principles of an open and decentralised Internet are now open for debate and the subject of competing interests and values at all stages of decision-making both within states and in the international realm.

Conflicts about online information and content are highly diverse, ranging from privacy to copyright to freedom of expression to security issues. The fight against "child pornography" or "child abuse images" has been one of the main reasons for introducing stricter content controls and block lists, especially in liberal democracies.[8] Tools that are often associated with the diffusion of illegal content, such as peer-to-peer file-sharing or circumvention tools have equally become the target of censors (Deibert *et al.*, 2008). States are by far not the only actors showing an interest in controlling Internet content, especially since content owners increasingly invest in network operating facilities. The emerging conflicts generally oppose consumers and producers of information who hold diverging interests in controlling or restricting the propagation of information (Busch, 2012). The following section offers a short overview of the evolution of content regulation.

2.2 From endpoint to bottleneck regulation

The early 1990s – ONI's "open commons" phase – was essentially a period with no or very limited state interventions, where governments, especially in liberal democracies, adopted a laissez-faire approach towards the nascent network to leave space for innovation and new developments (regulation was thus mainly user or market driven). In the domain of spam control, this type of self-regulatory system proved to be very effective as spam lists were edited collaboratively online and used by email systems to detect unwanted messages (Mueller, 2010). However, since the early 2000s, states have increasingly asserted their control online (Deibert and Crete-Nishihata, 2012; Deibert *et al.*, 2010).

As already stated previously, much attention has been paid to the filtering of Internet access by authoritarian regimes such as China or Iran (Deibert *et al.*, 2008, 2010; Boas, 2006). However, liberal democracies that base their legitimacy on the protection of civil liberties such as freedom of expression and the rule of law are also increasingly considering technological solutions

[8] Sexual representations of children are frequently referred to as "child pornography", a term rejected by child protection associations and police forces as hiding the child abuse behind those images.

to content regulation. Automatic information controls have emerged as a new policy tool *in* liberal democracies and a global norm for reasserting state sovereignty in the online realm (McIntyre, 2012; Deibert *et al.*, 2010; Zittrain and Palfrey, 2008). In fact, Edwards (2009, 39) argues that technological manipulations of Internet access to content "have been widely disparaged in the West". The Internet Watch Foundation's (IWF) role in blocking content in the UK for instance was unknown to a majority of users until the Wikipedia blocking of 2008.[9]

In authoritarian regimes, the government is generally directly involved in controlling Internet traffic (see for instance the Tunisian example in Wagner, 2012). In liberal democracies, direct government regulation has been hard, if not impossible, to implement (see below). Section 1 has shown that Internet regulation is driven by various forms of private and public orderings and different combinations of regulatory modalities, notably the use of design features by private actors. It is thus not surprising that we see these mechanisms also at work in Internet content control. However, states' attempts at directly regulating speech online against the backdrop of existing media and information and communication policies have been met with widespread criticism for being ineffective or irrespective of existing human rights protections (Brown, 2008).

Although the Internet's role is to root data packets over the networks without regards for what content they carry,[10] infrastructure is increasingly co-opted to perform content controls. This can be the case by denying certain actors access to hosting platforms or financial intermediaries as in the case of WikiLeaks (see below). Infrastructure is also increasingly used to enforce intellectual property rights, through Internet access termination laws for repeated copyright infringement (so-called three-strikes or graduated

[9] In 2008, access to the editing function of Wikipedia was blocked for all UK users after an image of a naked girl, the cover image of a famous rock band's album that could be officially purchased in UK stores, was flagged as child pornography and added to the IWF's blocklist. Because ISPs used a particular type of proxy blocking, this resulted in blocking access to Wikipedia's editing function for all UK users.

[10] This principle has also gained widespread political salience through the "net neutrality" movement particularly in the U.S. and since 2009 increasingly in Europe. Net neutrality advocates defend the Internet's end-to-end principle with no traffic discriminations that might prioritise certain types of traffic over others. For more information, see Marsden (2010).

response mechanisms as implemented for instance in France, Ireland or the UK, see Yu, 2010) or through domain name seizures (DeNardis, 2012).

In the West, the rapid development of the mobile Internet has contributed to increased control and filtering mechanisms being built into mobile access (Zittrain, 2008). As a result of increased government intervention and corporate demands, the Internet is increasingly bordered (Goldsmith and Wu, 2006). For some private actors, the development of technological means of control was a condition for providing access to content they owned in the first place. This is for instance the case of the entertainment industry who use Geo-ID technologies to control where users can have access to their content in the world. Technological innovation online is largely driven by advertising revenues. Large Internet corporations such as Google or Facebook are heavily reliant on advertising as their main source of revenue. Over the last three years, about 96% of Google's total revenue was generated by advertising.[11] To increase the effectiveness of advertisement, "contextual" or "targetted" advertisement has emerged, proposing targeted ads based on the assumption that a user interested in one article will be interested in similar products. Following this logic, the next step is to track user behaviour across websites, collecting data to establish user profiles and propose products that fit closest to his or her preferences (Kuehn, 2012). To do this, new technologies and tools had to be developed to track, collect and process personal data. The development of Geo-ID technologies for instance allows for geographically locating Internet users with great accuracy, therefore making Internet advertising easier.

In parallel, a surveillance and security industry has emerged whose interest lies in collecting, processing and selling data as well as expanding the technological possibilities for tracking user behaviour and filter out unwanted content. It is estimated that the cybersecurity market ranges in the order of hundred billions of U.S. dollars annually. "Commercial providers of networking technology have a stake in the securitization of cyberspace and can inflate threats to serve their more parochial market interests" argue

[11] Google Investor Relations, 2012 Financial Tables, Last consulted on 17 Januarw 2013, available at: http://investor.google.com/financial/tables.html.

Deibert and Crete-Nishihata (2012, 340). Most of the surveillance and filtering systems used in authoritarian regimes are provided by North American and European businesses that developed these for companies, governments and individual users (Hintz, 2012; Fuchs, 2012). Often, these technologies are customised to the particular demands of authoritarian regimes (Deibert and Crete-Nishihata, 2012), but this is not always the case as for the Tunisian pre-revolutionary filtering regime that relied on Western blocklists to control what type of content its citizens could access (Wagner, 2012).

