

Journal of Contemporary European Research

Volume 9, Issue 1 (2013)

Mediating Surveillance: The Developing Landscape of European Online Copyright Enforcement

Jon Bright *European University Institute*

José R Agustina *Universitat Internacional de Catalunya*

Citation

Bright, J. and Agustina, J.R. (2013). 'Mediating Surveillance: The Developing Landscape of European Online Copyright Enforcement', *Journal of Contemporary European Research*. 9 (1), pp. 120-137.

First published at: www.jcer.net

Abstract

After a period of relative *laissez faire*, governments around the world are beginning to attempt to regulate online life, for a variety of reasons, through various mechanisms of surveillance and control. The drive to enforce the respect of copyright is at the forefront of these attempts, a highly controversial topic which pits proponents of the rights of the creative industry against advocates of freedom of speech. Apart from their inflammatory nature, one distinguishing characteristic of most of these schemes is that they are *mediated*: that is, they are conducted with the help of third parties, most often internet service providers. The mediation of surveillance is something as yet relatively underexplored by the field of surveillance studies, whose theoretical tools are by and large focussed on a two way relationship between watcher and watched. This article seeks to remedy this deficit, by examining the dynamics of mediation in the context of online copyright enforcement. We argue that, far from being a neutral process, the displacement of surveillance to third parties has a crucial impact on the way in which it is conducted. In particular, the expanding capacity of mediators becomes a reason for justifying surveillance in and of itself.

Keywords

Copyright; Information society; Internet

The study of surveillance, whilst taking in a huge variety of situations and practices, most frequently concerns some sort of relationship between watcher and watched. This conceptualisation of surveillance as a two actor relationship, while clearly of use in many situations, nevertheless has the potential to exclude other parties who play an important role in structuring social control. As Aaron Martin et al. argue:

‘Traditional ways of understanding surveillance, by focussing on the increasing capabilities of the surveyors and the expansion of surveillance to include previously exempt groups, reinforce the conception that surveillance is a party for two: an exclusive relationship between the surveyor and her subjects. Looking at the world this way not only ignores some of the actors who resist surveillance, but also excludes the assemblages that conduct the surveillance.’ (2009: 215)

The surveillance of online space is a case in point. Like the technology of the internet itself, regimes of control online work not through a two way relationship between watcher and watched, but by distributing functions to a heterogeneous network of actors. These actors, of which the internet service provider is the most obvious example, may have little interest in pursuing a particular surveillance function; yet legislation, court decisions, and regimes of liability can nevertheless compel them to do so. The mediation of surveillance online is more than simple delegation, from a superior to a subordinate: it is a type of *deputization*, a (perhaps unwilling) co-option of private actors into the aims of the surveillance system (Michaels 2010). This mediation is something which as yet remains under-theorized and underexplored in literature on surveillance studies.

This article explores the mediation of surveillance online, placing particular focus on the enforcement of online copyrights in Europe. It aims to make two major contributions to the literature. In the first section, it seeks to define theoretically the concept of mediation, relating it to a broader literature on the notion of the surveillant ‘assemblage’. The key characteristics of surveillance mediation are explored, and several expectations about mediation are advanced. Secondly, it provides a comparative overview of legislation relating to online copyright in four European countries (the UK,

France, Spain and Italy). This empirical material allows us to better flesh out how the concept of mediation works in practice.

MEDIATION SURVEILLANCE: THEORETICAL REFLECTIONS

David Lyon, perhaps the leading author in the field of surveillance studies, defines surveillance as 'focused, systematic and routine attention to personal details for the purposes of influence, management, protection or direction (2007: 14). This is, as Lyon intends, is a broad definition: a wide range of human activity in a diverse set of fields could therefore be said to constitute some kind of surveillance (Lyon 2007: 25-45). Much early work on surveillance studies focussed on large public institutions such as schools, prisons and the military created during the broader construction of the modern Nation State (see, *inter alia*, Dandeker 1990, Giddens 1987). This work emphasised the important role such institutions played in the construction of identity, a concept which was perhaps most fully expressed through Michel Foucault's reading of Jeremy Bentham's "panopticon" (1975), which described a centralized, all embracing institution which completely defines those within its gaze ("soul training" as Haggerty and Ericson call it – 2000: 615). Also, more importantly for our purposes, it presented surveillance as a generally two way relationship: between surveillant institution and surveilled subject.

More recent literature has started to broaden the focus of surveillance studies, to look not only at state based forms of social control but also private institutions and different forms of public-private partnerships. As the focus of the field has shifted, the usefulness of the panopticon (and other concepts based around it) started to come into question (see Haggerty and Ericson 2000, Haggerty 2006). Newer types of surveillance (such as customer tracking schemes or the cookies installed by many websites) seemed to have aims much more mundane than 'soul training', while the networked nature of contemporary surveillance appears at odds with the description of one overarching institution.

In response to this apparent need, drawing on the work of Gilles Deleuze and Félix Guattari (1980), Kevin Haggerty and Richard Ericson developed the concept of the "surveillant assemblage" to help better describe this new turn in surveillance studies (while David Lyon has also made some remarks in the area, see Lyon 2007: 111-115). Deleuze and Guattari's more general concept of "assemblage"¹ is inspired by their reflections on the "rhizome", a type of plant which connects a variety of apparently separate shoots through an underground root system. Haggerty and Ericson regard contemporary surveillance as rhizomatic because apparently separate systems can nevertheless be joined, and work together, even in the absence of a centralized driving logic. An assemblage is decentralized, constantly shifting, and animated only by a range of temporary "desires" (Haggerty and Ericson 2000: 609), which are loose imperatives to organise and control information rather than affect changes in personality.

The assemblage is important for surveillance studies because it permits a change of focus, away from watcher and watched towards connections between surveillance system: what causes them to develop, and how different types of connections might have different types of effects. It permits, in other words, the study of multi-actor surveillance networks, breaking out of the traditional two way paradigm. However, while the term assemblage is by now also 'a conceptual benchmark in the surveillance literature' (Hier 2003: 400), its potential as a concept has remained mostly underexplored: there has been little literature dedicated to fleshing out the mechanics through which assemblages work, nor what type of expectations the appearance of an assemblage should generate.

In this article, we explore one crucial aspect of the surveillant assemblage: the fact that some or all of the work of surveillance is distributed onto a variety of different actors, which we call “mediation”. We define the mediation of surveillance as occurring when some or all of the “activity” of surveillance defined by Lyon is conducted by agents outside of the direct control of the surveillance institution. For example, banks act as agents of surveillance when they check the transactions of their customers for financial fraud (Bergström et al. 2011). Airlines act as agents when they enforce the visa regulations of countries that they are flying to (Guiraudon 2003). And, in our area of focus, internet service providers act as agents when they are called upon to both carry out surveillance and sometimes even control the activities of their customers. This mediation is crucial to the assemblage as a whole (without it, no systems would “assemble”).

