



Article

Policing the Network: Using DPI for Copyright Enforcement

Milton Mueller

School of Information Studies, Syracuse University, USA. mueller@syr.edu

Andreas Kuehn

School of Information Studies, Syracuse University, USA. ankuhn@syr.edu

Stephanie Michelle Santoso

School of Information Studies, Syracuse University, USA. smsantos@syr.edu

Abstract

Deep Packet Inspection (DPI) and other network surveillance techniques have become important factors in the policy debate over online copyright infringement. These new technical capabilities reopened an old debate about the responsibility of Internet service providers (ISPs) for policing the Internet. This paper attempts to understand the extent to which new technological capabilities have the power to alter regulatory principles. It examines political conflict and negotiation over proposals to use DPI for online copyright enforcement in the EU and the USA, using a hybrid of actor-network theory from science, technology and society studies and actor-centered institutionalism in political science. It shows that while the technology disrupted a policy equilibrium, neither the EU nor the US applied DPI to copyright policing in a way that realized its radical potential. The key factor preventing such an integrated response was the disjunction between the interests of network operators and the interests of copyright holders.

Introduction

The Internet created a new, globalized virtual space. A vast expanse for communication opened up to its users, one with very few established institutions and controls. That initial freedom created many benefits, but it also incubated new forms of conflict and crime. This has led to growing calls for more controls. One of the most high-stakes clashes over Internet regulation involves copyright protection. By radically amplifying users' ability to locate and share media objects, the Internet has undermined the exclusivity of recorded music, movies, books and software. For more than 15 years, the fate of the multi-billion dollar market for digital media has sparked intense political, economic and regulatory contention (Samuelson 1996; Litman 2001; Bach 2004; Gillespie 2007; Horten 2011). Copyright holders are a powerful, globally organized economic interest group. Trade organizations such as the Business Software Alliance (BSA), the International Federation of the Phonographic Industry (IFPI), and the Motion Picture Association (MPA) have strong influence over policymakers in national and international arenas. But the rights holders' policy agenda often clashes with that of Internet service providers (ISPs), who resist the burdens of policing and enforcement. Opposition to the rights holders' agenda also comes from supporters of

Mueller, Milton, Kuehn, Andreas, and Santoso, Stephanie Michelle. 2012. *Surveillance & Society* 9(4): 348-364.

<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author(s), 2012 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Internet freedom and access to knowledge, who believe that copyright and other forms of intellectual property protection are being transformed into needlessly rigid controls on online activity (Vaidhyanathan 2001; Stallman 2002; Lessig 2005). This battle has been described as one of the four key drivers of global Internet governance (Mueller 2010: 129-157).

Ten to fifteen years ago, it was unthinkable to contemplate regulatory mechanisms predicated on the notion that the network itself could monitor the activities of users and automatically detect and stop illegal or objectionable activity. Yet the progress of information technology now makes it not only thinkable, but in some respects doable. Most radically, a network management and surveillance technology known as deep packet inspection (DPI) can be used to detect copyrighted files as they move over the Internet, and trigger notifications or even blocking. Other network surveillance techniques can also be used, such as participating in file-sharing groups to identify media files and gather the Internet Protocol (IP) addresses of those involved. Those new capabilities are the topic of this paper. We highlight networks as the site of policy contention and examine the way DPI has been promoted, debated or implemented in the battles over copyright protection. The salient question is whether the emergence of a new technological capability – in this case, an enhanced ability to automatically examine, identify and act upon objects as they move through the network – is changing the way we govern the Internet. This is not just a question about public policy, but a deeper one about the relationship between technology and society.

DPI and Intermediary Responsibility

Network surveillance capabilities intrude upon a longstanding debate over the responsibilities of ISPs. Both the US and Europe have promoted Internet growth and openness by explicitly limiting network operators' liability for their users' actions (Casey 2000; Harrelson 2010). Section 230 of the 1996 Communications Decency Act immunizes US ISPs from liability for communications by their users. Section 512 of the Digital Millennium Copyright Act (DMCA) explicitly limits the responsibility of an American service provider for publication of infringing material they are unaware of. At the same time that it protects them, the DMCA obligates service providers to adhere to a strict notice and takedown policy, which requires them to expeditiously remove illegally posted content upon receiving a notice of infringement from a copyright owner. The European E-Commerce Directive (2000/31/EC) contains a similar, if somewhat weaker safe harbor. Under the Directive, ISPs have limited responsibility for transmitted or stored data when they act as 'mere conduits,' 'caches' or 'hosts'; i.e., when they do not have "actual knowledge" of the infringement. Article 15 of the Directive prevents Member States from imposing a general obligation on ISPs to monitor their network for evidence of illegal activity.

Those exemptions were thought to enhance freedom of expression and economic innovation. Making service providers responsible for third party actions would force them to monitor and restrict their users to protect themselves from legal liability. They were also predicated on the assumption that it was too costly or not technically feasible for ISPs to systematically monitor and act upon all the activity taking place on their platforms.

DPI alters the dynamics of the debate over the responsibility of Internet intermediaries. It increases the capacity of service providers to understand and act upon the traffic flowing over their facilities. Thus, there is growing inconsistency between what technology enables and the laws, governance principles and norms developed before those capabilities existed. But while DPI clearly has the *potential* to alter an established principle of Internet governance, it is also possible that its application and use will be constrained by pre-established laws, principles and norms. One cannot, *a priori*, predict how the gap between the new potential and older governance principles will be bridged. Instead, one must look empirically at how DPI is put into use, and how or whether those uses are contested politically. This article, therefore, conducts a detailed examination and comparison of the political process in Europe and the United States.

Theoretical Framework

By examining the way new network surveillance capabilities generate struggles over Internet policy, we hope to provide a more robust understanding of the relationship between changes in technology and changes in the institutions of public governance. We approach the topic using a hybrid of actor-network theory from science, technology and society studies (Law 1992), and actor-centered institutionalism in political science (Scharpf 1997). The idea of the *co-production of technology and society* serves as the conceptual anchor of this effort (Harbers 2005). Co-production is an attempt to bridge the dichotomy between realism (technological determinism) and a social constructivism that sees technology as a passive product of cultural and sociological forces with no agency of its own (Disco 2005). In our view, technology is afforded agency, but its impact is conditioned on the way it bestows differential capabilities, governance capacities, or power resources among a set of actors (Knill and Lehmkuhl 2002).

Technology-aware policy analysis (Bendrath and Mueller 2011) begins by analyzing how specific applications or uses of a new technology serve the interests of specific actors. The implementation becomes the first move in a game that triggers adjustments and countermeasures by others affected (including the technologies). We pay special attention to the institutional environment and the way it affects modes of interaction among the players. Political interactions around new technological capabilities will be shaped by existing laws and regulations, by the existence or non-existence of partisan groups promoting specific norms and their degree of organization, and by the structures and legacies of the political system. The challenge for technology-aware policy research is to empirically link the capabilities of new technologies to an analysis of the concrete conflicts and interactions around their usage and governance. The characteristics of the technologies matter, but so do the institutional settings and the specific actor constellations that form around them. Co-production is a path-dependent process in which technological capabilities and actors mutually constitute each other through strategic interactions within an institutional framework.

