Article

JIS

Journal of Information Science
XX (X) pp. 1-15

DOI: 10.1177/016555150000000
jis.sagepub.com
SAGE

Online copyright enforcement by Internet Service Providers

Adrienne Muir
Department of Information Science, Loughborough University, UK

Abstract
The culture of online sharing of information on the Internet extends to unauthorised sharing of copyright content, and is perceived as a major threat to copyright owners and content industries. Enforcement of existing copyright laws is difficult due to the widespread nature of unauthorised sharing. Rights holders have pursued individuals and organisations involved through existing legal channels, with limited success. They have also engaged in voluntary arrangements with Internet Service Providers to educate and, potentially punish infringers. Governments have more recently become involved in developing new legislation with similar aims. The approaches to addressing the issue have been controversial, mainly because of lack of transparency in their development and concerns about their potential impact on the rights of individuals. The approaches to addressing online copyright infringement are described. The nature of the policy making process and its impact on how legal measures are perceived are analysed. The potential impact of measures on the rights of subscribers is discussed. A key conclusion is that new measures to combat unauthorised file sharing need not, in principle, adversely affect the balance between rights, but the design and implementation of legal measures do raise concerns in terms of necessity and proportionality.

Keywords
File-sharing; Copyright; Enforcement; Privacy; Freedom of Expression; Due Process

1. Introduction

The Internet has changed and evolved enormously since its beginnings in military and academic communities. However, sharing information has always been a key activity carried out over the Internet and was the main motivation behind the development of the World Wide Web in the late 1980s and early 1990s. Since then, governments have developed public policies and programmes to encourage the development of inclusive information-intensive societies and digital economies. They have also taken an increasing interest in governance on the Internet, that is, in regulating behaviour on the Internet at domestic and international levels rather than how it operates.

With the advent of the World Wide Web and improved connections and bandwidth, the activities and types of users of the Internet have expanded and changed. Many individuals now experience the Internet as consumers. There is also a growing social aspect to Internet activity. The Internet also provides new, often easier, ways of committing established types of unlawful activity, including copyright infringement. The ease with which copyright material can be shared online and the fact that the Internet transcends geopolitical and jurisdictional borders have made it challenging for rights holders to enforce rights.

The actions of governments or inter-governmental organisations have often been helpful in protecting Internet users, for example in the development of data protection and e-commerce regulations in the European Union. However, there is often a need to balance the interests of different stakeholders. This can be difficult to achieve, particularly when there are power imbalances between interested parties or where their respective interests conflict. A current example of this problem is unauthorised sharing of copyright works. As Meyer remarks, "copyright protects while the Internet distributes" [1]. New technologies are used to copy and then disseminate copyrighted content without the authorisation of rights owners. In response, rights owners have used technological protection measures, supported by existing and new legislation to combat the use of technology to infringe copyright. However, this approach has had limited success

Corresponding author:
Adrienne Muir, Department of Information Science, Loughborough University, Loughborough LE11 3TU
a.muir@lboro.ac.uk

as the law is often ignored by large numbers of people and technological measures are by-passed by technically sophisticated Internet users.

Some online activities are clear infringements of copyright with the intention of financial benefit or to avoid acquiring content through legitimate means. However, much activity is more innocent in its intention and is about sharing with others interesting things that someone has seen or heard through linking and other activities. Copyright was initially conceived as a means of providing a balance between the interests of creators and society and this balance is reflected in the limitations placed on terms of protection and the provision of exceptions for activities with no economic significance and in the public interest. Rights owners in the content industries have understandably become increasingly concerned about the perceived levels of unauthorised appropriation or sharing of their content and the resulting interference with the rights holders' ability to exploit and enforce their rights. However, traditional legal remedies to pursue individuals have proved to be inefficient and largely ineffective in curbing such infringing activities. The strategy of pursuing alleged infringers *en masse* is becoming discredited, at least in the UK. Attempts to pursue third parties, such as Internet Service Providers (ISPs), has also had mixed results due to legal protections afforded to service providers under certain circumstances. There has been limited success in enlisting the voluntary cooperation of ISPs in tackling online infringement due to a lack of willingness on the part of some ISPs.

This has led to rights holder pressure on governments to introduce new statutory measures, which will force Internet Service Providers, as the source of the connection to the Internet, to have an active role in enforcing copyright. This approach could include blocking access to sites hosting or facilitating access to infringing material. Some countries have, or are in the process of implementing such measures, which are proving to be controversial amongst third party service providers, civil society and, sometimes, creators. There are several strands of criticism for emerging approaches to dealing with online copyright infringement, not least that existing legislation is sufficient. A related strand is economic in that there is disagreement as to the actual damage caused to the creative industries by online sharing and the potential stifling of digital creativity through strict enforcement of intellectual property rights. Another major basis for criticism is that enforcement of property rights should be balanced against the rights of Internet users. It has been argued that the way the new approaches will be implemented could infringe the right to privacy, damage freedom of speech and be based on a lack of due legal process.