We advance three major hypotheses about the mediation of surveillance. Firstly, we expect it to occur in situations where institutions conducting surveillance have incomplete power or information. While they might have the ability to successfully deputise other social actors into their surveillance system, they are unable (for financial, technical, legal or other reasons) to carry out the surveillance themselves. Mediation, in this reading, is a sub-optimal solution for a surveillance system, even if it might be financially or practically more viable. For example, Michaels notes how in the US, in the climate following 9/11, delivery companies were encourage to report suspicious behaviour in any of the premises they visited (Michaels 2010). The security services were interested in these companies because they had a kind of access to individual homes and dwellings which it would be impossible for the police to duplicate without a warrant. This contradicts somewhat the description of the assemblage which Haggerty and Ericson advance: for them, assemblages are indicative of the increasing power and spread of surveillance institutions (they see the development of a ‘monumental tide of surveillance which washes over us all’ - Haggerty and Ericson 2000: 609).

Secondly, we expect a significant degree of coercion to be required in the mediation of surveillance. Though Haggerty and Ericson theorise assemblages whose constituent parts cooperate to mutual benefit, in our reading mediators of surveillance rarely have an outright incentive to pass on information. Banks, for instance, have to go to significant time and expense to check their customers are not conducting financial fraud. The only way to persuade them to do so is to impose heavy regimes of liability, backed up by checks and financial sanctions. Finally, we expect the mediation of surveillance through third parties to have significant consequences for the effectiveness through which it is carried out, the opportunities that those who are “surveilled” have to resist the system, and the overall outcomes of the institution. Mediating surveillance, in other words, may create new opportunities for both watcher and watched. This is something which the literature has so far left underexplored.

In this article, we aim to explore these expectations through the example of online copyright enforcement in Europe. The internet as an environment presents an excellent opportunity to explore mediation because it represents a peculiar regulatory challenge for national governments. Its transnational nature challenges laws and regulations based around national political systems. Its design means that its users are relatively anonymous, or at least very complicated to identify from a legal point of view. Finally, its constantly evolving technology challenges attempts to create workable governance solutions, which will often be out of date even before they are brought into law.

Because of this challenge, we argue, governments are especially likely to resort to mediation. The major actor which is called upon to mediate surveillance online is the internet service provider [ISP]. ISPs are uniquely placed to observe the actions of their users. As Paul Ohm puts it:

‘Because the ISP is the gateway—the first hop—to the Internet, almost any communication sent to anybody online is accessible first by the ISP. Like the

naked eye, ISPs can view our online activity across the Internet landscape, seeing everything we do regardless of destination or application. In fact, no other online entity can watch every one of a user's activities, making the ISP's viewpoint uniquely broad.' (2009: 1438)

ISPs are also uniquely positioned to help other actors observe the actions of internet users. When a connection is made to a website, for instance, all the website sees is an IP address. This IP address cannot straightforwardly be connected to a particular individual². IP addresses can, however, be connected to the person or institution which allocates the IP address. These institutions, which are most often ISPs, are allocated chunks of IP addresses by regional "internet registries", which themselves receive them from the Internet Corporation for Assigned Names and Numbers [ICANN], the private organisation dedicated to allocating IP addresses (for an overview see Muller 2008: 4-6). Upon request, the ISP in question should be able to connect a given IP address with a particular account holder. In other words, ISPs occupy a special position in internet architecture. In Jon Zittrain's words, they represent natural "points of control" of content produced online (2003).

Contemporary governments are currently pursuing a wide variety of policy initiatives aimed at regulating certain aspects of online life, and thus reducing certain types of harmful activity such as distribution of terrorist material, incitement to religious hatred, the sale of extreme or child pornography and the violation of copyright and intellectual property rights. In this article, we choose to focus on the last aspect, largely because legal regimes surrounding the protection of copyright online are probably the most well developed, and hence provide more material for investigation and comparison.

We pursue a comparative analysis of four different countries (the UK, France, Italy and Spain). A comparative analysis is helpful in this instance because of the diversity of European approaches to the regulation of copyright enforcement. Looking at the mediation of surveillance in different contexts will allow us to highlight general characteristics relevant to the theory of assemblage in a way that a single case study would not. We chose to focus on these four countries in particular for several reasons. Firstly, they present a range of different stances on copyright enforcement, ranging from the more punitive approaches of the UK and France to the relatively lax stance adopted in Italy and Spain. Secondly, they have a variety of different legal systems and cultures, from the common law of the UK to the civil law of the three continental countries. Finally, they have diverse approaches to the question of digital "civil liberties": in particular, they have data protection authorities of diverging strengths.

Before turning to our case studies, we will provide a brief overview of the legislative situation at the European level, which forms the background context for all our four cases. As Ohm argues, up until now ISPs have made relatively little use of their position as an unrivalled internet "point of control" (2009)³. Indeed, for the most part, their eyes have remained shut to the activities carried out by their customers. One important reason for this, in Europe, is that the potential liability of ISPs (and other intermediaries) for crimes committed by users of their services was curtailed significantly by the European Electronic Commerce Directive [ECD] (Directive 2000/31/EC), adopted in the year 2000 and since then transposed into law in Member States (see Pearce and Platten 2000). This piece of legislation aimed to harmonise certain rules on ISP liability, following several court cases in EU Member States (Pearce and Platten 2000: 372). In particular, it aimed to establish a common minimum standard of protection for ISPs, which Member States could widen if they wished to, but not go below (Stalla-Bourdillon 2011: 52). It did so by establishing specific exemptions, also called "safe harbour provisions", for third party content which ISPs cache, host or transmit (Peguera 2010: 151). The directive also specifically forbade Member States from introducing legislation which required those transmitting content to systematically keep it under surveillance. This directive reinforces the absence of surveillance in online space in Europe. It creates a situation where an ISP has little to gain⁴, and potentially much to lose, by knowing

what is transmitted over or hosted on its networks (for a discussion see Bodard 2003: 268-269).

The ECD does not provide ISPs with the freedom to completely ignore illegal content. In particular, it does require those hosting such content (that is, storing it on their servers) to remove it expeditiously once they have “actual knowledge” of its presence, a so called “notice and takedown” procedure (Moore and Clayton 2009). Importantly, as Pablo Baistrocchi points out (2003: 124-125), it does not specify exactly how such a procedure might take place, leading to a diversity of opinions about what constitutes such knowledge (from a prior decision of a court to an email from a third party) and what format those wanting to provide such knowledge have to give it in (for example, can a rights holder email Youtube asking that all examples of its work be removed from its servers, or does it have to provide a specific link to each individual example of infringement? – see Peguera 2010). While little detailed research exists on the extent to which notice and takedown is used within Europe, studies which have taken place seem to suggest that ISPs act quickly to remove content simply on the basis of email notification, while conducting little checking of the veracity of the claims (see e.g. Nas 2004).