Copyright as an Application of DPI

Co-production requires one to take the actual features of the technology seriously. Analysis must encompass its powers and capabilities, but also its limitations and dependencies. This section thus briefly examines the technology and its application to copyright issues.

A DPI engine analyzes the traffic of an IP network in real time and considers any and all information in the packets to be subject to inspection, including the payload (Parsons 2008). The most basic and important feature of DPI is *recognition*; i.e., the ability to detect or identify objects in a bit stream (Mueller 2011). Recognition may then trigger *notification* or *manipulation* functions (Ibid). Manipulation is active intervention in a live traffic stream to optimize, control or change it. It is based on rule sets which instruct the network to behave in a certain way contingent upon recognition. Notification is an indirect form of intervention; it triggers an alert to a network administrator, initiates storage of records, or generates a billing incident without affecting the live traffic stream.

As a generic network surveillance and intervention capability, DPI has many applications. It can be programmed to detect the presence of a specific protocol (e.g., BitTorrent), and trigger manipulation functions to conserve bandwidth. DPI might be used to comply with censorship policies, by recognizing requests for the URLs of banned websites and blocking access to them. We refer to each of these applications as a distinct *use-case*. Each use-case will have different politics, because the DPI application and the institutional setting together create distinctive actor constellations and modes of interaction (Bendrath and Mueller 2011).

The copyright use-case is one of the most technically complex and politically unique. In most cases, DPI is implemented by network operators to perform functions that directly benefit their business, such as optimizing scarce bandwidth or monetizing access to services. The primary beneficiary of DPI for copyright, however, is the rights holder not the ISP. After failing to stem file-sharing in other ways, rights holders have, since 2005, pressured ISPs to take greater responsibility for policing Internet users (De Beer and Clemmer 2009; Bridy 2010). The pressure embraces not just commercial service providers, but university residential and campus networks. Copyright interests have seized upon the capabilities of surveillance technology to urge those who run networks to deploy “technical measures” to police copyright violations.

DPI for copyright enforcement works on a “fingerprinting” model. Copyright holders use a vendor’s software to generate a unique signature – a reduced digital representation – for each protected digital object. These fingerprints are stored in a registry. Unlike virus detection, DPI for copyright cannot rely on a simple bit-match or hash; it must be able to recognize copyrighted material in fragments, and in different media formats or compression levels. Thus a DPI appliance must calculate the distinctive perceptual features of the media in a way that can uniquely identify its source. It must intercept media content as it passes through the network and create a fingerprint of it, then calculate whether the fingerprint of the file it is inspecting matches that of the any one of the millions of fingerprints registered by rights holders.

There is an alternative model of copyright surveillance and enforcement that need not rely on DPI. In this model, sometimes called “over the top” (OTT), hired agents of copyright holders perform surveillance of network activity themselves, for example by operating torrents in file-sharing networks. They gather the illicitly traded media objects as a network user, using the same fingerprint-matching method to identify them, and collect the IP addresses of those involved. Then they ask ISPs to map the IP addresses to specific customer accounts, so that the users can be subjected to legal process. While this method relieves ISPs of installing DPI infrastructure, it still requires their cooperation. Only the ISP can match IP addresses to specific user accounts. ISPs may also be required to notify their users and to restrict or discontinue their service if users are deemed guilty (Meyer and Audenhove 2010). Thus, either DPI or OTT can enlist ISPs in i) surveillance of network activity, ii) the identification of users, iii) the notification of users, iv) the blocking of illicit traffic and/or v) disconnection of repeat offenders. Table 1 displays different modes of copyright enforcement. It contrasts current methods with a pure DPI-based method (inside the network) and the hybrid ‘graduated response’ model of France, which uses OTT.

Table 1
Modes of Copyright Enforcement on the Internet

Activity	Status quo	Hybrid (OTT)	Inside the Network (DPI)
Detection	Rights holder	Rights holder	ISP
Mapping	Rights holder subpoenas ISP	Government agency and ISP	ISP
Notification	Rights holder	Government agency with ISP	ISP
Enforcement	Court system	Government agency, Courts and/or ISP	ISP

Our theory leads us to believe that the application of DPI to copyright will differ in a very important respect from most other DPI applications. Most implementations directly serve the economic interests of ISPs. Copyright protection, on the other hand, is mostly inimical to an ISP’s economic interests. While it

benefits rights holders, it imposes administrative and hardware costs on the ISP, undermines their immunities and alienates or cuts off customers. We hypothesize, then, that ISPs will not adopt DPI for copyright protection services of their own volition. Either they must be forced to do so through hierarchical exercises of state regulatory authority, or the copyright owners must negotiate and provide inducements for ISPs to cooperate; some combination of both is of course possible.

With this framework in mind, we now turn to the analysis of the case studies.

DPI and Copyright Policing in the European Union

In the European Union the prospect of technical measures for online copyright enforcement led to complex, intense political interactions. Around 2005, the rights holders' agenda converged on the notion of *graduated response*, which implied a shift of responsibilities towards ISPs. Sometimes known as "three strikes," it involves ongoing surveillance of Internet users' activities, the identification and notification of those responsible for copyright infringement, and suspension or termination of Internet service for repeat offenders. The copyright holders' first political achievement was the Cannes Declaration in 2005, which expressed national Ministers' and EU Commissioners' support for "the 'graduated response' to unauthorized file-sharing or downloading of films which is being advocated in a number of Member States now [...]" (Cannes Declaration 2005).

The interaction with DPI began with a coordinated set of national-level lawsuits; it moved to national-level legislation and state-directed Memorandum of Understandings (MoUs) in the UK and France; it then metamorphosed into an EU-wide effort to rewrite the entire Union's telecommunications laws to require broadband Internet providers to police and enforce copyright. When that effort foundered, the EU brokered private negotiations among ISPs and rights holders and inaugurated EU-wide consultations on the E-Commerce Directive and the Intellectual Property Enforcement Directive.

A narrative of these events reveals that DPI capabilities were pivotal in the actor-networks. Litigants debated, and judges ruled on its efficacy; vendors of DPI equipment positioned themselves to meet the demand created by the prospect of a regime of "technical measures"; civil liberties groups mobilized around DPI's implications for user privacy and freedom; ISPs questioned its cost and feasibility for copyright enforcement, even as they used DPI for other functions. As the conflict escalated, the consistency of DPI with fundamental human rights was debated and dealt with by the European Court of Justice.

Litigation in Member States

Before it became a Europe-wide controversy, the music industry tried to use national litigation to establish a secondary liability for ISPs. This strategy appeared to succeed in June 2007, when the Belgian music industry association (SABAM) won an injunction from the Court of First Instance in Brussels requiring ISP Scarlet to install Audible Magic DPI technology to catch music piracy among its customers.