Although the Internet is a decentralised network, there exists a series of "points of control" (Zittrain, 2003) that have been rapidly used by governments and corporations to insert control into the Internet's infrastructure. The four main techniques of content control online are technical blocking (i.e. through blocklists that can either exclude – "blacklist" – or include – "whitelist" – particular types of content), removal of search results, takedown requests and self-censorship (Deibert *et al.*, 2008).

Point of control	**Technique**	**Actors**	**Challenges**
Source	Law enforcement	Courts	Costly, time intensive, identification, national jurisdictions, image
Intermediary	Notice-and-takedown	Any actor	Chilling effects
	Server takedown, domain deregistration, rating systems	State, company	Risk of overblocking
	Technical blocking	State, company	Accountability, overblocking, mission creep, transparency
Destination	(Parental) control filter, surveillance, social techniques	State, company, user	opt-in/opt-out

Figure 1: Internet content regulation

Figure 1 provides a summary of the main forms of content control on the Internet, which will be discussed in more detail below. Since the early 1990s, there has been an evolution in the way content has been regulated ranging from enforcement at the source (section 2.2.1) to enforcement at the destination (section 2.2.2) to enforcement through intermediaries (section 2.2.3), including through automatic filtering.

2.2.1 Enforcement at the source

Early attempts to deal with problematic content targeted the endpoints of the network, i.e. the producers and consumers of problematic content (Zittrain, 2003). States could effectively intervene when the content was produced in the country, by arresting and prosecuting individuals, or when the company hosting the content held assets in the said country. Because the U.S. company CompuServe had office spaces and hardware in Munich, Germany, Bavarian prosecutors succeeded in pressuring the group to block access to 200 Usenet messaging boards containing hard pornography and child abuse images illegal under German law in 1996. Similarly, a Parisian court convicted Yahoo in 2000 to remove nazi memorabilia items from its online auction site (see section 1.3). The company complied, although reluctantly, because it held several assets in France that could be seized by the courts. A similar case is *Dow Jones v. Gutnick* (2002), in which the Australian High court decided that the U.S. company Dow Jones was liable under Australian defamation laws for an unfounded mention of Joseph Gutnick in one of its articles that was also published online. All three examples demonstrate the state's power to effectively regulate what type of content can be accessed on its national territory. Because the technology of the late 1990s and early 2000s did not allow for effectively limiting content controls to particular geographical areas, the result of all three state interventions was that the content illegal in one state was effectively removed from the global Internet, i.e. also in states where the content was legal. The extraterritorial effects of the judgements resulted in much controversy especially in the U.S. where commentators condemned the censoring of the U.S. Internet through foreign speech restrictions (Goldsmith and Wu, 2006; Deibert *et al.*, 2010).

However, the U.S. were among the first to introduce legislation criminalising the initiation of a transmission of "indecent" material to minors. The Communications Decency Act of 1995 (CDA) aimed at introducing content restrictions for underaged minors but was eventually struck down as unconstitutional with regard to the first amendment protection by the courts. Online, it is not necessarily possible to distinguish between minors and adults, the restrictions would thus have effectively applied to all Internet users, which was considered excessively chilling of free speech. All liberal democracies dispose of a more or less broad set of laws that can be used against the source of digital content, e.g. in cases of defamation, trade secret misappropriation or particular types of speech (Zittrain, 2003).

Nonetheless, enforcement remains problematic when the endpoint is not situated on the state's territory and/or traditional legal procedures cannot cope with the exponential amount of content at stake (Mueller, 2010) The latter is particularly the case for pornographic or copyrighted material that is exchanged massively between individuals. Lawsuits are costly and time consuming and do not seem to effect the behaviour of many others engaging in similar behaviours. Furthermore, identification remains a challenge although ISPs increasingly cooperate with law enforcers in identifying the sources of problematic material. Enforcement is impossible when the source of the content is situated beyond the country's jurisdiction and there exists no cooperation mechanisms or both states disagree on whether the content is illegal or not (e.g. the case of *Yahoo v. LICRA*, 2000). Finally, some actors may also wish to control content in lire subtle ways in an attempt to avoid costly and time-consuming lawsuits against their own customers (Zittrain, 2003). Confronted with massive online copyright infringement, the entertainment industry for instance has first engaged in mass litigation or threats thereof against individual file-sharers and the companies operating online file-sharing platforms, often driving these out of business in a variety of countries (Yu, 2004). However, for one platform shut down, new ones would emerge avoiding the pitfalls that had brought their predecessors to fall. As part of these "copyright wars" that are fought in all developed democracies, industry players has come up with ever more aggressive tactics to defend its business model, including lobbying for stricter copyright enforcement legislation, education campaigns, copy-protection technologies (e.g. DRMs) and, more timidly, licensing to online retailers such as iTunes or, more recently, Spotify (Yu, 2004).

Efforts to harmonise content regulation at the international level have been made, notably at the EU level with regards to sexually explicit images of children, racism, terrorism or cybercriminality (Akdeniz, 2010). However, despite the international consensus to tackle issues such as child abuse and the trafficking of images of those abuses, international cooperation to remove such content and prosecute the offenders remains the exception. In fact, the introduction of Internet filtering tools to prevent access to such content correlates with a decrease in cooperative efforts to remove the content at the source (Villeneuve, 2010).

2.2.2 Enforcement at the destination

Control at the destination includes personal computer filtering software that allows to monitor and control what type of content is accessed with the destinations personal computer or network. These filters can be built directly into computers. Sometimes, they are also integrated into Web browsers. These type of filters are used in the corporate environment to prevent employers from accessing leisure or illegal content from within the company's network. Parents are also customers of so-called parental control filters to monitor and control what type of content their children access.

Additionally, governments in liberal democracies have reflected about so-called "opt-out" filters, which would be installed by default on particular Internet connections. In the U.S. funding for schools and libraries is for instance linked to the installation of blocking software that filters out child pornographic material (Zittrain, 2003; Brown, 2008). In other countries (e.g. France), ISPs are bound by law to provide their customers with so-called "opt-in" filters, which are activated upon the customers' request.