This paper provides a brief introduction to the issue of unauthorised content sharing and how rights holders have attempted to tackle this perceived threat to the content industries and to enforce their rights. This is followed by a generic description of the features of the new statutory approaches being considered or introduced to combat this activity. The UK approach will be used as a case study, but this will be supplemented by reference to approaches in other countries. The UK situation is interesting because although the relevant enabling legislation was passed in 2010, it was still not in force at the beginning of 2012, in part because it had been challenged in the courts. So far, the initial challenge and subsequent appeal have been unsuccessful, except on minor points. However, the legislation will be implemented through a code, which was still in the process of being drawn up at the time of writing. It is likely that the emergence of the code in its final version will give rise to further challenges. Similar legislation already in force in other countries has also been subject to challenge and improvement. Laws in France and New Zealand will be discussed and compared with proposals for the implementation of UK legislation. This paper will assess the likely impact of legislation on the different actors involved, focusing on conflicts with other areas of information policy, including protection of privacy and personal data, freedom of expression and access to information. The discussion is based on UK and European Union law, but legal frameworks, initiatives and cases from other jurisdictions are considered where appropriate. There is also consideration of alternative approaches to reducing unlawful use of copyright content.

2. Content sharing and copyright infringement

Digital content can be shared in various ways, including providing links to content hosted elsewhere and uploading and downloading content to and from a hosting site [2], but peer to peer (P2P) sharing has become a commonly used approach for sharing for both legitimate and illegitimate purposes. P2P software allows users to connect to a sharing network, make files available and discover the existence of files for downloading. Whilst P2P networks are essentially de-centralised, there is still third party involvement, even though these parties are not strictly part of the network. Examples include software developers and file indexing and/or tracking sites. However, this is not the only approach to unauthorised use of copyright material. For example digital hosting and sharing sites may also be used also for illegitimate purposes [3] and a recent prominent case is that of Megaupload Limited, which operated various sites that were closed down by the United States government.

The music industry has been concerned for some time about the economic impact of online copyright infringement. With increasing access to broadband connections, it is also now possible to share larger digital files, such as films. Whilst new artists are making increasing use of the Internet to promote themselves, provide access to their output and build up fan bases [4], many rights holders and their representatives argue that unauthorised file sharing causes economic damage. The nature and extent of the damage is difficult to quantify precisely and the causes of decreases in sales or income for content in different digital forms are disputed. In May 2011, Hargreaves' independent review of intellectual property rights in the UK stated that "Much of the data needed to develop empirical evidence on copyright and designs is privately held. It enters the public domain chiefly in the form of "evidence" supporting the arguments of lobbyists ("lobbynomics") rather than as independently verified research conclusions". The UK's Intellectual Property Office (IPO) also acknowledged the need for evidence in its 2011 IP crime strategy [7]. A freedom of information request to the UK government
t resulted in an admission that the government department involved did not hold any evidence of the damage to the content industries [6]. Danaher *et al's* 2012 review of the literature concluded that academic studies show that piracy has a negative impact on media sales [7]. However, another review of academic studies concluded that there are too many other factors to assume that file-sharing is the sole reason for entertainment industry losses [8].

The methodologies of studies carried out both by industry and other sources have been criticised. However, it is probably safe to conclude that illegal file sharing has become widespread, particularly amongst younger Internet users. In the UK, the Strategic Advisory Board for Intellectual Property (SABIP), commissioned an analysis of consumer behaviour and attitudes in the digital environment [9]. The research concluded that it is easy to find and share digital content and that many people who engage in such behaviour were ignorant of the legal implications. However, others were aware but have developed ethical justifications for their behaviour. Peer pressure is a factor, particularly amongst young people. In 2006, O'Flynn found that dissatisfaction with legal offerings also led to seeking illicit copies [10]. Whether these reasons still hold several years on is not clear but the reluctance of rights holders to become involved in new online enterprises or develop their own has been used as a rationale for unauthorised sharing.

File sharing activities are not necessarily unlawful, for example when individuals voluntarily share their original creations or content or where open licences are used by creators. However, when files are shared without the authorisation of rights holders, it is likely that the file sharers are infringing copyright. Uploading and downloading copies is clearly infringing in UK law if it involves making unauthorised copies [11] of the whole, or substantial parts, of copyright works [12]. It is possible to argue that merely placing lawfully acquired files in a sharing folder is not infringing behaviour, but it is arguably communicating to the public [13], another infringing act. It is possible that certain acts of file sharing could fall under copyright exceptions, for example the copying of literary works for non-commercial research or private study [14] but the purpose of much activity seems to be for entertainment purposes. In some European countries, it is not unlawful to download material (e.g. Switzerland and the Netherlands), but it is still unlawful to upload. Moral rights may also be infringed through removing authorship information from files or manipulating digital content in ways that are perceived as derogatory treatment [15]. Gillen provides an analysis of user liability for P2P sharing activities [16].