EMI, Sony, Warner and Universal then sued the largest Internet provider in Ireland, Eircom, on similar grounds. The music industry sought an injunction from the Dublin High Court in 2008 requiring Eircom to install the same Audible Magic appliance as in Belgium (McIntyre 2008). But in October 2008 the Belgian ISP convinced an appeals court that the DPI technology did not work and had not, as the music industry claimed, already been used elsewhere. The trial court in Belgium lifted the injunction against Scarlet. This pressured the music industry to reach an out of court settlement with Eircom, in which the ISP entered into a private agreement to implement a form of graduated response, one based on OTT methods rather than DPI (McIntyre 2009).

MoUs and Legislation in France and the UK

Late in 2007 a group put together by the Sarkozy government, known as the Olivennes Commission, engineered a Memorandum of Understanding (MoU) among ISPs and rights holders (Horten 2011, 83-95). It recommended a “three strikes” policy for repeat infringers. A regulatory entity would be created to oversee adherence to the agreement; non-collaboration by ISPs could lead to sanctions. The MoU laid the basis for France’s *High authority for the diffusion of works and protection of rights on the Internet* (HADOPI) law and had a significant impact on the initial EU Telecoms Reform proposals discussed in the next section.

At this stage, DPI was considered an element of the proposed graduated response regime. As part of the MoU, all major French ISPs agreed to experiment with technologies to filter illegal file sharing, and to deploy them if they were satisfied that the implementation was technically and economically feasible (Guez 2010). The rights holders then funded two tests on P2P filtering by the German laboratory EANTC. The first experiment only tested whether DPI appliances could detect P2P protocols. It found that the two best products detected 90% of P2P traffic with no significant impact on network performance (Rossenhövel 2008). But vendors of DPI appliances that claimed to be able to recognize and filter copyrighted content, including Audible Magic, declined to participate in EANTC’s tests. Their products, the testers surmised, did not work in large-scale environments (Ibid). The only evidence we have of the second test is a short slide presentation by a representative of the copyright interests (Guez 2010). It claims that a Vedicis product could recognize and block 99.98% of copyrighted content, allegedly with no impact on network performance or on ‘legal’ content. Vedicis had been working behind the scenes with MPA, IFPI and the French government for several years to inherit the business should such filtering become a legal requirement in France (Vedicis 2011).

Yet even France turned away from a DPI solution. The law that was eventually passed relied on outside-the-network (over the top) detection methods rather than DPI. Resistance from ISPs prompted even Vedicis give up on DPI as the technical vehicle for copyright surveillance.

The copyright owners don’t want to buy it, they want ISPs to buy it; the ISPs don’t want to buy it because it doesn’t do them any good. The business case was not there. We changed our business model to propose real value to [network] operators (Vedicis 2011).

Due to strong civil society resistance on privacy and due process grounds, the law created a new government agency known as the *High authority for the diffusion of works and protection of rights on the Internet* (HADOPI) to act as the intermediary between copyright holders, ISPs and users.

Great Britain also produced a ‘voluntary’ MoU among rights holders, ISPs and government agencies to address unlawful file sharing (BERR 2008). The July 24, 2008 agreement proposed a self-regulatory regime to be implemented in 2-3 years. It set out three goals: user notification when accounts are used for unlawful file sharing; a three month trial of notifying 1,000 illegal file sharers per week; and identification of mechanisms to deal with repeat infringers “including technical measures such as traffic management or filtering, and marking of content” (BPI 2008). Initially the agreement entailed warnings with no sanctions, but the British government stated its intention to legislate if the two industries could not agree on more permanent, follow-up measures. Driven by the British effort to take action against online copyright infringement, the British ISP Virgin Media announced in November 2009 that it would conduct an undisclosed trial of a DPI product named CView to monitor the level of copyright infringement of shared music on about 40 percent of their subscribers.¹ The trial was suspended less than a year later due to

¹ Williams, C.: “Virgin Media to trial filesharing monitoring system,” *The Register*, 26 November 2009, http://www.theregister.co.uk/2009/11/26/virgin_media_detica/

Virgin's concerns about adverse customer reaction.² Behind this planned use of DPI stood a deal with Universal Music to offer an unlimited music download service, making it a negotiated adoption of DPI between an ISP and a copyright holder. Complaints about the CView trial brought forward by Privacy International let the European Commission confirm its commitment to protect privacy and security of electronic communication. In January 2010, the EC announced it would closely monitor this case and consequently, Virgin Media halted its plans for a CView trial in late September 2010.

The French and UK negotiations overlapped with, and both influenced and were affected by, the EU Telecoms Package (see next section). In both countries, negotiated agreements built the foundation for hierarchical decisionmaking. Graduated response was enacted into law in France in October 2009 (HADOPI law) and in the UK in April 2010 (Digital Economy Act). In both cases, the ISPs were reluctant or opposed to the arrangement, and civil society groups mobilized strong opposition. The HADOPI law, originally passed in May 2009 had to be modified to survive a constitutional challenge: the court ruled that only a judge can deprive citizens of Internet access.

The EU Telecoms Reform

At the next level, copyright lobbyists attempted to make graduated response compulsory on a Europe-wide basis. On November 13, 2007, Commissioner Viviane Reding introduced to the European Parliament the first draft of the EU Telecoms Package. The package was a comprehensive policy reform that amended several existing directives in order to unify the EU Member States' telecommunications market. The rights holders seized upon the reform as a way to get uniform contractual provisions authorizing ISPs to disconnect subscribers for copyright infringement; this could not be done through modifying copyright law (Horten 2011: 110-7)

But this proposal was opposed by the representatives of ISPs, activists for civil rights such as La Quadrature du Net and the European Digital Rights Initiative (EDRI), and representatives of consumer protection organizations. A successful campaign to influence members of the European Parliament mounted by La Quadrature du Net took the graduated response advocates by surprise and raised numerous obstacles to its passage (Horten 2011: 96-7). The Bureau Européen des Unions de Consommateurs (BEUC), the European consumers' organization, repeatedly raised its voice against the deployment of technical measures and opposed the weakening of ISP immunity regulations. BEUC explicitly mentioned DPI as a threat to the security of personal data and privacy rights. Political debate focused not only on the cost and feasibility of making ISPs perform these functions, but on whether its reliance on automated judgments and technical systems undermined fundamental human rights to Internet access and judicial process.

The European Parliament finally approved the Telecom Package in its third reading November 9, 2009—without the graduated response mandate sought by the copyright lobby. Instead, a new “Internet Freedom” provision was added to the legislation, stating that any measures Member States take regarding end-users' access to Internet services “shall respect the fundamental rights and freedoms of natural persons.” According to Commissioner Reding, “three-strikes laws, which could cut off Internet access without a prior fair and impartial procedure or without effective and timely judicial review, will certainly not become part of European law” (European Commission 2009a). While the Internet Freedom provision may not prevent private agreements among ISPs and rights holders, from the copyright holders' perspective the outcome was definitely a failure: no hierarchical direction obligates ISPs to police their network to prevent copyright infringements.