To avoid state interventions in the 1990s, the World Wide Web Consortium (W3C) initiated a Platform for Internet Content Selection (PICS) to develop a global rating system that would enable users to determine their own access to Internet content (Resnick and Miller, 1996). The idea was notably supported by important publishing and media conglomerates and institutionalised through the Internet Content Rating Association (ICRA) in 1999, whose members were early Internet industry actors and supported by the European Safer Internet Action Plan from 1999 to 2002. However, the attempt to introduce similar ratings than for motion pictures and television content failed due to the lack of user adoption and the difficulty to rate highly dynamic and ever-increasing amounts of Internet content (Mueller, 2010; Brown and Marsden, 2013; Oswell, 1999).

2.2.3 Enforcement through intermediaries

Enforcement through intermediaries has become increasingly popular to avoid the pitfalls of other techniques mentioned previously. Following Zittrain (2003, 11), this method promises easier enforcement but less legal certainly. Intermediaries can be situated at the source or destination of content. Destination ISPs present the particular attraction for law officials to be situated within a state's jurisdiction and are thus more readily subject to regulation. "Intermediary-based regulations", bottleneck or "chokepoint" regulation (Froomkin, 2011) allow governments to transfer the technical implementation of their content legislation to those providing access to the Internet. Boyle (1997, 202) noted already in the 1990s that "the turn to privatised and technologically-based enforcement to avoid practical and constitutional obstacles seems to be the rule rather than the exception". Since, the reliance on private actors has steadily increased. For Marsden (2011, 12) "governments have outsourced constitutionally fundamental regulation to private agents, with little or no regard for the legitimacy claims". In practice, ISPs thus adopt self-regulatory or co-regulatory practices in association with governmental or independent institutions (Marsden, 2011; McIntyre, 2012). This way of action tends to become standard in governmental regulation but raises questions of effectiveness, transparency and accountability.

ISPs are not the only intermediaries in a position to enforce content regulations. Information providers (e.g. search engines), financial intermediaries, DNS registrars and hardware and software producers are also key actors. Zittrain and Edelman (2002) noted already in 2002 that Google filtered its search results in accordance with local laws, e.g. removing nazi propaganda and right extremism in Germany. Goldsmith and Wu (2006) point to the regulation of financial intermediaries in the U.S. to fight offshore gambling websites. By forbidding all major credit card institutions to transfer money to offshore gambling accounts, the U.S. government has effectively impacted user behaviour. It is still possible for U.S. citizens to engage in offshore gambling but the transaction procedure is significantly higher than previously. Also, commercial owners of the Internet's infrastructure (financial intermediaries, website hosts, etc.) play an essential role in that they can deny service to controversial speakers thus depriving these of being heard. After whistleblower WikiLeaks released thousands of U.S. diplomatic cables in 2010, its domain name was rapidly made unavailable, its data refused hosting by Amazon's cloud computing platform and the most popular forms of payment services to WikiLeaks were interrupted. The organisation, the website and the person of Julian Assange rapidly came under attack by both private and public actors (Benkler, 2011). WikiLeaks is an extreme case that still triggers wide debate. It illustrates nonetheless that the U.S. government could not directly prevent the Website from publishing the controversial cables. The termination of its hosting platform can also be considered a minor inconvenience, given that various other actors across the globe offered rapid hosting and mirrored the cables on hundreds of websites. Removing content from the Internet once it generates broad public interest is thus near-to-impossible.[12] The interruption of services by all major global financial intermediaries is however more problematic. It resulted in the loss of 95% of WikiLeaks revenue and lead WikiLeaks to publicly announce the suspension of further publications.[13] If the group continued to publish, the

[12] This phenomenon is also referred to as the "Streisand effect" following a case in which the U.S. singer and actress Barbra Streisand used legal means to remove a picture of a her villa online, unwillingly generating so much publicity that the picture was replicated to such an extent that the legal action had to be abandoned.

[13] Addley, Esther and Deans, Jason (24 October 2011). "WikiLeaks suspends publishing to fight financial blockage", *The Guardian*, available at: http://www.guardian.co.uk/media/2011/oct/24/wikileaks-suspends-publishing.

activity is considerably reduced and WikiLeaks continues to face financial difficulties.[14]

If it is true that other intermediaries should not be overlooked, ISPs and online content providers (OCPs) merit particular attention. As "gatekeepers" of the Internet, ISPs have the technical capability to monitor their user's activities and are able to block access to particular types of content through ever-more sophisticated blocking techniques (for an overview see Murdoch and Anderson, 2008). OCPs such as Facebook or Google attract millions of users on what has been called "quasi-public spheres", spaces that function as shopping malls or town-squares in the digital realm. However, their content policies are largely defined by their terms of use and contract law that does not benefit from the same constitutional free speech protections than governmental regulations (York, 2010; MacKinnon, 2012). Nonetheless, their content policy decisions impact millions of users across the world. For MacKinnon (2012) these giant Internet companies represent in fact new "corporate sovereigns" that make crucial decisions about the type of content one can access or not. In her 2012 book "Consent of the networked" she demands increased transparency and accountability from corporate and governmental sovereigns, rejecting however a state-led initiative or stricter legislation. A further self-regulatory measure that has attracted attention is the Global Network Initiative, a process set up by Yahoo, Google, Microsoft, human rights groups and academics in 2006 to reflect about how companies can uphold human rights in the digital realm particularly when operating in authoritarian regimes.[15] A number of reports and human rights commitments have resulted from the initiative, which failed however in attracting further corporations to join the effort.

[14] Greenberg, Andy (18 July 2012). "WikiLeaks Reopens Channel for credit card donations,d ares Visa and MasterCard to block them again", *Forbes*, available at: http://www.forbes.com/sites/andygreenberg/2012/07/18/wikileaks-reopens-channel-for-credit-card-donations-dares-visa-and-mastercard-to-block-it-again/.

[15] The European Parliament has for instance demanded sharper export controls of dual-use technologies. See: European Parliament (27 September 2011). *Controlling dual-use exports*. Available at: http://www.europarl.europa.eu/news/en/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports.