3. Rights holders and file sharing

Some creators make use of the Internet to publicise their work and consider giving away content as an incentive for consumers to buy legitimate copies, attend concerts or purchase merchandise. However, industry rights holders and trade groups have taken legal action against services that facilitate file sharing, for example for providing P2P (peer to peer) software or indexing and tracking services [17] [18] [19] [20]. They have also taken action against individual file sharers; some prominent US court cases have resulted in the imposition of large fines for individuals [21] and drawn out appeals processes. These high profile cases do not seem to have had a real deterrent effect, and as the individuals involved are unlikely to be able to pay large amounts of damages, these actions do not provide much compensation for the rights holders. The pursuit of individuals may lead to reputational and professional damage or public protests. For example in the UK, law firms involved in so-called speculative invoicing have attracted negative publicity and and solicitors have been sanctioned by their professional regulatory authorities [22] [23]. Another controversial case involves a UK student facing extradition to the USA for running a website allegedly containing links to infringing material and generating income through advertising [24].

An aspect of rights holder activity that has attracted criticism is how they identify potentially infringing behaviour and infringers. Rights holders have employed automated means to track user behaviour and gather data, such as IP addresses, to be used in conjunction with other data to identify individuals. There has been discussion over whether IP

addresses can be considered to be personal data and whether these activities by rights holders are lawful and the arguments are addressed later in this paper.

ISPs have objected to requests to voluntarily disclose subscriber details without court orders. Rights holders have also sought the cooperation of Internet Service Providers (ISPs) to prevent content sharing. The unwillingness of some ISPs to voluntarily cooperate has led attempts by rights holders to hold ISPs liable for authorising the infringing behaviour of their subscribers. A Belgian case has addressed the issue of whether ISPs should install a system to filter subscriber communications to detect potentially infringing behaviour. The case was finally referred to the EU Court of Justice which ruled that under EU e-commerce law, ISPs could not be compelled to undertake general monitoring of their subscribers [25]. The Court of Justice has also recently made a similar ruling in a case involving the social network Netlog [26]. Rights owners have also wanted ISPs to prevent illegal behaviour by implementing a system of escalating actions against file sharers or to prevent access to certain Internet sites. There has been some cooperation, for example Virgin Media in the UK has attempted to quantify the amount of infringing behaviour amongst its subscribers. The Recording Industry Association of America (RIAA) is making voluntary agreements with US ISPs [27]. The Irish ISP, Eircom, is now cooperating with the Irish Recorded Music Association (IRMA), but only as a result of an out of court settlement after a protracted legal dispute. Otherwise, legal actions have met with mixed success and no clear, consistent approach in judgments.

4. Statutory graduated response approaches to unlawful file-sharing

As court action against file sharers and ISPs is arguably an inefficient, expensive, and ultimately ineffective way for rights holders to protect their rights, some countries have now introduced at least the basis for statutory graduated or "three strikes" approaches. Other countries, such as France and New Zealand, have also taken a statutory approach, which tends to be implemented by amendments to copyright law. Relevant provisions in the UK's Digital Economy Act amend communications law rather than the Copyright, Designs and Patents Act 1998. In the UK, the approach has been adopted as one of the outcomes of the *Digital Britain* report, which set out the UK government's vision for promoting the country's role in the digital economy, including supporting digital industries [28].

Statutory initiatives differ in their detail, but there are some common features:

- identification of suspected infringing behaviour, usually by rights holders, with ISPs matching IP addresses to subscriber accounts
- a limited number of subscriber notifications (sent by the ISP or legal authority rather than the rights holders) of suspected infringements containing escalating warnings as to the potential consequences of their alleged repeated infringements. Further information may be provided to raise awareness, educate about security or alternative, legal sources of digital content
- sanctions imposed on repeat file sharers. These include provisions for ISPs to restrict or suspend accounts in addition to, or possibly as an alternative to, disclosure of personal data to facilitate legal actions by rights holders.

There may also be provision to black list suspended subscribers to prevent them from setting up a new account with a different ISP whilst their existing accounts are suspended.

In the UK, the legislation specifies that practical implementation is to be set out in codes agreed by stakeholders. Identification and notification procedures are to be set out in an Initial Obligation Code and, should it be necessary, sanctions procedures are to be dealt with in a Technical Obligations code. Responsibility for the development of the codes was delegated to Ofcom, the UK's communications regulatory agency. Ofcom duly produced a draft code for consultation in the summer of 2010 [29]. A revised draft code for consultation was published in June 2012. The UK's proposed system is compared to the operational systems in France and New Zealand. What all three systems have in common is that they have been controversial and subject to criticism. The French law was introduced in 2009 after a difficult passage through the Senate, National Assembly and Constitutional Court [30]. The new French President ordered a review of the law in May 2012. The New Zealand system became operational in September 2011, three years after legislation was first passed [31].