² Mark, J. “Virgin Media UK Halt Broadband ISP Trial of CView DPI to Track Illegal File Sharing.” *ISP Review*, 1 October, 2010 (7:30 AM) <http://www.ispreview.co.uk/story/2010/10/01/virgin-media-uk-halt-broadband-isp-trial-of-cview-dpi-to-track-illegal-file-sharing.html>

Stakeholders' Dialogue on Illegal Up and Downloading

A Stakeholders' Dialogue on Illegal Up and Downloading continued the political interactions around DPI and copyright. Organized in the waning weeks of the Telecom Package debate, it represented a renewed attempt to negotiate a private agreement among ISPs and rights holders on an EU-wide basis.

An informal body without binding power, the Stakeholders' Dialogue was convened by the European Observatory on Counterfeiting and Piracy, a recently-formed body intended to make the IPR Enforcement Directive (2004/48/EC) ("IPRED") more effective by fostering cooperation between authorities. The European Commission described the Stakeholders' Dialogue as "a new and innovative working method used [...] to bring together a representative group of stakeholders to discuss concrete problems in the field of Intellectual Property Rights enforcement and explore possible ways of voluntary cooperation in compliance with the existing legal framework".³ The closed, non-public nature of the consultation, however, was questioned by civil society groups and some parliamentarians.

Its meetings began in September 2009 and ended in July 2010. They covered educational measures and awareness raising, legal downloading services on offer, information sharing, the current legal framework, sanctions and other legal actions, technical measures, and economic implications. The participants fell into two main categories: copyright holders and telecom/broadband Internet providers. The BEUC was invited to participate several times but declined, as it did not consider private negotiations over the use of technical measures to be a legitimate policymaking method (European Commission 2010c).

The information presented here is based on leaked minutes from the seventh meeting on June 2, 2010. (European Commission 2010b, European Commission 2010c). They offer only a limited view of its work, but as the leaked minutes are concerned specifically with the deployment of DPI they serve our purpose well. At this meeting, the European Telecommunications Network Operators' Association (ETNO) and European Internet Services Providers Associations (EuroISPA) recognized the relevance of copyright protection and the need to counter illegal activities (Hutty 2010). But technical measures were rejected as ineffective, detrimental to the operation of networks, and harmful to innovation. The level of proficiency needed to circumvent such technical measures, they contended, was low while their implementation costs would be high. ISPs, they claimed, cannot be expected to actively protect third party's digital content. HADOPI-style disconnection was seen as disproportionate and contrary to the EU's Digital Agenda. The solution to copyright infringement was seen in new business models that offered affordable access and more attractive digital content legally (European Commission 2010b).

On the other side were representatives of the copyright holders and vendors of technical measures (IFPI, MPA, Société Civile des Producteurs Phonographiques and DPI vendor Vedicis). They argued that technical measures are not only feasible and effective when deployed in close cooperation with ISPs, but are already in place for traffic management and network security in many ISPs. In an appeal to ISP self-interest, rights holders argued that they should use these technologies to prevent malicious software in P2P file sharing and to enable network operators' entry into a content distribution-oriented business model. It was also claimed that a graduated response system with an effective threat of a sanction would be a significant deterrent. Several presentations emphasizing France and its HADOPI law claimed that they illustrated the successful application of technical measures to combat online copyright infringement (European Commission 2010b).

In July 2010 the Stakeholder's Dialogue group formally decided to continue the meetings, with the goals of a public synthesis report and a possible draft MoU. Interviews with ISPs, however, indicate that they were fed up with the copyright holders' demands and were considering withdrawing from any further

³ European Parliament, Parliamentary questions. Answer given by Mr. Barnier on behalf of the Commission, 4 May 2010, <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-1910&language=EN>

dialogue. An ISP we interviewed felt that “Rights holders have not learned anything from the last year; the concrete proposals on the table do not reflect progress.” The source saw graduated response as creating “a lot of paperwork for ISPs” and feared that additional work would be created by appeals and customers with legitimate excuses. The number of complaints per day coming out of the French case, they believed, suggested that there would be thousands of procedures per day.⁴

In March 2011 a brief synthesis report was published that summarized the outcome of the seven meetings. Though formulated in positive language, it concluded “at this stage, it is not clear whether this can result in industry- and EU-wide voluntary cooperation in a limited number of areas.” The Stakeholders’ Dialogue thus failed to produce a negotiated solution.

Public Consultations on the E-Commerce Directive and the IPR Enforcement Directive

It is not surprising that the fierce ongoing debates about the use of ISPs for policing copyright would lead to discussion of the E-Commerce Directive. As noted in the introduction, that Directive includes a safe harbor principle for ISPs which limits their liability and obligations to monitor. These immunities are strong incentives for ISPs not to deploy DPI for copyright policing; DPI could create “actual knowledge” of infringements and thus sacrifice their immunity (Harrelson 2010). On the other hand, as early as 2008 rights holders openly stated in EC consultations that the Directive was an “impediment to cooperation” between ISPs and rights holders, and openly called for the reversal of its ‘mere conduit’ principle (Horten 2011: 101). In August 2010, the EC opened a public consultation on the Directive. The questionnaire deals with interpretation problems of the liability regime and the monitoring and filtering obligations of ISPs. The consultation closed on November 5, 2010; although the Commission has not yet published any reports, inside sources indicate that it is unlikely the Directive will be significantly changed.

Yet still European policymakers issued ambiguous signals. On December 22, 2010, a different section published a report on the effectiveness of its 2004 IPR Enforcement Directive (2004/48/EC) (European Commission 2010e). The report claimed that existing laws were not strong enough to combat online IP infringement effectively and that powers to compel ISPs and other intermediaries to take more proactive steps to police copyright should be “examined.” A “blueprint” published four months later (May 2011) proposed that the tasks of the European Observatory on Counterfeiting and Piracy be extended to involve “research on innovative enforcement and detection systems that on the one hand allow licit offers to be as innovative and attractive as possible and on the other allow for more effective enforcement against counterfeiting and piracy.” It also put forward the idea that online infringement should be tackled “at their source and to that end, foster cooperation of Internet intermediaries [...].”

Resolution of Scarlet vs. SABAM

In a long-awaited opinion issued November 2011, the European Court of Justice (ECJ) ruled that the injunction requiring DPI use by ISP Scarlet, discussed earlier, would violate fundamental rights (ECJ 2011). The Court held that installing DPI to prevent copyright infringements for all electronic communications among all its customers as a preventive measure and for an unlimited time was illegal. The court addressed the users’ right to the protection of personal data, their freedom of expression and information, and the ISPs’ freedom to conduct business. Those rights are all protected under the Charter on Fundamental Rights and the European Convention on Human Rights by Articles 8, 11, and 16 respectively. The ECJ decision constituted the death sentence for the extreme, inside-the-network approach to network surveillance for copyright enforcement.