In the mid-1990s, many Internet industry actors in liberal democracies established private organisations, often supported by public funds, specifically to deal with sexual images of children. These private bodies set up hotlines to allow Internet users to flag problematic content and facilitate takedown and prosecution by the police. One of the more successful hotlines is run by the Internet Watch Foundation (IWF), set up in 1996 by the British Internet industry as part of the broader Inhope network, the International Association of Internet Hotlines. In the U.S. the National Center for Missing and Exploited Children (NCMEC) pre-existed the Internet but increasingly focuses on online child abuse. Hotlines were a response to the fact that the police was not able to effectively deal with illegal content online (Mueller, 2010). A second reaction were rating systems that equally developed in the 1990s but failed as indicated previously. The organisations behind the hotlines, such as the IWF, then converted to supporting the current notice-and-takedown system.

Internet service providers (ISPs) are generally exempt from liability for the content carried or hosted on their servers as long as they are unaware of its illegal nature and remove the content swiftly upon notification. This principle has notably been enshrined in the U.S.[16] and the European "mere conduit" (e-commerce directive, 2000) provisions. The importance of this principle has been repeatedly underlined by advocacy groups and international organisations (La Rue, 2011; OECD, 2011). However, the current notice-and-take down regime encourages ISPs to swiftly remove content as soon as they are notified of its potentially illegal or harmful nature to avoid liability issues. This results in so-called "chilling effects" on free speech as content is taken down upon notification with no or limited assessment on whether it is actually illegal. A growing number of reports suggest that perfectly legal content is being removed under notice-and-takedown procedures.[17] When

[16] Section 230 of the Communications Decency Act (CDA) states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". Sections of the Digital Millennium Copyright Act (DMCA, 1998) also provide "safe harbor" provisions for copyrighted material.

[17] The website http://www.chillingeffects.org/, a project of the Electronic Frontier Foundation (EFF) and various U.S. universities, aims to inform Internet users about their rights in dealing with

not complying with take-down-requests, ISPs or OCPs risk to be held liable, as has recently been the case with Google and Yahoo in two defamation cases in Australia.[18]

Furthermore, research by Moore and Clayton (2009) indicates that there are strong variations in removal times after a request depending on the type of content being taken done. Despite lacking an overarching legal framework, phishing websites[19] are removed very rapidly while child abuse images, which are illegal across the globe, suffer long removal times. The authors argue that this has to do with the incentive of the involved actors, banks acting very promptly while child abuse images are dealt with by the police and encounter many jurisdictional issues when not being situated within the police's country.

To overcome critiques about notice-and-take down excesses, Google publishes since 2009 all state-initiated removal requests as part of its Google Transparency Report. This provides a useful source of information of what type of content is requested to be removed by which state actors and for which reasons. Among the countries that request most content to be removed are the U.S. and Germany, although no reliable information is available for China for instance. Google also lists the requests from copyright owners. Figure 2 presents a screenshot from the rapid increase in copyright removal requests addressed to Google search per week.[20] Since July 2012, the requests have increased exponentially.

notice-and-takedown requests and documents abuses of the DMCA safe harbor provision in chilling legitimate speech.

[18] Holland, Adam (28 November 2012). Google Found Liable in Australian Court for Initial Refusal to Remove Links, in: *Chilling Effects*, accessed on 18 December 2012 at:http://www.chillingeffects.org/weather.cgi?WeatherID=684

[19] Phishing websites are sites that appear genuine (typically banking sites) to dupe Internet users to enter their passwords and login credential to be used for fraud.

[20] Google Transparency Report, *Copyright removal Requests*, retrieved on January 18, 2013 from: https://www.google.com/transparencyreport/removals/copyright/.

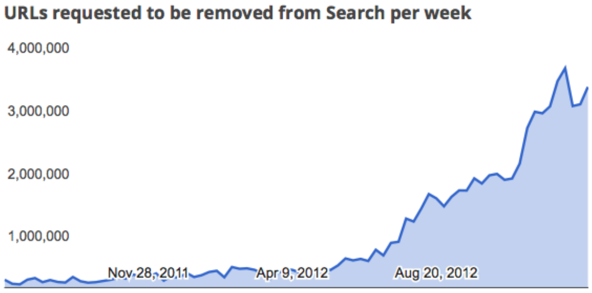

Figure 2: Copyright removal requests to Google search per week

As a result of the difficulty to control or restrict digital content, Internet blocklists have become increasingly popular to deal with problematic content. In the UK for instance, the IWF started to use a blocklist from 2004 onwards that near to all ISPs use voluntarily or to prevent governmental legislation. Blocklists establish a system of “upstream filtering”, without consulting the users whose access is affected (Edwards, 2009; McIntyre, 2012). Internet filtering or blocking technologies “provide an automatic means of preventing access to or restricting distribution of particular information” (McIntyre and Scott, 2008, 109). They resemble traditional forms of censorship (e.g. the Index of the Catholic Church) but many authors argue that because of their automatic and self-enforcing nature, they are qualitatively different from prior forms of content control and pose new problems in particular in terms of accountability and legitimacy (Brown, 2008; McIntyre and Scott, 2008; Deibert *et al.*, 2008; McIntyre, 2012). Studying Internet content restrictions remains however challenging notably due to technological and methodological issues.

2.3 Assessing Internet filtering and directions for future research

The assessment of automatic or technology-based content restrictions has only just began, predominantly by legal scholars reflecting on the legitimacy and accountability of this type of mechanisms (section 2.3.1). The technical nature of filtering systems has also been investigated with research only just emerging on the political and economic drivers of filtering systems (section 2.3.2).

2.3.1 Legal and democratic questions

Internet blocking techniques have led to several occasions of “over-blocking”, where legitimate content was equally blocked,[21] and are often criticised for being ineffective as Internet users can choose from a wide-range of tools to circumvent blocking. As Brown and Marsden (2013) state the “super-user” is in effect able to bypass information controls. However, this is not the case of the broad majority of users. Also, the absence of information of what type of content is blocked and by whom lacks any clear accountability mechanism. Automatic blocking poses a series of democratic questions in relation to the proportionality of Internet blocking, fundamental rights of freedom of expression, privacy and questions of due process and the rule of law in what regards their implementations.