The existence of such procedures encourages those with an interest in the legality of internet content to engage in the active surveillance of the online environment (as Katyal, 2004, argues), looking for ISPs hosting illegal content, in order to ask them to remove it; and, in recent years, several pieces of legislation have attempted to extend this ability.⁵ At the forefront of these efforts has been recent legislation aimed at combating copyright infringement, frequently referred to as “piracy”. While all of this legislation differs, it also has one thing in common: the important position of the ISP in the production of surveillance and control. As Fanny Coudert and Evi Werkers put it, ‘copyright societies are currently pushing for increased private enforcement of intellectual property rights on the Internet, in particular by trying to involve Internet Service Providers (ISPs) in their combat against copyright infringements’ (2010: 50).

The EU continues to legislate in the area. However, in the absence of European wide agreement on what to do, many important decisions have been left to Nation States (for example, in 2008 the ECJ decided that there was no obligation for an ISP to disclose the IP addresses of its users under European law, but neither was it prohibited, passing the responsibility to Member States to decide – see Coudert and Werkers 2010: 51). This situation has led to considerable diversity within European States over the regulation of copyright online, making it an especially fertile area for comparative analysis. In the next four sections, we present an overview of the situation in our four countries of study, focussing on the most recent developments in legislation.

UK

We will begin with the situation in the United Kingdom. The Digital Economy Act, which became law in Britain in June 2010, contains two measures designed to restrict online copyright infringement (sections 3-18 of the act). Most controversial amongst these is the creation of “copyright infringement reports” [CIR], a tool which a rights holder can use to initiate a system of sanctions against individuals thought to be violating copyright. The precise mechanics of a CIR are set out by the “Initial Obligations Code”, a set of rules to be created by Ofcom, the UK’s independent regulator of the communications industry. At the time of writing this code was available in draft format only (see OFCOM 2011: 42-64), and had yet to be ratified by parliament, hence some of the details provided here may be subject to change. Nevertheless, the draft version provides a good idea of how the act could work in practice.

According to the wording of the act, if it appears to the copyright owner that a certain IP address has infringed on their copyright, they have the right to submit such a report to the internet service provider responsible for the IP address (OFCOM 2011: 45), who is then responsible for sending details of the report on to the person who holds the account (OFCOM 2011: 51-52). Rights holders are also allowed to request from ISPs aggregate “infringement lists” of those subscribers who have had at least three copyright infringement reports relating to their work (OFCOM 2011: 48), so as to pursue litigation against them. Furthermore, the Secretary of State may decide to impose “a technical obligation” on the ISP to limit the access of the internet subscriber in some way. This may include reducing the bandwidth available to the user (making downloads of large files like films impractical), preventing (or trying to prevent) peer-to-peer connections, or conducting more invasive surveillance of the user’s account. Or it may simply involve suspension of the individual’s internet access.

All these measures amount to increased incentives for copyright holders to monitor the behaviour of individuals using the internet as a means of watching or listening to copyrighted material (especially those connected to peer-to-peer networks). This incentive has not gone unnoticed: a recent study claimed that several companies were engaged in the en masse collection of information (particularly IP addresses) about those using peer-to-peer technology; many of which appeared not to be copyright holders per se, but rather private companies who might intend to sell this information on at a later date.

The Digital Economy Act also contained provisions for injunctions to be provided against specific locations on the internet (sections 17 and 18), which would have required service providers to prevent their subscribers from having access to these locations. Again, the motivation is copyright: the secretary of state can make provision for the injunction only when a court is satisfied that the website is facilitating access to “a substantial amount of copyright material”, either by hosting it itself or, potentially, by linking to it. Even before these measures have been implemented, a UK High Court granted an order on behalf of the Motion Picture Association requiring British Telecom [BT], the largest British ISP in terms of subscriber numbers, to block access to “Newzbin2”, a file sharing website, the first time such an order had been granted in the UK ([2011] EWHC 1981 (Ch)). This case turned on an argument about whether BT had “actual knowledge” that its subscribers were using its services to infringe copyrighted material, and thus could be served an injunction under the provisions of the information society directive (Directive 2001/29/EC). The judge determined that they did (Article 157 of the judgment). The ruling was widely viewed as potentially the first of many, as future injunctions claims are unlikely to be challenged (Ashford 2011). Also of importance was the fact that Newzbin2 was not hosted in the UK, making blocking the only sanction the MPA could realistically pursue in UK courts. BT already takes step to block some websites on the internet through an inbuilt filter called “cleanfeed”, which had been developed to block websites suspected of containing child pornography, in collaboration with the “internet watch foundation”, a non-profit organisation which encourages members of the public to submit links to potentially offending material (and thus itself an interesting example of public participation in online surveillance). Newzbin2 could in theory be added quite simply to this filter, something which proved important in the judgment. However, it is unclear whether BT will really be able to effectively block the site (see Clayton 2011), and, importantly, what the court will require them to do if they are not (Halliday 2011).

To what extent the provisions of the Digital Economy Act will be implemented remains to be seen, though despite legal challenges Ofcom appears set to press ahead. Nevertheless, several conclusions can be drawn for the more general topic of surveillance mediation. Firstly, we can see that surveillance of online copyright in the UK is essentially a four way relationship, between companies hosting potentially infringing material, companies providing internet access, individuals using that access and rights

holders themselves. The government is involved only to the extent that it sets the rules of the game in terms of what power rights holders have to oversee the use of their material. Secondly, we can see that the decision about where to locate the surveillance (with the ISP) depends crucially on what knowledge they have; something which is fiercely debated in court. Thirdly, as Aaron Martin (et al. 2009) speculated, the inclusion of mediators serves to increase potential points of resistance to surveillance, demonstrated by continuing legal challenges to both the DEA and other types of internet blocking.

FRANCE

We will now turn our attention to France, where, in 2009, a new administrative authority was created: the *Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur l'Internet* [HADOPI] ("High authority for the distribution of creative work and the protection of copyrights on the internet")⁶. Hadopi aims to combat illegal file sharing through a system of surveillance of peer-to-peer traffic, supplemented by a system of sanctions known as a "graduated response" (Meyer and Van Audenhove 2010; Dejean et al. 2010)⁷. The HADOPI body itself acts as a coordinator of the sanctions. Online copyright holders are allowed to send in reports of apparent copyright infringement to HADOPI, which checks that these reports contain sufficient information to warrant a response. If so, the body sends a series of letters to the person who owns the connection suspected of infringing. Two warning letters are sent; upon receipt of a third complaint, the case is sent to a judge⁸, who decides if there is sufficient evidence to warrant suspension of the internet account.

While in theory a variety of methods are available to rights holders who wish to look for online infringements, in practice the majority of infringement reports are sent by Trident Media Guard [TMG], a private company contracted by music industry rights holders in France. TMG conducts surveillance on peer-to-peer networks on the basis of a library of 10,000 different pieces of music (which is updated periodically), and sends infractions on to HADOPI (Rees 2010e). Up to 25,000 submissions per day are allowed, while TMG also retains this information for use in potential prosecutions (Rees 2010a).