To summarize, in Europe the capabilities of DPI put it in the center of a maelstrom of policy debate and political mobilization around online copyright enforcement. But in general, efforts to make full, untrammled use of network surveillance capabilities for copyright policing and enforcement were

⁴ Interview with European ISP, 10 November, 2010.

defeated or severely checked. Even when graduated response initiatives were successful, the resistance to DPI from ISPs and Internet rights advocates and concerns about its impact on fundamental rights led to the selection of the hybrid, OTT model. Though the E-Commerce Directive (2000/31/EC) immunities were directly challenged, they were not overturned.

DPI and Copyright Policing in the United States

In the US, rights holders have generated the same push for greater ISP responsibility over the same time period, for the same reasons. But a stronger and more settled legal regime was in place. The Digital Millennium Copyright Act (DMCA) and Section 230 of the Communications Decency Act (CDA) are the two main features of the relevant institutional framework in the US. Section 230 says 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.” The DMCA was signed into law 1998; the CDA in 1996. Both became settled law a decade before Europe’s current turmoil over telecommunications and copyright.

The combination of Section 230 and the DMCA safe harbor gave copyright interests in the US no basis for lawsuits that would impose technical measures on the major commercial ISPs. Further, a major ISP had already successfully resisted, through litigation, attempts by rights holders to require it to map IP addresses to customer accounts without a judicial warrant to facilitate prosecution of P2P file sharers.⁵ Just as in Europe, Internet access and service providers strongly opposed efforts to use law to impose surveillance responsibilities on them. Thus, copyright interests have been forced to pursue more indirect, negotiated solutions in the US

Copyright Infringement at Higher Education Institutions

US rights holders focused their attention on the higher education sector, where campus networks were perceived as a hotbed of P2P file sharing. In December of 2002, the copyright interests prompted the formation of a Joint Committee of the Higher Education and Entertainment Communities (JCHEEC) to address the problem of unauthorized file-sharing on campuses. The committee was made up of leaders from colleges and universities, entertainment industry representatives (including the Motion Picture Association of America and the Recording Industry Association of America), and members of education advocacy groups such as the American Council on Education (ACE) and Educause.

The JCHEEC’s activities took place in two phases. The first phase, running from the end of 2002 to the spring of 2004, was dominated by information gathering and some preliminary reports. It began by issuing two public requests for information (RFIs). The first RFI in April 2003 was intended to collect information on how technologies are currently being used to address the management of P2P applications in the academic environment (JCHEEC 2003). The second RFI in June 2003 solicited information on ways to make available legitimate online movie and music services to reduce the demand for illegal file sharing. The group also asked a law firm to produce a “Background Discussion” on copyright law and the potential liability of students engaged in file sharing (Remington 2003). That report discussed the importance of campus education policies around legal rights and responsibilities, and introduced the idea that higher educational institutions could possibly be subject to contributory and/or vicarious liability as a result of the illegal file-sharing activity committed by students on university networks.

The first phase concluded with the issuance of a report detailing university “best practices” in addressing P2P file sharing. Drawing upon the results of the first RFI and the ideas introduced in the Background Discussion white paper, the report, *University Policies and Practices Addressing Improper Peer-to-Peer*

⁵ Recording Industry Association of America, Inc., v. Verizon Internet Services, Inc., 19 December 2003, <http://www.Internetlibrary.com/pdf/RIAA-Verizon-DC-Cir.pdf>

File Sharing (JCHEEC 2004), described the technologies that could be used to manage P2P activity by campus administrators at that time. Some universities already had technological solutions in place which limited P2P activity, mostly in the form of firewalls which were installed for traffic shaping and bandwidth management. The monitoring of P2P activity was considered a secondary use for these technical resources. Both papers were distributed to the executives of colleges and universities throughout the US via ACE, an organization of the presidents and chancellors of US accredited, degree-granting higher education institutions.

One can infer from subsequent activities that the copyright interests were not satisfied with these efforts. File sharing did not seem to be diminishing. In August 2005, the JCHEEC sent out another letter via ACE which strongly recommended that universities implement anti-piracy hardware or software to prevent further copyright infringement.⁶ The letter was strategically co-signed by Cary Sherman, the president of the RIAA and a member of the JCHEEC.

During 2006 and 2007, as widespread file-sharing failed to abate, relations between higher education and the copyright interests deteriorated. The copyright holders unleashed a litigation campaign against file sharing and got sympathetic legislators to publicly attack universities for their alleged abetting of copyright infringement. This pressure led to the second phase of JCHEEC activities. This time, technological capabilities took center stage. On October 2006, JCHEEC held another Washington workshop on filtering technologies, with presentations and submissions by DPI vendors. The discussions among vendors and higher education network operators and ICT administrators led the latter to conclude that “each product addresses different elements of the problem, but no product addresses all of them.” The University interests emphasized the unique aspects of the academic environment and the diversity of institutional policies and requirements.

On February 28, 2007, the RIAA announced a campaign in which it would send pre-litigation settlement letters to universities (as well as commercial ISPs) informing them that they were about to sue individual students (customers) on their networks. The letters were part of an RIAA strategy that gave students accused of piracy a chance to settle outside of court with discounted payments.⁷ The reaction to the letters by higher education institutions was varied, but in most cases, colleges refused to pass the letters along to students, claiming that it was difficult to accurately link IP addresses to specific students. As part of the RIAA’s larger strategy, it also launched p2plawsuits.com, a site where individuals whose names were submitted to the RIAA from their university or ISP for copyright infringement could settle the issue out of court by paying their settlement to the RIAA online.⁸ The creation of this portal was premature, as the RIAA assumed that service providers (colleges and universities included) would provide them with the personal information of their users going forward, when this did not happen.⁹

Prodded by the copyright industry members of the Joint Committee, another workshop was organized for April 2007. Its goal was to define a systematic set of requirements for technological control of illegal file sharing on college and university networks. This two-day workshop was attended by university network managers, members of the entertainment industry and DPI technology vendors. Universities balked at the

⁶ JCHEEC letter to presidents from Penn State University president Graham Spanier and RIAA president Cary Sherman regarding illegal file sharing, 16 August 2005, http://www.acenet.edu/AM/Template.cfm?Section=Government_Relations_and_Public_Policy&template=/CM/ContentDisplay.cfm&ContentID=11754

⁷ Nick Semenkovich, “RIAA sends thirty pre-litigation letters over alleged music piracy,” *The Tech*, 12 October 2007, <http://tech.mit.edu/V127/N45/riaa.html>

⁸ Eliot Von Buskirk, “RIAA launches P2PLawsuits.com,” *Wired*, 27 February 2007, http://www.wired.com/listening_post/2007/02/riaa_launches_p/

⁹ Nate Anderson, “Another school says “no” to RIAA pre-litigation letters,” *Ars Technica*, 9 March 2011, http://arstechnica.com/tech-policy/news/2008/01/another-school-says-no-to-riaa-prelitigation-letters_ars

cost of comprehensive interception measures and questioned any implementations that would put them in the role of copyright police. While a few universities had deployed Audible Magic and others blocked BitTorrent (mostly for bandwidth management reasons), the university representatives were simply unable to agree on a common technological approach to combating digital piracy.