Authors such as Bambauer (2009) have thus called for process-tracing frameworks to assess Internet filtering regimes in light of a series of democratic principles, in particular in terms of openness, transparency, narrowness and accountability. Initiatives such as the British IWF would fail on most of these criteria despite being successful in removing child porn from UK servers argues Edwards (2009). The problem is indeed that private organisations such as the IWF perform a “quasi-judicial” function and that content is removed without any intervention of a judge and is not held accountable for its actions. In the case of the Wikipedia over-blocking mentioned previously, the discussion centred around the lack of legal competence of the IWF for deciding whether the image was illegal or not, the fact that no notification about the blocking had been given and that no possibility for appeal existed at the time (Edwards, 2009). Blocking systems remain thus particularly vulnerable to questions of effectiveness and the respect of democratic principles and human rights. However, many authors do not outrightly reject blocking techniques anymore but argue for increased

[21] Blocklists have sometimes been leaked on the Internet. The Australian’s Communications and Media Authority (ACMA) blocklist was leaked by WikiLeaks in 2009 and several sites were detected as non-conform to ACMA’s content rating system, for instance the Website of a dentist in Queensland. More recently, in March 2012, more than 8000 Websites, including Google and Facebook, were blocked by the Danish child pornography list. See EDRi (14 March 2012). *Google and Facebook Blocked by the Danish Child Pornography Filter*, available at: http://www.edri.org/edrigram/number10.5/danish-filter-blocks-google-facebook.

transparency and accountability to be introduced to the existing systems (see for instance Bambauer, 2009; Edwards, 2009 for a critical stance on this development see Mueller, 2010)

Much of the literature on Internet blocking in particular adopts a legal perspective by focusing on particular types of content blocking (e.g. child pornography for McIntyre, 2012) or particular countries (for Germany alone, two dissertations have been published analysing the implications of Internet blocking in light of the particular legal system. See Greve, 2011; Heliosch, 2012). Country comparisons remain the exception.

Brown and Marsden (2013) use a transdisciplinary framework to assess “hard cases” of Internet governance, including online censorship principally in the anglo-saxon world and the “usual suspects” of Internet blocking China and Iran. They conclude to the near-to absence of appeal and due process principles and overall reduced democratic scrutiny. They call for the development of international standards and the adoption of best practices (e.g. the IWF before it engaged into automatic blocking, banks’ responses to phishing and a combination of spam filtering and takedown procedures). The “[a]nswer should be to go to [the] source: arresting producers not blocking viewing” (2013, 309).

The political controversies and discourses surrounding Internet blocking have until recently been the object of little research. McIntyre and Scott (2008) explored the rhetoric underlying blocking proposals, with McIntyre (2012) distinguishing between two main arguments advanced against Internet blocking: practical and principled ones. Practical arguments refer to the functional aspects of Internet blocking such as the blocking techniques used and whether Internet blocking is an effective form of stopping the diffusion of problematic content and the societal issues that drive the production and diffusion of such content. Principled arguments directly appeal to democratic and human rights principles, mainly freedom of expression and constitutional safeguards such as due process, public oversight or transparency and accountability mechanisms. Breindl (2012) and Breindl and Wright (2012) proposed an analysis of the networks of actors and discourses surrounding two government proposals to introduce Internet blocking of "child pornography" in France and Germany. Breindl (2012) concludes that the characteristics of the network of actors of the opponents to Internet blocking was structurally different in both countries. The German opponents' network was particularly large and cohesive. Furthermore, they dominated all core frames of the debate, succeeding in providing a coherent alternative in "removing not blocking" the content. In France, however, the debate was largely dominated by other issues, leaving few discursive opportunities to challengers of Internet blocking, which was eventually adopted in France and revoked in Germany.

2.3.2 Measuring technological blocking

Internet filtering and blocking is based on a diversity of technologies, including DNS tampering, IP header filtering, deep packet inspection or end-user filtering softwares (Murdoch and Anderson, 2008). These techniques are often combined into hybrid filters, with states starting with IP address or DNS filtering to move onto more sophisticated methods to increase effecttiveness (Deibert *et al.*, 2008, 2010). The EU's CIRCAMP blocklist, used by various national hotlines, relies on DNS filtering, even though it can be easily circumvented. British Telecom's Cleanfeed system employs a hybrid filter. In the U.S., the National Centre for Missing and Exploited Children (NCMEC) provides "voluntary" blocklists to ISPs since 2007, many of who*m* use them to filter their networks. Some companies, such as AT&T, also use the so-called hash-values provided by NCMEC to monitor and filter private communications for known images based on their hash value, thus including non-Web content (McIntyre, 2012). Computer science literature focuses on the detailed implementations of this type of blocking techniques principally in authoritarian regimes (for China, see for instance Wright *et al.*, 2011, but see Clayton (2005) for an analysis of the UK Cleanfeed system; see also our technical report about Internet blocking).

Policy-analyses of the development of filtering regimes, in particular in liberal democracies, are lacking. The Open Network Initiative (ONI) has been the frontrunner with the publication of the Access books (Deibert *et al.*, 2008, 2010, 2011a), including detailed country profiles. Their research represents the first systematic attempt to document information restrictions around the globe. Their research methods combine on-the-ground fieldwork and collaboration with local experts to the measurement of content restrictions using specialised software (Faris and Villeneuve, 2008). Their testing focuses on user reports of blocked content notably through the crowd-sourced website Herdict, set up by the Berkman Center for Internet & Society at Harvard University. Their measurement results in scores ranging from pervasive, substantial, selective, suspected to no evidence of filtering for four broad categories of political, social, conflict and security and Internet tools types of content. They then correlate the filtering scores to World bank indicators of the rule of law and voice and accountability, concluding to no straightforward relationship between the rule and law and Internet filtering while countries who hold low voice and accountability scores also hold strong filtering scores (Faris and Villeneuve, 2008). For liberal democracies, Deibert *et al.* (2010) find no evidence of filtering also because, for legal and ethical reasons, ONI abstains from measuring child pornographic content (Faris and Villeneuve, 2008). In comparison to authoritarian regimes, liberal democracies therefore show no evidence of filtering while many anecdotal evidence suggests growing filtering in these countries too.