4.1. Warning Stage

Under the Digital Economy Act 2010, rights owners will be able to notify ISPs of suspected infringements and, at some point, may be given anonymised reports [32] to allow them to gauge the extent of infringing behaviour associated with particular ISP addresses. The legislation specifies information to be provided by rights holders [33]. There have been

concerns about the standard of evidence of infringing behaviour to be provided and accurate matching of infringements to IP addresses and then to subscriber accounts. These concerns were only partially addressed in the 2010 draft Initial Obligation Code, which did not really expand on what evidence should be provided, but did introduce quality control process for copyright holder and ISP processes and procedures. As there was an element of self-certification, there was also provision for independent audit. However, responses to the 2010 consultation included questioning whether IP addresses can be definitive evidence for the identification of infringers, and rights holder self-certification as to quality control in its data gathering processes [34]. The issue how rights holders gather evidence and what constitutes evidence of infringement in the context of the BitTorrent system arose in an Australian case on ISP liability for subscriber behaviour. In this case, notices of infringements sent to the ISP provided no explanation of how the data was gathered. Therefore it was not reasonable to expect the ISP to take the evidence provided at face value and act upon it. [35]

In addressing these concerns Ofcom makes the point that is constrained in what it can impose on rights owners in terms of robustness of evidence and that rights holders can submit copyright infringement reports when they have evidence that gives *reasonable grounds to believe* infringement has be carried out or authorised by a subscriber. [36] Ofcom also refers to possibility of appeal as an incentive to take all reasonable measures to verify evidence. Rights holders must also submit a description of their evidence gathering procedures for approval to Ofcom on an annual basis and copyright infringement reports may only be submitted using evidence gathered according to approved procedures. Ofcom proposes that a technical standard for evidence gathering is developed by an independent body. Rights holders must publish descriptions of their evidence gathering procedures to ensure transparency. The revisions are certainly an improvement on the initial draft code, but whether they will be acceptable to all stakeholder groups will only become apparent when responses to the consultation are published.

In the UK and New Zealand, rights owners communicate directly with ISPs. This is not the case in France where the warning stage is run by the independent Haute Authorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi). Hadopi has the power to verify the allegations of infringement that it receives before asking ISPs to identify alleged infringers and sending out first warnings. Hadopi received almost 18.5 million reports from rights holders between October 2010 and the end of June 2011 [37], but had sent out 470,935 first warnings. Whether the discrepancy is due to a backlog in processing infringement reports or as a result of investigation of reports by Hadopi is not clear.

Copyright Infringement Reports from rights holders result in warnings sent to the subscribers. Up to three warnings are sent in the UK [38] and New Zealand [39]. The July 2011 voluntary arrangement between six major US ISPs and the film and music industries involves a six strike approach, with punitive actions only coming into play from the fifth warning. Recipients of warnings in the UK may appeal on limited grounds: there was no infringement or the report does not relate to the subscriber's IP address [40]. Responses to the first draft of Ofcom's code questioned the use of the term "appeal", specifically what subscribers would be appealing against, as no ruling, judicial or otherwise, had been made. [41] The Tribunal would be dealing with objections to untested accusations of copyright infringement and there is an assumption of guilt, rather than rights holders having to show that the subscriber infringed. Subscribers would not only have to show that they have not infringed copyright, but that they have secured their connections against use by others to infringe. There were also concerns about the transparency of the membership, operation and review of the Tribunal and recommendations that the Code should be more specific on this. Ofcom disagreed that the burden of proof is with the subscriber and stated that it is for the Tribunal to determine whether the evidence provided is sufficient. Ofcom also made provisions for the Tribunal to publish its procedural rules and guidance on how it will determine what constitutes taking reasonable steps to secure Internet connections for the benefit for accused subscribers. The procedural rules will be subject to approval by Ofcom. Ofcom did not, however, go as far as agreeing to a suggestion to set up a consumer advice body.

4.2. Action Stage

The UK system will work alongside existing remedies for rights holders and data protection law. Rights holders will still need to request court orders to force ISPs to release subscriber details to allow them to take legal actions against repeat infringers. However, arguably the most controversial aspect of the graduated response approach is the possibility that people may have their Internet accounts suspended. ISPs may also be obliged to take technical measures to reduce or suspend connections. However, this would require further regulation and it is likely this course would only be taken if the initial stage were not successful to meeting the government's target for reducing infringement levels. The UK Government did indicate that it did not expect to implement this stage. If it did, there would be another appeal process. The legislation states that the technical code will provide that technical measures will not be started [42] until the

appeal process is complete. However, it also states that the person who determines appeals has the power to require that a measure is not be taken or withdrawn [43]. If measures cannot be implemented until the process is complete, it is not clear how they can be withdrawn. The subscriber must presumably show that there was no infringement or they are not responsible [44]. It should be noted that rights holders will have to pay a fee to issue notifications. Furthermore, the UK government has indicated that it wishes there to be a fee for subscribers to appeal against notifications, to be refunded if the appeal is successful [45].

5. Other approaches to copyright infringement

Another controversial aspect of the UK legislation is that the relevant Secretary of State (not specified in legislation) is given power to make regulations on courts granting blocking injunctions against Internet sites through which infringement may take place [46]. This provision appears to take into account sites that routinely host infringing material, allow downloading of material or point people to other sites that do so. The legislation does point out the importance of freedom of expression, but it is not clear how this would be taken into account. There are various safeguards, including consideration of steps taken to prevent infringement and the provision of legal access to the content by rights holders [47]. Early in 2011, the Government asked Ofcom to review whether the site blocking provision is workable [48] and set up a working group for a voluntary site blocking system. The UK Government has since indicated that it is not currently minded to implement this provision. At the same time, there have been government-sponsored discussions around a voluntary approach to site blocking. It is not clear what such an approach would involve, including on what basis sites would be blocked.