The law was very recently introduced, so it is too early to say with any great certainty how effective it will be. Preliminary evidence is mixed. HADOPI themselves conduct online polling to try and establish their own impact, and their most recent survey (HADOPI 2011) seemed to indicate some success: 41 per cent of those asked indicating that the law had compelled them to change the way they gain access to copyright material online. However, a survey conducted by Sylvain Dejean et al. (2010), seemed to suggest that many users may simply be switching to other methods of illegal viewing, rather than purchasing content lawfully. This highlights once again the important impact that changes in technology can have undermining systems of surveillance.

The HADOPI law is interesting for the mediation of surveillance for several reasons. Firstly, it recognises the fact that, even with the help of an ISP, an IP address may be difficult to securely connect to an individual person: an internet contract holder might possess more than one IP address (for example, a home wifi network might have several different computers connected to it), more than one computer might use the same IP address, and more than one person might use the same computer. As we expected in other words, mediation of surveillance occurs when the surveillant institution (in this case rights holders) have limited information. However, it transforms this previously anonymising characteristic of the internet into a way of deciding where to place surveillance: with the holder of the internet account. As the law puts it, it is the subscriber's obligation to secure their internet access, and to make sure it is not used for illegal downloads⁹. Hence here in fact it is not so much the ISP but the individual subject who is employed as the mediator of the mechanism of surveillance.

Secondly, the system of graduated response develops a new regime of sanctions. The warning letter to the subscriber serves to remove any sense of perceived anonymity online: upon receipt, the user will become aware that at least some of their actions are being monitored. This is designed to lead them to modify their own behaviour, either by changing their own online activities or monitoring the activities of others who use their internet connection. The warning letter also contains information about security measures the subscriber can take in order to obstruct illegal downloads, such as the installation of various types of security software. If repeated infractions are discovered, the law allows the complete suspension of a user's internet access for a period of up to a year; but this suspension may be reduced or even eliminated, if the user accepts the installation of security software. Sanctions therefore become a mechanism of ensuring the participation of mediators (while the aim of modifying user behaviour invites comparisons with the "panopticon" style of surveillance mentioned above).

Thirdly, in contrast to the UK, it is important to note the central place of the HADOPI body in the surveillance system, acting as a clearing house for infringement reports. HADOPI has been designed to accept automatic submissions of infringing IP addresses, which presents the first genuine opportunity to enforce copyright through the *en masse* sanctioning of individuals. In late 2010, HADOPI was sending several hundred warning emails per day, though it aimed to raise that number to 2,000 by the end of the year (Rees, 2010f). While, as Nicola Lucchi points out, 'this is much lower than the number of illegal downloads actually committed', and certainly lower than the number of complaints it was receiving from TMG, it still represents an astonishingly high figure (Lucchi 2011: 25). TMG have since confirmed that the IP addresses sent will not be checked individually by a human operator: the system, in other words, is entirely automatic from complaint to sanction (Champeau 2010b).

ITALY

We will now turn our attention to the case of Italy. In March 2010, the so called "Decreto Romani", named after the Minister for Economic Development Paolo Romani, was approved by the Council of Ministers (Apa and Besemer 2010). The decree made a series of modifications to Italy's media law (the "*Testo Unico dei servizi di media audiovisivi e radiofonici*"). One of the most important of these was the attribution of responsibility for regulating copyright online to the "*Autorità per le Garanzie nelle Comunicazioni*" [AGCOM], Italy's national communications regulator.¹⁰

On the 6th of July 2011, AGCOM approved a draft regulation (668-10), which it opened to public consultation before the final text, in November 2011 (Scorza 2011). The regulation itself has two main parts. The first deals with a series of measures designed to help stimulate the legal market for online media. The second, of more interest to the present discussion, sets out a range of sanctions designed to combat copyright theft. Unlike the Hadopi law and the Digital Economy Act, the AGCOM regulation deals only with internet service providers, and targets especially those hosting content. It provides a two stage procedure for those who suspect their copyright has been infringed upon (AGCOM, 2011), though it should be noted that wide exceptions are provided for educational, scientific and not for profit use.

In the first place, the rights holder can submit a report to the host provider of the website, detailing the sites which are alleged to have infringed upon copyright (the format for which is set out in AGCOM 2011: 15). If the host does not agree the material infringes, or otherwise fails to remove the content, the matter can be passed to AGCOM, which has ten days to undertake a process of deliberation. After this time, the authority will either order the removal of the material, or its reinstatement. The website host is liable to pay a heavy fine if they do not comply with the results of the order. If the host is outside of Italy, AGCOM will send several messages asking them to remove the

content; if this is unsuccessful, they will refer the matter to the courts. Whether the site is foreign or not, AGCOM will also have the power to request internet service providers to block access to specific sites which are deemed infringing (Article 14 and 15; Boresa 2011).

In many respects, the AGCOM regulation does little more than formalise the notice and takedown procedure which was partially created by the ECD. In particular, the aim was to make this procedure effective, as before even if it did theoretically exist there was little possibility of effective enforcement. This absence of functioning notice and takedown procedure was a major contributing factor in Italy's inclusion on the US Trade Office's "Watch List" of countries with, in their opinion, deficient intellectual property regimes, something which itself seems to have been a motivation behind the AGCOM regulation (AGCOM 2011: 38). The AGCOM case highlights a further aspect of the mediation of surveillance: how the mediator may have much less incentive to resist surveillance than the individual. The ISP must take responsibility for the content it hosts, paying fines if it does not remove it expeditiously, and facing legal battles to keep content online.

As Marco Pierani and Mauro Vergari note, ISPs will have little incentive to contest requests received to remove material, as it was not theirs originally (2010: 62-63). While the person who uploaded the content might conceivably wish to complain, the hoster is not under any obligation to inform them that the process is going on, making it likely that any request will be automatically complied with. Unlike in France and the UK therefore, the mediation of surveillance here, somewhat paradoxically, removes the subject of surveillance (that is the person uploading the content) almost entirely from the equation. This serves to reverse the position of knowledge of copyright infringement quite radically. Rather than a situation where absolute knowledge is required of an infringement, something which ISPs were hardly likely to obtain, the slightest suspicion could become grounds for the removal of content. Clearly, as in France, if the potential volume of requests approaches that seen in France (with TMG sending 25,000 requests per day, albeit in the context of peer to peer sharing rather than hosting), it is possible that ISPs will not even have time to confirm their *prima facie* veracity, let alone contest ones that do not appear credible. Here the system may tend towards full automatised.

However, also of interest in this context are related legal judgments in the area. Of particular relevance is the Peppermint case (AGCOM 2011: 13; Caso 2007). In this case, a private company acting on behalf of Peppermint records collected the IP addresses of several thousand users of peer-to-peer networks; Peppermint records went to court to seek the names of those users. The court established that the ISP could not provide them. Furthermore, the Italian Data Protection authority established that the very act of collecting the IP addresses was illegal, as there were no grounds providing for it in the Italian Data Protection Act (Coudert and Werkers 2010: 60). In contrast to the UK and France, therefore, Italy erects a specific barrier to the prosecution of individuals in the online environment, creating a natural obscurity which hides their identities (something which is another factor in Italy's continuing presence on the US Trade Office Watch list), and also limiting the likely involvement of third party companies such as Trident Media Guard.