Non-academic reports provided by NGOs and freedom of expression advocates (see for instance the annual reports by Freedom House, 2012; Reporters without borders, 2012) provide an important source of information about what type of content is blocked in the countries included in the reports. Publications by advocacy groups such as European Digital Rights (McNamee, 2011a, b) or AK Vorrat provide often up-to-date information on latest developments in Internet blocking. Groups such as the Tor network, which developed the widely used circumvention tool, are also interested in gathering data about online blocking and developed the Open Observatory of Network Interference (OONI), which provides only data about blocking incidents in two countries for the moment but might be expanded in the future.

The lack of reliable data measuring Internet blocking has already been invoked in 2003 by Zittrain, who subsequently participated in building up

ONI and Herdict. More recently, the New America Foundation's Open Technology Institute, The PlanetLab Consortium, Google Inc. and individual researchers have initiated the Measurement Lab, a Web platform that can host a variety of network measurement tools for broadband and mobile connections. While some of the available tests are more specifically targeted at measuring the quality of broadband connections, the use of deep-packet inspection (DPI), a technology that allows to open up data packets and examine their content has come to the centre of attention more recently. DPI is used for a variety of reasons including bandwidth management, network security or lawful interception but can also be used to regulate content, prioritise certain products over competing services, target advertising or enforce copyright (Bendrath and Mueller, 2011). As a result, several teams of researchers have developed new tools to measure and assess DPI use by Internet service providers, which is unregulated in most countries (see for instance Dischinger *et al.*, 2010).

First academic assessments have emerged: Dischinger *et al.* (2008) for instance assessed Bit Torrent blocking, presenting particularly high values for U.S. ISPs such as Comcast. More recent research by Mueller and Asghari (2012) and Asghari *et al.* (2012b), using the Glasnost test available on M-Lab, investigate the particular use of DPI technology for throttling or blocking peer-to-peer (P2P) applications over three years. They use bivariate analysis to test possible correlations for economic and political drivers of DPI technology and its implementation by 288 ISPs in 75 countries.[22]

They find that DPI use is surprisingly widespread worldwide, including in liberal democracies in particular in Canada and the UK. They find that market factors such as bandwidth scarcity, costs of bandwidth and lower levels of competition correlates with higher DPI use. Furthermore, political factors such as governmental censorship and weak privacy protections correlate with higher DPI use. Contrary to their initial expectations, they find that the strength of the copyright industry does not correlate with DPI use by ISPs. Similarly, network security correlates negatively with the ISPs DPI use.

[22] For a critical assessment of methodological issues regarding Internet throttling measurements see Asghari *et al.* (2012a).

Interestingly, Mueller and Asghari (2012) find that governmental regulation in the U.S. and Canada did not impact DPI use. In both countries, DPI use resulted in public protests, litigation and the development of new regulation based on net neutrality principles. The public confrontation clearly impacted DPI use in the U.S. where ISPs considerably decreased their use of the technology, even when the FCC ruling was challenged. In Canada, however, the new, uncontested, regulation did not reduce DPI use, which actually increased after the regulation was passed. Legislation alone is therefore not able to explain this apparent paradox.

3 Future research

The literature review presented the main research questions and findings on Internet content regulation as they have evolved since the introduction of the Internet in the early 1990s. Of particular interest is the nature of new regulatory arrangements that range from self- to co- to state regulatory interventions (see also Marsden, 2011) set in place to respond to growing concerns about a wide range of illegal or harmful content such as copyright infringing material or content deemed harmful to minors or threatening public order.

The various techniques and points of control have been discussed to highlight where states and private actors could intervene to control digital information flows. Particular attention has been paid to blocking techniques and the legal and democratic implications of these. Finally, we have discussed recent research providing empirical evidence of the amount of blocking carried out in liberal democracies, identifying several shortcomings.

First, there remains a lack of reliable and longitudinal data about what type of content is blocked or removed by which type of actor, where and through which process. Recent initiatives such as the M-Lab provide first opportunities to gather and analyse large amounts of data but present nonetheless several methodological challenges (see for instance Asghari *et al.*, 2012a). Regulatory authorities such as the U.S. Federal Communications

Commission (FCC) or the Body of European Regulators for Electronic Communications (BEREC) are in the process of carrying out large broadband connection tests that might result in relevant data for this research project in the coming years.

Second, there is a clear opportunity to carry out a comparative public policy research project specifically on liberal democracies. As much of the literature has until now focused on authoritarian regimes, liberal democracies merit to be examined in their own rights. They present both possibilities and challenges for research. On the one hand, there exist more reliable data and indicators about the political and institutional systems in liberal democracies. On the other hand, Internet blocking initiatives are often carried out by private actors and lack democratic scrutiny and public oversight. Access to reliable data remains, again, a challenge.

Finally, there has been limited attention for the political drivers and factors surrounding the adoption and implementation of blocking techniques. Much of what we know about Internet blocking in liberal democracies is the result of media reports, freedom of expression advocates with little systematic analysis. Future research will benefit from a comparative and systematic perspective on Internet blocking in liberal democracies in particular.

References

Akdeniz, Y. (2010). To block or not to block: European approaches to content regulation, and implications for freedom of expression. *Computer Law & Security Review*, 26:260–272.

Asghari, H., Mueller, M. L., van Eeten, M. J. G., and Wang, X. (2012a). “Making Internet measurements accessible for multi-disciplinary research. an in-depth look at using M-Lab’s Glasnost data for policy research”. Submitted to IMC’12.

Asghari, H., van Eeten, M. J. G., and Mueller, M. L. (2012b). “Unravelling the economic and political drivers of deep packet inspection. An empirical study of DPI use by broadband operators in 75 countries”. Paper presented at the GigaNet 7th Annual Symposium, November 5, Baku, Azerbaijan.

Bambauer, D. E. (2009). Guiding the censor’s scissors: A framework to assess Internet filtering. *Brooklyn Law School. Legal Studies paper*, (149):1–72.

Bendrath, R. and Mueller, M. (2011). The end of the Net as we know it? deep packet inspection and Internet governance. *New Media & Society*, 13(7):1142–1160.

Benkler, Y. (2011). A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate. Working draft. Forthcoming in *Harvard Civil Rights-Civil Liberties Law Review*.