Arguably there is no need to provide statutory provision for site blocking. Courts in various jurisdictions have ordered ISPs to block certain sites. This includes the United Kingdom where BT was ordered to block access to a site hosting infringing content [49] (Newzbin2) under s. 97A of the Copyright, Designs and Patents Act 1998, and more recently five major UK ISPs were ordered to block the Pirate Bay site [50]. Seeking redress through the courts means that rights holders will have to make a clear case for infringement, which requires time and resources. So it would be interesting to see what shape any proposed UK voluntary scheme would take. There is also the question of whether site blocking is actually workable. The Ofcom report on site blocking indicated that blocking measures can be circumvented. A Reuters report on the Spanish "Sinde" law also stated that less than a month after the law came into force, traffic was moving away from sites linking to potentially infringing content and moving to P2P and other types of content sharing services [51].

However, this is still an approach that has been actively considered in other jurisdictions. Particularly controversial examples have been the 2011 US bills, the *PROTECT IP Act* (PIPA) [52] and the *Stop Online Piracy Act* (SOPA) [53]. Criticisms of the blocking proposals in the bills included, that blocks would be applied to domains as a whole, rather than to a particular site. Criticism has been international, as the draft legislation also provided that court orders could be obtained to seize the domain names of foreign sites. Other provisions include removal of sites from search engine results and withdrawal of advertising and financial support to infringing sites. Interestingly, there was also provision for sanctions against rights holders making false accusations of infringement. The bills have been withdrawn for the moment in response to the controversy they provoked, but may re-appear in some form in the future. In the UK, the Government has recently endorsed the withdrawal of advertising and finance from infringing sites in a response to a review of the film industry [54].

Another major development, which has also provoked much controversy, is the Anti-Counterfeiting Trade Agreement (ACTA) [55]. Chapter II of this international Treaty deals with enforcement of intellectual property rights. The stated aim is to harmonise national measures to prevent intellectual property infringement. Supporters argue that the proposed remedies already exist in different jurisdictions. However, the negotiations were largely carried out in private and ACTA only came to public notice through Wikileaks. The negotiations were carried out independently of existing international mechanisms and this lack of transparency has raised suspicions, particularly since civil society was excluded from the process. The reaction to the Treaty has been so strong that it has provoked public demonstrations and some countries have backed away from signing it. Article 27 addresses online infringement and there are concerns that enforcement provisions could interfere with fundamental rights.

For example, the European Data Protection Supervisor has warned about lack of precision of provisions and the potential for invasions of privacy and potential lack of due process and judicial protection [56]. Korff and Brown also drafted a critical opinion on the compatibility of ACTA with the European Charter of Human Rights and the European Convention of Fundamental Rights for the Greens/European Free Alliance in the European Parliament [57]. Korff and Brown's analysis found that ACTA gives disproportionate protection to major rights holders and that human rights are

not given sufficient attention. For example, they argue that ACTA lowers the threshold for criminal infringement without specific safeguards against criminalising trivial non-commercial infringement and the circumvention of digital rights management. Neither does it adequately respect data protection principles in its provisions on gathering and analysing online activities. Korff and Brown feel that ACTA effectively privatises intellectual property law and, further, would erode the rule of law. The EU Trade Commissioner recognised that concerns exist, but in referring ACTA to the European Court of Justice for a ruling on whether it is compatible EU law, he stated that part of the reason was to make sure debate is based on fact rather than misunderstandings. The European Parliament did not wait for a ruling from the ECJ and rejected ACTA in a vote in July 2012 [58], which means that it cannot become law in the EU despite the fact that some EU Member States are signatories. Whilst recognising the problems that ACTA is intended to address, the European Parliament reiterated the view that ACTA is an inappropriate balance between intellectual property rights and the fundamental rights of citizens. The views of MEPs reflected the concerns raised by others that the scope of the agreement is not defined precisely enough and therefore there is a risk of interpretations that could have a negative impact on citizen's rights.