SPAIN

The recent approval of the Sustainable Economy Law has introduced significant changes in the methods through which copyright infractions are combated in Spain. The relevant parts of this law, known as the "*Ley Sinde*" in reference to the Minister for Culture Ángeles González-Sinde who was responsible for its drafting, has generated an intense debate in both social and political spheres, promoted especially by associations of internet users in the defence of universal access to culture and freedom of expression.

Spain adopts a particularly permissive stance towards online file sharing, with wide exceptions for those who download content for private, non-commercial use. In fact, in its 2011 report, the US Congressional Anti-piracy Caucus placed the Iberian country among the top five countries worldwide with the most illegal downloads (the others being Canada, China, Russia and the Ukraine), arguing that illegal downloaders from peer-to-peer networks act with “near impunity” (CIAPC 2011: 4).

The Sinde Law was designed to alter this situation somewhat. However, it is not directed specifically towards consumers, rather, the principle target of the *Ley Sinde* are the intermediaries which facilitate the illegal download of content, in particular web pages which contain links to files for peer to peer download (Peguera 2010: 163). In this respect, the *Sinde* law has more in common with the *Decreto Romani* in Italy than the Hadopi or Digital Economy laws in France and the UK, as it does not target individual users. However, the text of the *Ley Sinde*, whose precise functioning awaits further definition, is ambiguous. It allows the adoption of measures against service providers who act ‘for profit, directly or indirectly, or who have caused or is susceptible to causing patrimonial damage’. So while in theory it is aimed only at web pages containing lists of links to pirated material, in practice this formulation could apply to a wide variety of services and situations.

The mechanism through which these websites are targeted is also similar to that of the *Decreto Romani*. The law aims to endow the Intellectual Property Commission, part of the Ministry of Culture, with the power to restrict the activities of these types of web pages, up to and including requiring their eventual closure. This administrative organ establishes in the first instance whether a website is indeed violating intellectual property rights. Following a heated debate, it was determined that the administrative body will not be able to order the takedown of the website without authorisation from a judge, as web pages are a type of media, which, following article 20.5 of the Spanish constitution, cannot be shut down without a court order (Peguera 2010: 164). However, the court themselves will not be able to assess the alleged copyright violation, but only confirm the constitutionality and proportionality of the measures proposed. Their inability to rule about the existence of the claimed infringement will, somewhat paradoxically, make it very difficult to confirm this proportionality.

Furthermore, current case law provides little legal basis for the act. Existing court decisions have consistently rejected the idea that the mere fact of creating a hyperlink could be an infraction of the Intellectual Property law, regardless of what type of page the link points to. In this way, as Miquel Peguera argues, the *Ley Sinde* appears like an administrative way of achieving something that the courts have been so far denying (Peguera 2010: 165). As the *Ley Sinde* has not reformed the underlying Intellectual Property Law upon which previous judicial decisions are based (by, for example, establishing clearly that linking constitutes an infringement, or creating the offence of contributory infringement seen in other jurisdictions) the *Sinde* Commission will conduct its work in the absence of a proper legal basis: in fact, they will be forced in a sense to ignore existing interpretations of the law made by the judicial system. Here we can see, in other words, that the creation of intermediaries not only creates points of responsibility and resistance, but can help to shift these points as well. The creation of the *Sinde* law was an attempt to deliberately bypass judicial control of copyright enforcement, or at least limit it to a procedural check rather than a substantial determination of the merits of an individual case.

ANALYSIS: THE EFFECTS OF MEDIATING SURVEILLANCE

A complex “assemblage” of actors are implicated in the control of the internet: private actors, internet service providers, autonomous regulators, as well as of course legislators and the judiciary. In Europe, this situation is further complicated by quite diverse

national contexts, with only weakly harmonised community law. While France and the UK have implemented a range of increasingly aggressive pieces of online surveillance technology, Italy and Spain have taken different approaches, with their courts especially limiting to a great extent what types of online activity can be controlled. Despite this variety of approaches, a few general conclusions can be drawn about the mediation of surveillance. In this section, we seek to draw these conclusions out.

The first conclusion relates to the selection of surveillance mediators. Surveillance is distributed onto the “points of control” which are perceived to be capable of achieving it. As we outlined above, ISPs are the most frequent mediator of online surveillance; but they are by no means the only one. Individual users are also being pressed into taking legal responsibility for the surveillance and protection of their own internet connections, at least in the UK and France, which is a way of getting round the difficulty of securely connecting an IP address to a particular person. This may place these users in the invidious position of having to regulate the activities of their friends and family members, who may also be using their connection. Meanwhile, rights holders themselves can also act as a point of control, exploiting the overall visibility of the internet to conduct surveillance of their own works; and they frequently have done, often through privately contracted firms. Differing national viewpoints on the practice exist, but where it is allowed, this “privatization” of copyright enforcement presents an enormous data gathering opportunity for private firms (Scorza 2008: 87), and also allows them to be somewhat selective in what rights they actually enforce; in the US at least they have tended towards tolerating many types of use (Katyal 2009). It is a tendency that also seems to risk disadvantaging smaller rights holders, who perhaps lack the capacity to effectively police their work (Meyer and Van Audenhove 2010: 77).

This distribution of responsibility points to the importance of the *capacity* of mediators to regulate surveillance, which is one of the crucial means through which such mediators are selected. Many ISPs have attempted to argue, as in the Newzbin case, they do not have the ability to conduct the surveillance being assigned to them as they are not in a position to know when content is infringing. ISPs can also argue that they do not have the financial capacity to fulfill their surveillance obligations, and many pieces of legislation refer to the need for the duties imposed on ISPs to be proportionate in terms of the effort required, or have (as in the example of OFCOM’s code of conduct) restricted their obligations only to larger ISPs. The capacity of mediators, crucially, is not fixed. The way information flows online is mutable in a variety of ways; and the speed with which this changes can defy conventional regulation attempts. The displacement effect of online surveillance can be high, as the cost of changing to a different form of communication is quite low for users. So, as we noted in the French case, the rise of streaming media makes it less necessary for copyright infringers to use peer-to-peer technology, which erodes the utility of the Hadopi law. In the case of the DEA, meanwhile, the difficulty of blocking websites for any length of time was acknowledged, especially acute in, for example, the broadcast of live sports events. But it may also cut the other way: the changing makeup of service providers themselves could in fact increase both their capacity and even their incentives to control online users. As we noted in the Newzbin case, the pre-existence of a filter makes it easier for more websites to be added.

A second conclusion is that mediation of surveillance also implies the mediation of sanctions; and these sanctions can be inexact. Points of control are proxies for the subject of surveillance (Kreimer 2006), providing a sort of indirect and in many cases approximate access. As several commentators have noted, the potential suspension of internet access punishes all users of that account, even if only one of them had committed any infringement. The blocking of websites presents a similar problem: an IP address can encompass a website with both legal and illegal functions, or may well even encompass several websites. This approximation of access is something that can cut both ways. On the one hand, it seems likely that punishments handed down might be

too broad, unjustly falling on innocent victims. On the other, it also provides potential for infringing material to hide amongst the crowd, in a certain sense. In this respect, it is interesting to note the careful consideration made in the Newzbin case of whether any part of the site offered legal content; in the future, we may well see copyright infringing sites adding legal sections to their websites, in the hope of evading being blocked.