Boas, T. (2006). Weaving the authoritarian web: The control of Internet use in non-democratic regimes. In: Zysman, J. and Newman, A., editors, *How revolutionary was the digital revolution? National responses, market transitions, and global technology*, pp. 361–378. Stanford University Press, Palo Alto, CA.

Boyd, Danah (2008). *Taken Out of Context. American Teen Sociality in Networked Publics*. PhD thesis, University of California, Berkeley.

Boyd, Danah (2009). Social media is here to stay... now what? http://www.danah.org/papers/talks/MSRTechFest2009.html. Paper presented at the Microsoft Research Tech Fest, Redmond.

Boyle, J. (1997). Foucault in cyberspace, surveillance, souvereignty, and hard-censors. *University of Cincinnati Law Review*, 66:177–205.

Braman, S. (2009). *Change of State: Information, Policy, and Power*. MIT Press, Cambridge, MA.

Breindl, Y. (2012). “Discourse networks on state-mandated access blocking in France and Germany”. Paper presented at the 7th GigaNet Symposium, November 5, Baku, Azerbaijan.

Breindl, Y. and Briatte, F. (2013). Digital network repertoires and the contentious politics of digital copyright in France and the European Union. *Policy & Internet*, forthcoming.

Breindl, Y. and Wright, J. (2012). “Internet filtering trends in liberal democracies: French and German regulatory debates”. Paper presented at the FOCI’12 workshop, 2nd USENIX workshop on Free and Open Communications on the Internet, August 6, 2012, Bellevue, WA.

Brown, I. (2008). Internet filtering – be careful what you ask for. In: S.Kirca and L.Hanson, editors, *Freedom and Prejudice: Approaches to Media and Culture*, pp. 74–91. Bahcesehir University Press, Istanbul.

Brown, I. (2010). Internet self-regulation and fundamental rights. *Index on Censorship*, 1:98–106.

Brown, I. and Korff, D. (2012). “Digital freedoms in international law. Practical steps to protect human rights online”. Technical report, Global Network Initiative.

Brown, I. and Marsden, C. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*. MIT Press, Cambridge, MA.

Busch, A. (2012). Politische Regulierung von Information – eine Einführung. In: Busch and Hofmann (2012), pp. 24–47.

Busch, A. and Hofmann, J. (2012). In: Busch, A. and Hofmann, J., editors, *Politik und die Regulierung von Information*, volume 46 of *Politische Vierteljahresschrift*. Nomos, Baden-Baden, Germany.

Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press.

Clayton, R. (2005). “Failures in a hybrid content blocking system”. Presented at the Workshop on Privacy Enhancing Technologies, Dubrovnik, Croatia.

Clayton, R., Murdoch, S. J., and Watson, R. N. M. (2006). Ignoring the great firewall of China. In: Danezis, G. and Golle, P., editors, *Privacy Enhancing Technologies workshop (PET 2006), LNCS*. Springer.

Deibert, R. J. and Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance*, 18(3):339–261.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Information Revolution and Global Politics. MIT Press, Cambridge, MA.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Information Revolution and Global Politics. MIT Press, Cambridge, MA.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2011a). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Information Revolution and Global Politics. MIT Press, Cambridge, MA.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2011b). Access contested: Toward the fourth phase of cyberspace controls. In: Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J., editors, *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, Information Revolution and Global Politics, pp. 3–20. MIT Press, Cambridge, MA.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance*. MIT Press, Cambridge, MA.

DeNardis, L. (2010). “The privatization of Internet governance”. Paper presented at the GigaNet 5th Symposium, Vilnius, Lithuania.

DeNardis, L. (2012). Hidden levers of Internet control. *Information, Communication & Society*, 15(5):720–738.

Dischinger, M., Gummadi, K. P., Marcon, M., Mahajan, R., Guha, S., and Saroiu, S. (2010). “Glasnost: Enabling end user to detect traffic differentiation”. Paper presented at the USENIX Symposium on Networked Systems Design and Implementation (NSDI).

Dischinger, M., Mislove, A., Haeberlen, A., and Gummadi, K. P. (2008). “Detecting bittorrent blocking”. Paper presented at IMC.

Dutton, W. H., Dopatka, A., Hills, M., Law, G., and Nash, V. (2011). F”reedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet”. Technical report, [UNESCO].

Dyson, E., Gilder, G., Keyworth, G., and Toffler, A. (1996). Cyberspace and the American dream: A magna carta for the knowledge age. *Information Society*, 12(3):295–308.

Edwards, L. (2009). Pornography, Censorship and the Internet. In: Edwards, L. and Waelde, C., editors, *Law and the Internet*. Hart Publishing, Oxford, UK.

Faris, R. and Villeneuve, N. (2008). Measuring global Internet filtering. In: Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J., editors, *Access Denied: The Practice and Policy of Global Internet Filtering*, Information Revolution and Global Politics, pp. 5–28. MIT Press, Cambridge, MA.

Flichy, P. (2001). *L’imaginaire d’Internet*. La Découverte, Paris.

Freedom House (2012). “Freedom on the Net 2012. A Global Assessment of Internet and Digital Media”. Technical report, Freedom House.

Froomkin, M. (2011). “Lessons learned too well: The evolution of Internet regulation”. Technical report, CDT Fellows Focus series.

Fuchs, C. (2012). Implications of deep packet inspection (dpi) Internet surveillance for society. *The Privacy & Security – Research Paper Series 1*, Uppsala University.

Goldsmith, J. and Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press, Oxford/New York.

Greve, H. (2011). *Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet*. PhD thesis, Humboldt Universität zu Berlin.

Haunss, S. (2011). The Politicization of Intellectual Property: IP Conflicts and Social Change. *WIPO Journal*, 3(1):129–138.

Heliosch, A. (2012). *Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von kinderpornographischen Inhalten im Internet*, volume 10 of *Göttinger Schriften zur Internetforschung*. Göttinger Universitätsverlag.

Hintz, A. (2012). Challenging the digital gatekeepers: International policy initiatives for free expression. *Journal of Information Policy*, 2:128–150.