Unsatisfied, the copyright holders increased the pressure even further. They seized upon the reauthorization of the Higher Education Act as an opportunity to use the power of the purse to coerce colleges and universities into enacting their agenda. US Representative Rick Keller (R) introduced the “Curb Illegal Downloading on College Campuses Act.” This bill was submitted after extensive lobbying by the RIAA and MPAA and what some in the higher education community considered to be an unfair campaign targeting universities (Green 2007). The Keller bill proposed to take money from the Fund for the Improvement of Postsecondary Education Program that would otherwise be used for bandwidth management by universities, and reallocate it to the development of “innovative on-campus, anti-piracy pilot programs designed to reduce digital piracy.”¹⁰ Keller’s bill was referred to a subcommittee where it served as a foundation for the copyright protection provisions of a new Higher Education Opportunity Act (HEOA).

The provisions of the HEOA that addressed illegal file-sharing on college campuses were met with strong opposition from educators and related interest groups. In November of 2007, the higher education members of the JCHEEC submitted a letter opposing the requirement that higher education institutions develop and implement anti-piracy plans involving the use of technological measures.

Despite the general opposition of universities to mandatory use of technical measures, they organized yet another workshop to explore the current technologies available. Common Solutions Group (CSG), consisting of CIOs and technologists from 28 major research universities and other technology experts, met with vendors of detection and suppression technologies including Audible Magic, Red Lambda and SafeMedia. Their products and suggestions for implementation were presented at Virginia Tech on January 9, 2008. The consensus of attendees was that “current products cannot stop all (or even most) unauthorized sharing of copyrighted material without interfering with the efficiency of the networks essential to research and teaching in higher education” (CSG 2008). In March 2008, ACE, Educause and other higher education institutions submitted a letter voicing similar concerns (Cesarini and Cesarini 2008).

Despite these efforts the final version of the HEOA passed July 31, 2008 and was signed into law August 14 of that year. The law required a college or university to develop a plan to combat digital copyright infringement, including the use of one or more “technology-based deterrents.” The regulations define four types of technical deterrents: 1) bandwidth shaping, 2) traffic monitoring 3) accepting and responding to DMCA notices and 4) commercial products designed to detect and block illegal file sharing.¹¹ Schools that fail to comply with these provisions risk incurring steep fines and losing federal funding for students (Wada 2008).

The result of this mandate has been a growing adoption of technological solutions by higher education institutions to monitor P2P file-sharing activity on campuses, including in dorm areas. A niche market of DPI-based solutions has developed, with vendors designing and marketing packages specifically for colleges and universities. In October 2010, for example, Procera released PacketLogic Smart Campus, a solution with DPI capabilities that the company bills as a turnkey network and traffic management

¹⁰ Brooks Boliek, “Politician eyes taxpayer money for piracy war,” *Reuters*, 29 March 2007, <http://www.reuters.com/article/2007/03/29/industry-piracy-dc-idUSN2934796120070329>

¹¹ Federal Register Part II: Dept. of Education 34 CFR Parts 600, 668, 675, et al. General and Non-Loan Programmatic Issues; Proposed Rule, 21 August 2009, <http://edocket.access.gpo.gov/2009/pdf/E9-18550.pdf>

solution specifically for higher education institutions. Audible Magic CopySense is another DPI-based solution which has become fairly popular with colleges and universities. The vendor positions CopySense as aiding HEOA compliance, and boasts of a built-in graduated response system.

The requirements of the law, however, provide universities with a great deal of leeway to choose their implementation. The general sentiment of higher education administration is that while some kind of “technology-based deterrent” is required, universities are given a significant amount of autonomy with regards to the design of their plans and it is up to each school to review its plan on a regular basis for effectiveness (Educause 2011). Like commercial ISPs, higher education institutions are not eager to incur infrastructure or administrative costs to serve the needs of rights holders. Legal experts retained by Educause for a Webinar advised Universities that they are not required to forward DMCA notices with pre-litigation settlement letters to their students (Educause 2011). University experts are warning universities to be careful not to implement content filtering tools too broadly, as this could cause them to lose their safe harbor protections under the DMCA (Storch and Wachs 2011). As one legal expert noted, “Active monitoring is not only not required by the HEOA, but it may make you lose your safe harbor – be very, very careful before you implement one of those systems” (Educause 2011).

One example of an implementation comes from Syracuse University in central New York State. The costs of responding to DMCA notices and the legal risks to students and the university led its Information Technology and Services department to purchase a pair of Palo Alto PA-4060 firewalls, which are used to block all P2P protocols within campus borders. The firewalls do not detect copyrighted files per se. By pre-emptively and indiscriminately blocking P2P applications, the firewalls have dramatically reduced the number of DMCA notices received by the University. Responding to a DMCA notice can be arduous. When a notice is received at Syracuse University, the Director of Information Security must look through the school’s web logs to find the student ID matching the IP address and time stamp of the notification. Once this information is found, the University policy follows a graduated response approach with three steps. Like most colleges and universities, Syracuse claims that it goes to great lengths to ensure that the personal details of the alleged infringers are never disclosed to copyright holders directly. In this respect, there is only a one-way dialogue between copyright holders and higher education institutions.

The cost savings created by these technological measures became apparent after a hardware failure of one of the two firewalls in October 2010, when the Director of Information Security suddenly received between 30-40 DMCA notices in one week (Croad 2011). When the firewalls are fully functioning, the number of DMCA notices per week is basically zero. The Syracuse University IT department is now considering using the firewalls for other purposes. They may replace access control lists (ACLs), a way of blocking common security threats that involve costly and mistake-prone command line input, with the Palo Alto firewalls. The firewalls might also be configured to start investigating web traffic for malware.

Negotiations between ISPs and Rights Holders

On July 8, 2011 a group of US film producers, record labels and ISPs announced a voluntary agreement to implement a six-step graduated response framework called the Copyright Alert System. The parties include the main US rights holders organizations and the five largest US ISPs: AT&T, Verizon, Comcast, Time Warner Cable and Cablevision.

Each time rights holders notify an ISP that one of their users has engaged in illegal downloading, he/she will receive an electronic warning from the ISP. After approximately 6 of these educational warnings, additional mitigation measures may be taken at the discretion of the ISP. These measures include redirection to a landing page until the subscriber contacts the ISP or reviews information about copyright, or a reduction in the speed of the user’s Internet connection. The MoU relies on OTT methods for surveillance rather than on DPI. Section 4 states that “Each Participating ISP will develop and maintain methodologies... to match Internet Protocol (IP) addresses identified by the Content Owner

Representatives to the Participating ISP Subscribers' accounts, to keep a record of repeat alleged infringers..." (CCI 2011).