6. Copyright Policy Making: Balancing Intellectual Property and Other Rights

The various initiatives described above are examples of policy makers' efforts to support digital economies and creative industries. Supporting innovation and creativity and the production of intellectual property are key parts of such policies. Having decided that intellectual property rights are an appropriate way to meet policy goals, it is reasonable that the owners of such rights should wish to protect their intellectual property and enforce these rights. Confronted with evidence that this is becoming increasing difficult in the digital environment, it is equally understandable that rights holders would seek solutions to improve the situation and that policy makers to intervene if they feel this is not happening. However, other considerations must also be taken into account. Two themes emerge from an analysis of recent initiatives. These are the manner in which policy is made in democratic societies and implemented and the balance between policy goals such as protecting intellectual property rights and basic human rights of due process, privacy and freedom of expression. Specifically, a key concern is the balance between the legitimate interests of copyright holders to enforce their rights and the rights of the Internet subscribers, including the right to privacy, due process and access to information. There may be unforeseen and unintended consequences to regulation or other arrangements and measures may have a disproportionate impact on fundamental rights. In the UK, two ISPs, BT and TalkTalk, won the right to a judicial review of the anti file sharing parts of the Digital Economy Act 2010. They have their own reasons for being unhappy with the legislation, but part of the challenge was that the legislation breaches EU Directives on data protection and online privacy. At the time of writing, the two attempts to challenge the legislation have largely failed [59]. It is not just ISPs who oppose anti-file sharing legislation. The French Constitutional Court Copyright had rejected parts of the initial Hadopi bill as unconstitutional [60]. A revised Hadopi 2 was passed but now the short life of Hadopi is in some doubt as the Minister for Culture and Communication has reportedly commented on the disproportionate nature of the sanctions and decided to reduce Hadopi's funding while it is under review [61]. Copyright is an area of information policy and law that seems to arouse very strong reactions in different stakeholder groups and it is not always clear where the truth actually lies. It is worth examining the concerns and questions that have been raised to try and gain a better understanding of the potential human rights issues arising from attempts to combat online copyright infringement.

6.1. Transparency and Stakeholder Involvement in Decision Making

Law enforcement in the online world is fraught with difficulties and appropriate and effective governance on the Internet is complicated, particularly given the lack of geo-political boundaries and ease with which efforts at regulation or enforcement can be circumvented. A detailed theoretical discussion of the various modes of governance is beyond the scope of this article, but the multi-stakeholder approach to Internet governance is relevant here. The Working Group on Internet Governance (WGIG) developed the following working definition of Internet governance: "The development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" [62]. The definition implies that all the stakeholders should work together, but it is not entirely clear how much involvement each group should have at different levels of governance as the term *respective roles* is used alongside *shared*. Many of the initiatives discussed in this article are national in scope. However, some are international and/or will have international impact. There are also common complaints against national initiatives. The World Summit on

the Information Society (WSIS) Geneva Declaration of Principles say that the international management of the Internet should be "multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations" [63]. More generally, according to the United Nations (UN) good governance is:

- Consensus Oriented
- Participatory
- Following the rule of law
- Effective and Efficient
- Accountable
- Transparent
- Responsive
- Equitable and Inclusive [64].

These basic principles of good governance reflect Western liberal attitudes, and some States may only recognise the rule of law and perhaps effectiveness and efficiency. However, this is the international standard and the WSIS view on Internet governance is certainly compatible with these principles. Of course, principle and practice are two different things, but there are elements of recent initiatives that, despite wordings and assurances to the contrary, do appear to go against the characteristics of good governance.

Lack of transparency is a recurring complaint about online copyright enforcement measures. A perceived lack of representation and involvement of civil society is most likely a key reason underling public unrest. The perception is that governments are making and implementing policy on the basis of influence of private and economic interests to the detriment of public and social interest. The emerging trend of voluntary agreements between private sector players to enforce copyright is just another manifestation of lack of transparency and due concern for the rights of individuals. For example, there was anger and concern at the speed with which the UK legislation was introduced as it went through the curtailed "wash-up" process just before Parliament was dissolved pending a general election in 2010. A response to this as that the Digital Economy Bill was well-scrutinised on its passage through the House of Lords before being sent to the House of Commons. The perceived lack of meaningful consultation is perhaps reflected in the main criticism of the legislation: that it is ill-considered and unworkable in practice. Lack of precision in drafting is a criticism of the ACTA Treaty as well, as the secrecy surrounding the negotiation and drafting process. Another aspect of balance between rights arose with the US anti-piracy bills, with the concern that the US was using its historical dominance of the domain naming system to control the activities of web sites in other jurisdictions, and the potential security risks to the Internet itself that could arise from interfering on the naming system [65]. In this case, attempts to control behaviour on the Internet could result in interference with governance of the Internet itself.

6.2. Privacy and Data Protection

The right to privacy is articulated in Article 12 of the Universal Declaration of Human Rights (UDHR) [66] and in Article 8 of the European Convention of Human Rights (ECHR) [67]. Article 8(1) of the European Convention on Human Rights refers to respect for private and family life, home and correspondence. The ECHR is implemented in the laws of EU Members States, including the UK's Human Rights Act 1998. Any new legislation, such as the French and British graduated statutory schemes, must be accompanied by a declaration regarding its compatibility with human rights provisions. Methods to detect infringing behaviour can include using technical means to identify the IP addresses associated with potentially unlawful file sharing and monitoring subscriber activities by ISPs. Three strikes systems involve the former. There are doubts as to the accuracy of the results, particularly in the case of dynamic IP addresses where there is no one-to-one relationship between an IP address and a subscriber. A related question is whether IP addresses can be considered to be personal data and whether sniffing out IP addresses potentially raise data protection issues. IP addresses identify machines, rather than people. However, ISPs are able to link IP addresses to subscriber accounts and, therefore, personal data. It can be argued that although the IP address itself does not identify an individual, it can be used in conjunction with data held by ISPs to at least identify the person responsible for the account to which the IP address has been allocated.