Hofmann, J. (2012). Information und Wissen als Gegenstand oder Ressource von Regulierung. In: Busch and Hofmann (2012), pp. 5–23.

Johnson, D. R. and Post, D. G. (1996). Law and borders – the rise of law in cyberspace. *Stanford Law Review*, 48(5):1367–1402.

Johnson, P. (1997). Pornography drives technology: Why not to censor the Internet. *Federal Communications Law Journal*, 49(1):217–226.

Katz, J. (1997). Birth of a digital nation. *Wired*, 5(04).

Klang, M. (2005). “Controlling online information”. Paper presented at WSIS, Internet Governance and Human Rights, Uppsala, Sweden.

Kuehn, A. (2012). *Cookies versus Clams. Tracking Technologies and their Implications for Online Privacy*, Paper presented at the GigaNet 7th Annual Symposium, November 5, Baku, Azerbaijan.

La Rue, F. (2011). “Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression”. Technical Report A/HRC/17/27, Human Rights Council Seventeenth session Agenda item 3.

Lessig, L. (1999). *Code: And Other Laws of Cyberspace*. Basic Books, Cambridge, MA.

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books, New York.

Löblich, M. and Wendelin, M. (2012). ICT policy activism on a national level: Ideas, resources and strategies of German civil society in governance processes. *New Media & Society*, 14(6):899–915.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle For Internet Freedom*. Basic Books, New York.

Marsden, C. (2010). *Net Neutrality: Towards a Co-Regulatory Solution*. Bloomsbury Publishing, London.

Marsden, C. T. (2011). *Internet co-regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace*. Cambridge University Press, UK.

McIntyre, T. (2012). Child abuse images and cleanfeeds: Assessing Internet blocking systems. In: Brown, I., editor, *Research Handbook on Governance of the Internet*. Edward Elgar, Cheltenham.

McIntyre, T. J. and Scott, C. (2008). Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility. In: Brownsword, R. and Yeung, K., editors, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, pp. 109–124. Hart Publishing, Oxford, UK.

McNamee, J. (2011a). “Internet blocking. crimes should be punished and not hidden”. Technical report, EDRi.

McNamee, J. (2011b). “The slide from “self-regulation“ to corporate censorship”. Discussion paper, European Digital Rights.

Moore, T. and Clayton, R. (2009). The Impact of Incentives on Notice and Take-down. In: *Managing Information Risk and the Economics of Security*, pp. 199–223. Springer US.

Mueller, M., Pagé, C., and Kuerbis, B. (2004). Civil society and the shaping of communication information policy: Four decades of advocacy. *The Information Society: An International Journal*, 20(3):169.

Mueller, M. L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Information Revolution and Global Politics Series. MIT Press, Cambridge, MA.

Mueller, M. L. (2010). *Networks and States: the global politics of Internet governance*. Information Revolution and Global Politics Series. MIT Press, Cambridge, MA.

Mueller, M. L. and Asghari, H. (2012). Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States. *Telecommunications Policy*, 36(6):462–475.

Murdoch, S. J. and Anderson, R. (2008). Tools and technology of Internet filtering. In: Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J., editors, *Access Denied: The Practice and Policy of Global Internet Filtering*, Information Revolution and Global Politics, pp. 29–56. MIT Press, Cambridge, MA.

Murray, A. D. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. Routledge Cavendish, Oxford, UK.

Murray, A. D. and Scott, C. (2001). “The partial role of competition in controlling the new media”. Presented at the Competition Law and the New Economy University of Leicester.

Musiani, F. (2011). Privacy as Invisibility: Pervasive Surveillance and the Privatization of Peer-to-Peer Systems. *tripleC – Cognition, Communication, Co-operation*, 9(2):126–140.

OECD (2011). “Joint declaration on freedom of expression and the Internet”. Technical report, OECD.

Oswell, D. (1999). The dark side of cyberspace Internet content regulation and child protection. *Convergence: The International Journal of Research into New Media Technologies*, 5(4):42–62.

Rasmussen, T. (2007). Techno-politics, Internet governance and some challenges facing the Internet. Research Report 15, Oxford Internet Institute.

Reidenberg, J. (1998). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review*, 76(3):553–584.

Reporters without borders (2012). “Internet enemies 2012”. Report, Reporters without borders for Press Freedom.

Resnick, P. and Miller, J. (1996). PICS: Internet access controls without censorship. *Communications of the ACM*, 39(10):87–93.

Vanobberghen, W. (2007). “’The Marvel of our Time’: Visions about radio broadcasting in the Flemish Catholic Press, 1923–1936”. Paper presented at the 25th IAMCR conference, Paris, France.

Villeneuve, B. (2010). Barriers to Cooperation. An Analysis of the Origins of International Efforts to Protect Children Online. In: Deibert *et al.* (2010), pp. 55–70.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy*, 36(6):484–492.

Wellman, B. (2001). Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research*, 25(2):227–252.

Wright, J., de Souza, T., and Brown, I. (2011). Fine-grained censorship mapping – information sources, legality and ethics. In: *Proceedings of Freedom of Communications on the Internet Workshop*.

Wu, T. (2010). *The Master Switch: The Rise and Fall of Information Empires*. Atlantic Books, London.

York, J. C. (2010). “Policing content in the quasi-public sphere”. Technical report, Open Net Initiative Bulletin.

Yu, P. (2010). The Graduated Response. *Florida Law Review*, 62:1373–1430.

Yu, P. K. (2004). The Escalating Copyright Wars. *Hofstra Law Review*, 32:907–951.

Zeno-Zencovich, V. (2009). *Freedom of Expression: A Critical and Comparative Analysis*. T & F Books UK.

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

Zittrain, J. (2008). *The Future of the Internet – And How to Stop It*. Yale University Press, New Haven, CT.

Zittrain, J. and Edelman, B. (2002). “Localized Google search result exclusions: Statement of issues and call for data”. Available at http://cyber.law.harvard.edu/filtering/google/.

Zittrain, J. and Palfrey, J. G. (2008). Internet filtering: The politics and mechanisms of control. In: Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J., editors, *Access Denied: The Practice and Policy of Global Internet Filtering*, Information Revolution and Global Politics, pp. 29–56. MIT Press, Cambridge, MA.