The agreement ends the previous contentious relationship between rights holders and ISPs, for the time being. It was acceptable to the ISPs because it was completely voluntary on their part, and termination of service is not part of the response measures. The authors do not have detailed information about the timeline or evolution of these negotiations. It is believed that New York Attorney General Andrew Cuomo played a role in fostering them some time in 2008. Later, as Governor of New York, he is thought to have worked closely with the Obama administration to help foster discussions between the stakeholders. Pressure from the President was reported to have led to the finalization of the agreement. These discussions could be likened to the EU Stakeholders' Dialogue, with the obvious difference being that a framework was actually agreed and implemented.

Analysis and Conclusions

The emergence of a technological capability for automated copyright enforcement on networks has provoked intense, prolonged political interactions around changes in Internet law and public policy. Specifically, it has led to a major reassessment of Internet service providers' responsibilities, destabilizing an earlier policy equilibrium built around an immunity principle. In this respect, the technology had agency. But while rights holders openly challenged the principle of intermediary immunity other influential actors strongly reaffirmed it, creating a fork in the road. With DPI on the table, the principle had to be reaffirmed, discarded, or revised. In the end, neither the US nor Europe discarded the principle completely. Neither applied DPI to copyright policing in a way that realized its radical, disruptive potential.

A radical implementation would make the Internet access network itself responsible for surveillance, detection, notification and enforcement. The key factor preventing such an integrated response was the disjunction between the interests of network operators and the interests of rights holders. As predicted, network operators resisted shouldering the costs and burdens of a technology designed to benefit a third party (copyright holders) – even when they were willing to adopt other DPI applications that met their own operational needs. The rights holders agenda was also blunted by features of the technology itself, as engineering studies brought to light the scalability limitations of DPI for copyright enforcement. While ISPs may have varied in the intensity with which they opposed DPI for copyright and in their willingness to bargain with rights holders, there is no evidence that any of them actively embraced or advocated it. ISPs in the cable TV industry were no exception, even though some have economic interests in copyrighted content.

If the ISPs had any tendency to waver in their opposition, the presence of committed public interest groups in the US and Europe countered it. Advocacy groups viewed policing the network via DPI as an assault on Internet users' rights, and mobilized accordingly. European digital rights and consumer groups successfully politicized the issue and waged campaigns against graduated response, invoking privacy and the rights to Internet access, free expression and due process.

While the principle of ISP immunity did not break, it did bend. The key compromise underlying the new equilibrium was the use of *over-the-top (OTT)* forms of surveillance. OTT limited the role of the ISP to mapping IP addresses to user accounts, and avoided new infrastructure investments. In France, where graduated response went the furthest, an elaborate system of legal and procedural safeguards surrounds the mapping and disconnection process. ISPs are actually paid for every IP address they map, and a judge must order them to disconnect a subscriber. Structurally, these arrangements are not that distant from the *status quo ante*.

As actor-centered institutionalism predicted, distinct institutional frameworks affected the modes of interaction available to the parties in the US and Europe. A more far-reaching debate took place in Europe, where the possibility of legislation making DPI part of a Europe-wide mandatory graduated response system was, for a time, a live option. The stronger, more settled US laws immunizing ISPs seem to have kept the American debate confined to private negotiations. Private ordering within the constraints set by the DMCA law is evident in the response of the US universities, and in the Copyright Alert System agreed by commercial ISPs.

Private stakeholder negotiations played a role in both the US and Europe. In most cases they failed. When implementation of a new technology involves a zero sum game over the distribution of costs and benefits, negotiations are unlikely to succeed in the absence of hierarchical direction. Only the US Copyright Alert System could be considered a successful negotiation, and it is a very soft agreement that gives ISPs near-total discretion. Although the UK and France generated MoUs between ISPs and rights holders, the agreements were mediated and directed by governments, and the end result was hard legislation anyway (the HADOPI law and Digital Economy Act). Europe's Stakeholder Dialogue Group produced no results whatsoever, and the American JCHEEC, while thoroughly educating the parties about technical options and each other's needs, did not prevent later recriminations and a resort to legislation by the copyright interests. Legislation that threatened educational institution's federal funding helped to create an incentive structure that nudged many universities into graduated response policies, educational programs and, occasionally, DPI-based technical measures. While many resisted having DPI for copyright imposed on them, many universities nevertheless choose to block file-sharing protocols to conserve bandwidth, or to minimize the transaction costs associated with responding to notice and takedown requirements.

Despite the political resistance and the limitations placed on its use, DPI use is spreading. But so far it is deployed more as a tool of network operators' policy than as a direct tool of public policy. As such, deployments of DPI reflect the concerns, interests and constraints of individual network operators. In the copyright arena, law and public policy set the parameters of ISP responsibilities, such as notice and takedown requirements. But for the most part, network operators decide how DPI fits into those requirements, if at all. However, the more responsibility for regulation and control of Internet use that is placed upon ISPs, the stronger their incentives to adopt some kind of network surveillance technologies. Thus, a proposed law such as the US Stop Online Piracy Act (SOPA), which may require ISPs to block access to websites engaged in infringement, may require many of them to install DPI to implement the law's requirements. Furthermore, once it is installed, DPI can absorb and integrate some additional functions beyond the ones that led to its initial installation.

Acknowledgement

Research supported by Science, Technology and Society program of the Social, Economic and Behavioral Science Directorate of the US National Science Foundation (NSF).

References

- Bach, D. 2004. 'The Double Punch of Law and Technology: Fighting Music Piracy or Remaking Copyright in a Digital Age?' *Business and Politics* 6(2).
- Bendrath, Ralf and Milton L. Mueller. 2011. 'The End of the Net as we Know it? Deep Packet Inspection and Internet Governance.' *New Media and Society* 13(7): 1142-1160.
- BERR. 2008. Consultation on Legislative Options to Address Illicit P2P File-Sharing. London, UK, Department for Business, Enterprise and Regulatory Reform. <http://www.berr.gov.uk/files/file47139.pdf>.
- BPI. 2008. MOU between ISPs and rights holders <http://www.bpi.co.uk/our-work/protecting-uk-music/article/joint-memorandum-of-understanding-on-an-approach-to-reduce-unlawful-file-sharing.aspx>. London British Recorded Music Industry.
- Bridy, Annemarie. 2010. "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement." *Oregon Law Review* 89: 89-132.
- Cannes Declaration. 2005. Declaration of the European Ministers for Audiovisual Affairs and the Member of the Commission in charge of Information Society and Media. Europe Day at the Cannes Film Festival (May 17). http://ec.europa.eu/avpolicy/docs/other_actions/cannes_decl_2005_en.pdf.