Various courts, data protection authorities and commentators have addressed the issue of whether IP addresses are personal data. Moiny's analysis of case law [68] concludes that there is no consistent approach and that IP addresses are sometimes considered to be personal data and sometimes not, depending on the context. However, in the context of

EU data protection law, the Article 29 Working Party[1] Opinion document stated that IP addresses are personal data [69]. If IP addresses can be considered to be personal data, it is necessary to consider whether rights holder activities constitute *lawful* processing of personal data. Data protection regulations differ by jurisdiction, but in EU Member States national legislation gives effect to the EU Data Protection Directive. Data controllers, i.e., those managing personal data, must abide by the data protection principles [70]. If IP addresses can be considered to be personal data, processing would be governed by the Directive. If the data being gathered is considered to be traffic, rather than personal data, the E-Privacy Directive [71] governs this activity.

One contention is that personal data is gathered without the consent of individuals. Arguably, individuals have given consent to the ISPs to do this, depending on the terms of their contracts [72]. ISPs are obliged to process data to meet legal obligations anyway [73]. The individuals have not given consent to the rights holders, but the data gathering could be supported by Art. 7(f) of the Data Protection Directive, if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)" [74]. It would depend on whether the right to privacy trumps copyright law, or the right to enforce copyright is seen as seen as overriding privacy rights [74]. One answer to this question, comes from the Court of Appeal of England and Wales England, which has recently ruled that any processing of personal data by copyright holders would fall under Article 8(2) of the ECHR, as "the processing is plainly necessary for the establishment, exercise or defence of legal claims even if the beneficial consequence of the sending of a notification by the ISP pursuant to a copyright information request will be that in the majority of cases the infringing activity ceases and no further action is required" [75]. The French Constitutional Court ruled that data gathering by rights holders or their agents would be a disproportionate infringement of the right to privacy unless it was done solely for the purpose of legal action for copyright infringement. The Court found that gathering the data and sending it to Hadopi were preliminary activities to legal action and if processing was carried out solely for the purposes of copyright protection then it did not disproportionately infringe the right to privacy [60].

The European Court of Justice has ruled on the question of whether European law requires an obligation on ISPs to disclose personal data to facilitate civil proceedings (for copyright infringement rather than commercial piracy) and found there was neither an obligation to divulge nor to withhold data [76], rather it was a matter for Member States' laws. Under the British and French statutory approaches, ISPs are only obliged to divulge personal details in response to a legal order. Some other Member States have considered the question and found constitutional difficulties with the disclosure of personal data for civil proceedings. For example, courts in Italy and Germany have ruled that ISPs may only disclose subscriber data for the purpose of criminal proceedings [78] [79][2]. In New Zealand law, subscriber data is disclosed to the Tribunal by the ISPs and the Tribunal decides on whether subscribers are to be sanctioned for infringements [80].

Even where data gathering and processing is lawful, there is the question of allegations being made against individuals on the basis that IP addresses are linked to their accounts. It may not be possible to definitively identify an individual as the infringer for various reasons, even if dynamic IP addresses are not used by a subscriber's ISP. For example, another member of the subscriber's household may have carried out infringements or the connection may have been hacked and used without the subscriber's authorisation. The UK proposals acknowledges this possibility, although it is not clear whether the subscriber would always be able to provide evidence to show that they were not responsible for an infringement. In both the French and British three strikes systems, subscribers would not be able to escape liability if they have not secured their connections. Under New Zealand law, the subscriber can only challenge accusations of infringement on two grounds: that no copyright infringement took place, or the infringement did not come from the subscriber's IP address [81]. This suggests that a Tribunal would find a subscriber liable even if their connection was used fraudulently by someone else. Subscribers need to be able to see and challenge data held about them, at least under EU data protection principles. Subscribers are given information about the alleged infringements

[1] The Article 29 Working Party is an advisory body set up under under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] However, the German Federal Court of Justice has more recently ruled that ISPs do have to disclose describer details when requested by copyright owners. Bundesgerichtshof zum Auskunftsanspruch gegen Internet-Provider über Nutzer von IP-Adressen http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=61279&linked=pm&Blank=1 (2012, accessed August 2012).

under three strikes regimes. However, whether innocent subscribers have the requisite knowledge and expertise to challenge the evidence is debatable.

There is some immunity from liability for infringing behaviour carried out by subscribers for ISPs in some jurisdictions, for example under the EU's E-Commerce Directive [82] and the US Safe Harbor provisions [83]. The question of whether ISPs can be forced to routinely monitor what subscribers are doing rather than blocking access to sites voluntarily or when ordered to do so, has already been touched on in this article. At least in the European Union, ISPs cannot be obliged to do this and proactive blanket monitoring would seem to not only a burden on ISPs but also a disproportionate and unnecessary invasion of privacy on behalf of rights holders. In any case, the EU E-Privacy Directive does not sanction disclosure of traffic data for civil proceedings [84].