Finally, and perhaps most importantly, the distribution of surveillance onto mediators also serves, as Martin et al. have noted (2009), to distribute the possibilities for the resistance of that surveillance. By acting as a point of connection between rights holders, internet users and ISPs, administrative bodies can both regulate how surveillance is performed (by formalising notice and takedown procedures and thus guaranteeing rights) and facilitate its execution (by automating procedures to sanction individuals). ISPs themselves can, in certain circumstances, check individual claims made by rights holders against them, as in the notice and takedown procedure formalised in the AGCOM regulation, or the copyright infringement reports to be made under the DEA. Here, the worry is of course that the ISPs themselves will have little incentive to contest these on a case by case basis.

CONCLUSION

We will conclude with some brief remarks about the future of surveillance of copyright online, which illustrate the importance of understanding the dynamics of the mediation of surveillance. While media lobbies remain powerful, and their business models remain open to online abuse, the development of copyright enforcement is likely to continue to be a topic of interest: more legislation undoubtedly awaits. Several areas of change are important. The diversity of national opinion on the subject means that EU legislation on issues such as graduated response seems unlikely in the near future (Meyer and Van Audenhove 2010: 73)¹¹: however other pieces of EU legislation such as the recently negotiated telecoms package may well turn out to be important in the area (Horten 2011), while the EC is also in the process of negotiating recommendations on notice and takedown procedures, albeit ones targeted more at xenophobia, terrorism and child pornography than copyright offences (McNamee, 2010). Different national initiatives are also likely to continue, as legislators struggle to accommodate the demands of both the creative industry and international trading partners such as the US. Furthermore, the continuing evolution of web services will mean the continuation of an active role for the courts in deciding the applicability of old rules to new contexts. The rise of Web 2.0 services also deserves a mention in this regard: sites such as Youtube blur the distinction between content provider and content hoster (though most decisions have extended the liability protection of the ECD to cover these types of services, providing they have efficient notice and takedown procedures – see Viola et al 2010). Recent US court cases on whether safe harbour protection can be extended to those providing “cloud services” (Rosenblatt 2011) and on the exact nature of the knowledge required to bring about ISP liability (Gray 2011) may well be duplicated at some point in Europe. While it is difficult to predict with any certainty what direction these initiatives will take, one area which seems likely to be the focus of conflict is that of outright blocking: either through the disconnection of users who are deemed to have committed copyright offences, or the blocking of (foreign) websites from entire national internet spaces. The symbolic finality of this blocking has made it a focal point of resistance: the idea of user disconnection, for example, has been criticised by the European Parliament, European Data Protection Supervisor (EDPS 2010), and the UN Special Rapporteur for Human Rights (Human Rights Council 2011); while the idea of website blocking was seen as potentially contrary to EU law in a recent opinion of an ECJ advocate general (OSCE 2011: 143).

Given the strength of these opinions, it seems quite likely that both legislators and courts will move in the direction of requiring increased surveillance of infringing user's

accounts, rather than outright disconnections or blocking, at least in a majority of cases (as Katyal suggests, in the US record industries are also moving from hard sanctions such as prosecution to more passive types of surveillance – see Katyal 2009). Several technical options may be available to them: in the UK, it has been proposed that account speed be limited enough to make downloading infeasible, whilst in France the SCPP are continuing the development of filtering software which blocks access to specific files (Rees 2010e). These solutions may seem, *prima facie*, less extreme, but they bring with them the worrying possibility of the continued development and normalisation of online surveillance technology. As we argued above, the mere existence of this technology affects legal decisions about whether it should be used, as it reduces costs for the mediator of surveillance. This could lead to a potential ratchet effect, whereby each decision compelling the use of surveillance tools furthers their development, making subsequent uses more likely. It is in this area that understanding the dynamics of the mediation of surveillance becomes crucial.

* * *

ACKNOWLEDGEMENTS

The authors would like to thank Miguel Peguera, Angela Daly, Ben Farrand, Aaron Martin and Marcus Felson, all of whom provided useful comments and criticisms on earlier drafts of this paper. We would also like to thank the members of LiSS Working Group 4, especially Charlotte Bagger Tranberg, for their discussion and encouragement, as well as the editors of JCER and this special issue, and two anonymous reviewers, for their helpful comments and suggestions. All errors and omissions remain our own.

¹Though beyond the scope of the present article, it is worth mentioning that debate exists about the appropriateness of “assemblage” as a translation of the French word *agencement* originally employed by Deleuze and Guattari. See Phillips 2006 for a brief overview.

² Of course, many websites have mechanisms, such as cookies, or ask for information, such as a username and password, which *try* to identify their users. But only the ISP is capable of knowing for certain to whom an IP address is allocated.

³ Ohm was talking specifically about ISPs based in the US. However the point applies in Europe as well.

⁴ With the rise of what is known as “Deep Packet Inspection” technology, some are beginning to argue that ISPs might develop their own commercial interest in knowing what is transmitted over their networks. Deep Packet Inspection is however beyond the scope of the present article.

⁵ As yet, no legislation exists which aims to substantially reverse provisions of the ECD (indeed, the safe harbour provisions were once again reaffirmed in the EU’s 2009 Universal Services Directive - see Viola et al, 2010).

⁶ In France, Spain, and Italy, there exists no direct translation of the term “copyright”. Rather, there is what might be translated as the “Right of the Author” (*droit d’auteur*, *diritto d’autore*, *derecho del autor*).

⁷ A peer-to-peer network is one which enables the direct connection of two computers across the internet, a connection which can be used for a variety of purposes, such as the transmission of files. (Riehl, 2001)

⁸ The necessity of judicial authorisation for the suspension of internet accounts was a key point in the legislative debate over Hadopi. (Lucchi, 2011)

⁹ This obligation was actually introduced by a preceding piece of legislation.

¹⁰ Although this responsibility had been accreting little by little in various preceding pieces of legislation (Aria, 2011: 3).

¹¹ There was some speculation that it would form part of the recently negotiated Anti-Counterfeiting Trade Agreement, but in the end this proved not to be the case (see DG EXPO 2011: 57).