- Casey, Timothy D. 2000. *ISP Liability Survival Guide: Strategies for Managing Copyright, Spam, Cache, and Privacy Regulations*. New York, Wiley.
- Cesarini, Lisa M. and Paul Cesarini. 2008. 'From Jefferson to Metallica to your campus: Copyright issues in student peer-to-peer file sharing.' *Journal of Technology Studies* 34(1).
- Croad, Chris. 2011. Interview with Chris Croad, Director of Information Security, Syracuse University, 23 February 2011.
- CSG. 2008. Infringement-Suppression Technologies: Summary Observations from a Common Solutions Group Workshop January 9, 2008 Common Solutions Group. <http://www.stonesoup.org/docs/copyright-technology.pdf>.
- De Beer, Jeremy F. and Christopher D. Clemmer. 2009. 'Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?' *Jurimetrics* 49(Journal Article): 375-409.
- Disco, Cornelius. 2005. 'Back to the drawing board: Inventing a sociology of technology.' *Inside the Politics of Technology: Agency and Normativity in the Co-Production of Technology and Society*. H. Harbers. Amsterdam, Amsterdam University Press: 29-60.
- Educause. 2011. Alphabet Soup: A P2P, DMCA, & DMCA, & HEOA FAQ. 2011 Webinar (101 minutes), <http://www.educause.edu/ResourcesAlphabetSoupAP2PDMCAandHEOAFAQ/228726>.
- European Court of Justice. 2011. Judgment of the Court (Third Chamber), Scarlet Extended SA v. SABAM *Case C-70/10*. Brussels, Court of Justice of the European Union
- European Commission. 2000. Directive on Electronic Commerce 2000/31/EC. Official Journal L 178 , 17/07/2000 P. 0001 – 0016. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>.
- European Commission. 2004. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. Official Journal of the European Union L 157 of 30 April 2004. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:EN:PDF>.
- European Commission. 2009a. Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open Internet, a single European telecoms market and high-speed Internet connections for all citizens, MEMO/09/491, Brussels, 5 November 2009. <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491>.
- European Commission. 2009b. Study on Online Copyright Enforcement and Data Protection in Selected Member States, November 2009. Brussels, 2009. http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf.
- European Commission. 2010a. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A Digital Agenda for Europe, COM(2010) 245 final/2, Brussels, 26 August 2010.
- European Commission. 2010b. Stakeholders' dialogue on illegal up- and downloading, draft summary of meeting minutes (2 June 2010), Brussels, 2010.
- European Commission. 2010c. Stakeholders' dialogue on illegal up- and downloading, draft summary of meeting minutes (1 July 2010), Brussels, 2010.
- European Commission. 2010d. Study on Online Copyright Enforcement and Data Protection in Selected Member States, April 2010. Brussels, 2010. http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf.
- European Commission. 2010e. Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights. COM(2010) 779 final. Brussels, 22.12.2010. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:PDF>.
- European Commission. 2011. Intellectual Property Strategy – Frequently Asked Questions (MEMO/11/332). <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/332>
- Gillespie, Tarleton. 2007. *Wired Shut: Copyright and the Shape of Digital Culture*. Cambridge, Mass, MIT Press.
- Green, K. (2007). 'Swiftboating Higher Education on P2P.' *Inside Higher Ed*. Washington, DC.
- Guez, M. (2010). 'Technical measures in the context of the Hadopi Law (France).' Presentation before the Stakeholders' dialogue on illegal up- and downloading. <http://fr.readwriteweb.com/wp-content/uploads/2010/09/Slides-SCPP.pdf>. Brussels Société civile des producteurs phonographiques (SCPP).
- Harbers, Hans, ed. 2005. *Inside the Politics of Technology: Agency and Normativity in the Co-Production of Technology and Society*. Amsterdam, Amsterdam University Press.
- Harrelson, W. C. 2010. 'Filtering the Internet to Prevent Copyright Infringement: ISP Safe Harbors and Secondary Liability in the US and France.' *New Matter* 35(1).
- Horten, Monica M. 2011. *The Copyright Enforcement Enigma: Internet politics and the 'telecoms package.'*. London, Palgrave-MacMillan.
- Hutty, Malcolm. 2010. 'Analysis of technical measures to suppress online copyright infringement.' *Presentation at the Stakeholders' Dialogue on Illegal up and Downloading*. Brussels, 2 June 2010.
- JCHEEC (2003). Request for Information: Technology Opportunities for Addressing Issues Associated with Peer-to-Peer File Sharing on the University and College Campus, Joint Committee of the Higher Education and Entertainment Communities.
- Knill, Christoph and Dirk Lehmkuhl. 2002. 'Private Actors and the State: Internationalization and Changing Patterns of Governance.' *Governance* 15(1): 41-63.

- Law, John. 1992. 'Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity.' *Systems Practice* 5(4): 379-393.
- Lessig, Lawrence. 2005. *Free Culture: The nature and future of creativity*. New York, Penguin.
- Litman, Jessica. 2001. *Digital Copyright*. Amherst, NY, Prometheus.
- McIntyre, T. J. 2008. 'Filter or Else! Music Industry Sues Irish ISP.' *SCL Blog* 19, July 14, 2010.
- McIntyre, T. J. 2009. 'Three strikes for Ireland - Eircom, music industry settle filtering case.' *IT Law in Ireland (blog)* <http://www.tjmcintyre.com/2009/01/three-strikes-for-ireland-eircom-music.html> (January 29).
- Meyer, Trisha and Leo van Audenhove. 2010. 'Graduated response and the emergence of a European surveillance society.' *Info* 12: 69-79.
- Mueller, Milton L. 2010. *Networks and States: The global politics of Internet governance*. Cambridge, MA, MIT Press.
- Mueller, Milton L. 2011. 'DPI Technology from the Standpoint of Internet Governance Studies.' *The Network is Aware* http://dpi.ischool.syr.edu/Papers_files/WhatisDPI-2.pdf.
- Parsons, Christopher. 2008. 'Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials.' *The New Transparency Project Working Paper* http://www.sscqueens.org/sites/default/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf
- Remington, Michael. 2003. Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks, American Council on Education (ACE).
- Rosshövel, Carsten. 2008. 'Peer-to-Peer Filters: Ready for Internet Prime Time?' *Internet Evolution* http://www.Internetevolution.com/document.asp?doc_id=148803.
- Samuelson, Pamela. 1996. 'Intellectual property rights and the global information economy.' *Communications of the ACM* 39(1).
- Scharpf, Fritz W. 1997. *Games real actors play: Actor-centered institutionalism in policy research*. Boulder, Westview Press.
- Stallman, Richard. 2002. *Free software, free society : selected essays of Richard M. Stallman*. Boston, MA, Free Software Foundation.
- Storch, Joseph and Heidi Wachs. 2011. 'A legal matter: Peer to peer file sharing, the Digital Millennium Copyright Act, and the Higher Education Opportunity Act: How Congress and the entertainment industry missed an opportunity to stem copyright infringement.' *Albany Law Review* 74(1): 313-360.
- Vaidhyanathan, Siva. 2001. *Copyrights and Copywrongs: The rise of intellectual property and how it threatens creativity*. New York, New York University Press.
- Vedicis. 2011. Telephone interview with staff members, Vedicis, Inc. Paris, France, July 5, 2011.
- Wada, Kent. 2008. 'Illegal File Sharing 101.' *Educause Quarterly* 31(4).