REFERENCES

- AGCOM (2011). 'Consultazione pubblica sullo schema di regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica (Delibera n. 668/10/CONS)', *Gazzetta Ufficiale della Repubblica italiana*, 163. Available at: <http://www.agcom.it/default.aspx?DocID=6693>. Last accessed 30 September 2012.
- Agustina, J. R. (2010). 'La arquitectura digital de Internet como factor criminológico: Estrategias de prevención frente a la delincuencia virtual', *International E-Journal of Criminal Sciences*, 4 (3), pp. 1-31.
- Apa, E. and Besemer, F. (2010). 'Il nuovo Testo Unico dei Servizi di Media Audiovisivi: le innovazioni del Decreto Romani', *Key4biz*, 5 March. Available at: http://www.key4biz.it/News/2010/03/05/Policy/decreto_romani_agcom_minori_diritto_dautore_lcn_product_placement_pubblicita.html. Last accessed 30 September 2012.
- Aria, L. (2011). 'Azioni positive ed enforcement, le due "gambe" del regolamento', *lettera@gcom*, 3/2011, pp.3-6. Available at: <http://www.agcom.it/default.aspx?DocID=6877>. Last accessed 30 September 2012.
- Ashford, W. (2011). 'Why the High Court ruling in the Newzbin2 case is such a big deal', *ComputerWeekly*, 29 July. Available at: <http://www.computerweekly.com/Articles/2011/07/29/247456/Why-the-High-Court-ruling-in-the-Newzbin2-case-is-such-a-big.htm>. Last accessed 30 September 2012.
- Baistrocchi, P. A. (2003). 'Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce', *Santa Clara Computer & High Technology Law Journal*, 19 (1), pp. 111-130.
- Bergström, M., Helgesson, K. S., Mörtz, U. (2011). 'A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management', *Journal of Common Market Studies*, 49 (5), pp. 1043-1064.
- Bodard, K. (2003). 'Free access to information challenged by filtering techniques', *Information & Communications Technology Law*, 12 (3), pp. 263-279.
- Boresa, G. (2011). 'Ecco la delibera Agcom sulla pirateria online', *Mytech*, 6 July. Available at: <http://mytech.it/web/2011/07/06/ecco-la-delibera-agcom-sulla-pirateria-online/>. Last accessed 30 September 2012.
- Brenner, S. W., Clarke, L. (2005). 'Distributed Security: Preventing Cybercrime', *John Marshall Journal of Computer and Information Law*, pp. 659-709.
- Caso, R. (2007). 'Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint - profili di diritto comparato'. Technical Report, Scienze Giuridiche, University of Trento. Available at: <http://www.jus.unitn.it/users/caso/DRM/Libro/peppermint/home.asp>. Last accessed 30 September 2012.
- Champeau, G. (2010a). 'HADOPI: la CNIL avait dénoncé l'absence de contrôle de TMG !', *Numerama*, 20 September. Available at: <http://www.numerama.com/magazine/16826-hadopi-la-cnil-avait-denonce-l-absence-de-controle-de-tmg.html>. Last accessed 30 September 2012.
- Champeau, G. (2010b). 'Hadopi : 10 % d'échec dans l'identification des abonnés ?!', *Numerama*, 25 October. Available at: <http://www.numerama.com/magazine/17144-hadopi-10-d-echec-dans-l-identification-des-abonnes.html>. Last accessed 30 September 2012.
- CIAPC. (2011). '2011 Country Watch List'.
- Clark, B. (2007). 'Illegal downloads: sharing out online liability: sharing files, sharing risks', *Journal of Intellectual Property Law & Practice*, 2 (6), pp.402-418.
- Clayton, R. (2011). 'Will Newzbin be blocked?', *Light Blue Touchpaper*, July 28. Available at: <http://www.lightbluetouchpaper.org/2011/07/28/will-newzbin-be-blocked/>. Last accessed 30 September 2012.
- Cohen, J. E. (2006). 'Pervasively Distributed Copyright Enforcement', *Georgetown Law Review*, 95, pp. 1-48.
- Coudert, F., and Werkers, E. (2010). 'In The Aftermath of the Promusicae Case: How to Strike the Balance?', *International Journal of Law and Information Technology*, 18 (1), pp. 50-71.

Dandeker, C. (1990). *Surveillance, power and modernity: bureaucracy and discipline from 1700 to the present day*, Cambridge: Polity Press.

Dejean, S., Pénard, T., and Suire, R. (2010). 'Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français'. Study prepared for M@rsouin, CREM and the University of Rennes. Available at: <http://www.01net.com/fichiersAttaches/300415066.pdf>. Last accessed 30 September 2012.

Deleuze, G., and Guattari, F. *Mille Plateaux*, Paris : Éditions de minuit.

DG EXPO. (2011). *The Anti-Counterfeiting Trade Agreement (ACTA): An Assessment*. Brussels: European Parliament.

EDPS. (2010). 'Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (2010/C 147/01)'. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf. Last accessed 30 September 2012.

Foucault, M. (1975). *Surveiller et Punir: Naissance de la prison*, Paris: Gallimard.

Gray, N. J. (2011). 'Blindsided! Will U.S. Supreme Court Patent Ruling on Willful Blindness Determine Standard for Red-Flag Knowledge Under DMCA?', *The 1709 Blog*, 5 July. Available at: <http://the1709blog.blogspot.com/2011/07/blindsided-will-us-supreme-court-patent.html>. Last accessed 30 September 2012.

Giddens, A. (1987). *The Nation State and Violence*, Berkeley: University of California Press.

Guiraudon, V. (2003). 'Before the EU border: remote control of the "huddled masses"', in K. Groenendijk, E. Guild, and P. Minderhoud (eds), *In search of Europe's borders*. New York: Kluwer Law International, pp. 191–214

HADOPI. (2011). 'Hadopi, biens culturels et usages d'internet: pratiques et perceptions des internautes français'. Available at: http://www.hadopi.fr/download/sites/default/files/page/pdf/t1_etude_courte.pdf. Last accessed 30 September 2012.

Haggerty, K. D. (2006). 'Tear down the walls: on demolishing the panopticon', in D. Lyon (ed), *Theorizing Surveillance*. Portland: Willan Publishing, pp. 23-44

Haggerty, K. D., and Ericson, R. V. (2000). 'The surveillant assemblage', *British Journal of Sociology*, 51 (4), pp. 605-622.

Halliday, J. (2011). 'Filesharing: BT and TalkTalk fail in challenge to Digital Economy Act', *The Guardian*, 20 April. Available at: <http://www.guardian.co.uk/technology/2011/apr/20/filesharing-bt-talktalk-digital-economy-act>. Last accessed 30 September 2012.

Hesseling, R. (1994). 'Displacement: A Review of the Empirical Literature', *Crime Prevention Studies*, 3, pp.197-230.

Hier, S. (2003). 'Probing the Surveillant Assemblage', *Surveillance & Society*, 1 (3), pp. 399-411.

Horten, M. (2011). *The Copyright Enforcement Enigma: Internet Politics and the 'Telecoms Package'*. London: Palgrave Macmillan.

Human Rights Council. (2011). 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/17/27)'. Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Last accessed 30 September 2012.

Katyal, S. (2004). 'The New Surveillance', *Case Western Law Review*, 54, pp. 297–385.

Katyal, S. (2009). 'Filtering, Piracy Surveillance, and Disobedience', *Columbia Journal of Law & the Arts*, 32 (4), pp. 401-426.

Kreimer, S. F. (2006). 'Censorship by Proxy: the First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', *Scholarship at Penn Law*. Paper 133. Available from: http://lsr.nellco.org/upenn_wps/133. Last accessed 30 September 2012.

Larsson, S. (2011). 'The Path Dependence of European Copyright', *SCRIPT-ed*, 8 (1), pp. 8-31.

- Lianos, M. (2003). 'Social Control after Foucault', *Surveillance & Society*, 1 (3), pp. 412-430.
- Lyon, D. (2007). *Surveillance Studies: An Overview*, Cambridge: Polity Press.
- Lucchi, N. (2011). 'Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI)', *Cardozo Journal of International and Comparative Law*, 19 (3), pp. 645-678.
- Martin, A. K., van Brakel, R., and Bernhard, D. (2009). 'Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework', *Surveillance and Society*, 6 (3), pp. 213-232.
- McIntyre, J. J. (2011). 'Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information', *DePaul Law Review*, 60 (3), pp. 895-936.
- McNamee, J. (2010). 'Commission finds solution on notice and takedown and it seeks the problem', *EDRI-gram*, 8 (24). Available at: <http://www.edri.org/edriagram/number8.24/recommandations-notice-takedown-ec>. Last accessed 30 September 2012.
- Meyer, T., and Van Audenhove, L. (2010). 'Graduated response and the emergence of a European surveillance society', *info*, 12 (6), pp. 69-79.
- Michaels, J. (2010). 'Deputizing Homeland Security', *Texas Law Review*, 88, pp. 1435-1473.
- Moore, T., and Clayton, R. (2009). 'The Impact of Incentives on Notice and Takedown'. In: M. E. Johnson, *Managing Information Risk and the Economics of Security*, London: Springer, pp. 199-223.
- Muller, M. (2008). 'Scarcity in IP addresses: IPv4 Address Transfer Markets and the Regional Internet Address Registries', *Internet Governance Project*. Available at: http://www.internetgovernance.org/pdf/IPAddress_TransferMarkets.pdf. Last accessed 30 September 2012.
- Nas, S. (2004). 'The Multatuli Project: ISP Notice & take down'. Available at: <http://www.bof.nl/docs/researchpaperSANE.pdf>. Last accessed 30 September 2012.
- Nock, S. (1993). *The Costs of Privacy*, New York: De Gruyter.
- Ohm, P. (2009). 'The Rise and Fall of Invasive ISP Surveillance', *University of Illinois Law Review*, 2009 (5), pp. 1417-1496.
- OFCOM (2011). 'Draft Initial Obligations Code'. Available at: <http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/>. Last accessed 30 September 2012.
- OSCE (2011). 'Freedom of Expression on the Internet'. Available at: <http://www.osce.org/fom/80723>. Last accessed 30 September 2012.
- Pearce, G., and Platten, G. (2000). 'Promoting the Information Society: The EU Directive on Electronic Commerce', *European Law Journal*, 6 (4), pp. 363-378.
- Peguera, M. (2010). 'Internet Service Providers' Liability in Spain: Recent Case Law and Future Perspectives', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1 (3), pp. 151-171.
- Pierani, M., and Vergari, M. (2010). 'Gli utenti e il diritto d'autore nel nuovo contesto tecnologico digitale', in F. Sarzana di Santa Ippolito (ed), *Libro Bianco su Diritti D'Autore e Diritti Fondamentali nella Rete Internet*. Rome: FakePress.
- Rees, M. (2010a). 'Hadopi et TMG : un système de seuils aiguillera les sanctions', *PCINpact*, 24 June. Available at: <http://www.pcinpact.com/actu/news/57855-hadopi-seuil-tmg-cnii-deliberation.htm>. Last accessed 30 September 2012.
- Rees, M. (2010b). 'Hadopi : le moyen de sécurisation labellisé, future niche du DPI', *PCINpact*, 2 August. Available at: <http://www.pcinpact.com/actu/news/58565-hadopi-moyen-securisation-dpi-filtrage.htm>. Last accessed 30 September 2012.
- Rees, M. (2010c). 'Hadopi : comment persuader l'abonné de subir le filtrage par DPI', *PCINpact*, 2 September. Available at: <http://www.pcinpact.com/actu/news/59106-hadopi-dpi-vedicis-scip-filtrage.htm>. Last accessed 30 September 2012.

Rees, M. (2010d). 'Hadopi, la négligence caractérisée et la contrefaçon', *PCINpact*, 9 September. Available at: <http://www.pcinpact.com/actu/news/59263-hadopi-negligen-ence-caracterisee-contrefacon-delit.htm>. Last accessed 30 September 2012.

Rees, M. (2010e). 'Interview : la SCPP veut bien marier Hadopi avec filtrage par DPI', *PCINpact*, 16 September. Available at: <http://www.pcinpact.com/actu/news/59386-hadopi-filtrage-dpi-scpp-securisation.htm>. Last accessed 30 September 2012.

Rees, M. (2010f). 'L'Hadopi vise 1000 à 2000 emails/jour d'ici fin 2010', *PCINpact*, 25 October. Available at: <http://www.pcinpact.com/actu/news/60008-hadopi-volumetrie-identification-email.htm>. Last accessed 30 September 2012.

Riehl, D. A. (2001). 'Peer-to-Peer Distribution Systems: Will Napster, Gnutella and Freenet create a copyright nirvana or gehenna?', *William Mitchell College of Law Review*, 27 (3), pp. 1761-1760.

Rosenblatt, B. (2011). 'Mixed Verdict for EMI against MP3tunes.com', *Copyright and Technology*, August 23. Available at: <http://copyrightandtechnology.com/2011/08/23/mixed-verdict-for-emi-against-mp3tunes-com/>. Last accessed 30 September 2012.

Scorza, G. (2008). 'Il diritto d'autore e la società dell'informazione', *Consumatori, Diritti e Mercato*, 2, pp.84-95. Last accessed 30 September 2012.

Scorza, G. (2011). 'Agcom e copyright, cosa sta succedendo', *Wired*, 29 July. Available from: <http://daily.wired.it/news/politica/2011/07/29/agcom-copyright-126238743.html>

Stalla-Bourdillon, S. (2011). 'Uniformity v. Diversity of Internet Intermediaries' Liability Regime: Where does the ECJ stand?', *Journal of International Commercial Law and Technology*, 6 (1), pp. 51-61.

Sweney, M. (2011). 'Government scraps plan to block illegal filesharing websites', *The Guardian*, 3 August. Available at: <http://www.guardian.co.uk/technology/2011/aug/03/government-scraps-filesharing-sites-block>. Last accessed 30 September 2012.

Sweney, M. and Halliday, J. (2011). 'High court forces BT to block file-sharing website', *The Guardian*, 28 July. Available at: <http://www.guardian.co.uk/technology/2011/jul/28/high-court-bt-filesharing-website-newzbin2>. Last accessed 30 September 2012.

Viola de Azevedo Cunha, M., Marin, L., and Sartor, G. (2011). 'Peer-to-peer privacy violations and ISP liability: Data Protection in the User-Generated Web', *EUI Working Paper LAW 2011/011*.

Zittrain, J. (2003). 'Internet Points of Control', *Boston College Law Review*, 44, pp. .653-688.