6.3. Universal Access to Telecommunications Services and Freedom of Expression

The graduated response approach could ultimately result in loss of Internet access for persistent file sharers. The availability of this sanction in the French and (potentially) UK approaches needs to be compatible with recent reforms to EU telecommunications regulations. Graduated response reproaches only apply to Internet access, so subscribers with combined packages of Internet access, television and telephone services should not lose all services. Whilst it is clear that access to the Internet is only to be curtailed in certain circumstances, at least in EU Member States, it is not clear whether access to the Internet is now considered a fundamental human right, either of itself or as part of another right.

Article 10 of the ECHR on freedom of expression includes the right to receive and impart information and ideas. Internet connections are used to communicate and gain access to information, but in most cases they are not the only means to do so at the moment. This may change in the medium to long-term. It looks unlikely that the UK government will press ahead with technical measures at least in the short term, since the warning stage is not yet even in place and the first warning may not be sent out until 2014 at the earliest. At the time of writing, the French system is still at the warnings stage. The proposed voluntary system will involve more warning stages than the typical "three strikes" system. For the sake of argument, implementing technical measures, such as throttling or suspending connections may well have implications for people other than alleged infringers. All members of a community may lose access to Internet connections because of the action of one person. The community may be a household, but it could also be a provider of free wifi, or a library or similar body depending on how these organisations are categorised under the law [85]. It would be ironic if regulations designed to support digital societies or economies have the potential to force the closure of wifi hotspots.

Legal provisions or voluntary arrangements that require ISPs to block access to sources of infringing material, may have an impact of freedom of expression if such sites also host or facilitate access to legitimate material as well. It could be argued that users of locker sites, should have effective backups elsewhere, but such users may wish to use Internet sites to share material and access to this material would be lost. There is also the issue of over-blocking, the online equivalent of using a hammer to crack a nut. Legitimate sites may be shut down alongside any unlawful sites. On the face of it, it seems more difficult to justify this imbalance between protecting copyright and the right to freedom of expression than invasions of privacy to identify individuals who are carrying out infringing acts.

6.4. Due Process

Returning to the nature of the way copyright enforcement regulations are being made, not only does there seem to be a lack of transparency or scant consideration of social as well as economic goals in some instances, another concern is a perceived lack of due process or judicial oversight. Article 6 of the ECHR guarantees the right to a fair trial and presumption of innocence for criminal proceedings, but legal proceedings relating to alleged copyright infringement are often civil matters. Critics claim that actions can be taken against individuals based on allegations of infringement or on a lesser standard of evidence and scrutiny than would be norm under copyright laws in general. In France, sanctions cannot be imposed without going through a judicial process, thanks to the Constitutional Court's scrutiny of the original bill. However, the curtailed process envisaged has caused concern in that it still may not be compatible with the right to due process. In the UK, the detail of the process that might lead to a decision to cut off Internet access has not yet been confirmed but the primary legislation provides that subscribers can appeal against this sanction. However, it is not clear whether subscribers really will be able to fully defend themselves against accusations.

In the EU an amendment to the Common Regulatory Framework Directives introduces a new Internet freedom provision [86], which provides that:

- human rights must be respected

- any measures taken that restrict such rights should be appropriate, proportionate and necessary within a democratic society
- procedures must be fair and impartial and they must respect rights such as the presumption of innocence, the right to be heard, and effective and timely judicial review

The UK law is not yet in force and in France, there is some recourse to judicial authority before Internet connections are cut off. In New Zealand, subscribers can send challenge infringement reports to ISPs, who can forward them the copyright holders. However, they only have one week to submit a challenge and if ISPs and copyright holders reject the challenges, there does not appear to be any recourse to an independent body until the Tribunal or District Court stage [87]. Decisions are expected to be taken on the basis of the paperwork, although it is possible for any party to request a hearing. The arrangements envisaged might disadvantage subscribers because they may have little expertise and little time to make challenges and others cannot represent them at Tribunal hearings.

7. Conclusions

It is possible for rights holders to pursue primary and secondary copyright infringers through the courts already. However, it is neither efficient nor effective in achieving the aim or curtailing mass copyright infringement. Making examples of a few individuals does not seem to have had an impact on the general population, and therefore it is not surprising that rights holders and Governments have chosen to pursue other approaches to the problem. It seems to be widely acknowledged that an awareness and education programme is needed for people who are not hardened file-sharers. It seems reasonable to give illegal file sharers a chance to stop their activities and, incidentally, to make them aware of ways to reduce the risk of becoming victims of wifi hackers. Whilst there are some examples of rights holders and ISPs cooperating to tackle the problem, statutory approaches have the advantage of placing legal obligations on the various stakeholders. It is too early to say whether statutory graduated approaches are effective. Hadopi's annual report does say that by the end of June 2011, Hadopi had sent out 470,935 first warnings and 20,598 second warnings. Whilst this could mean that there has been an impact on file sharing in France, it could also mean that the people who have been warned have found other ways to share their content. This has been acknowledged by Hadopi in its announced plans to widen its activities.

Whilst it is possible to object to the existence of property rights over intellectual and artistic creations on a philosophical basis, they exist. The protection of copyright works is enshrined in law in many jurisdictions and there have been recent attempts to harmonise enforcement provisions, including the international ACTA treaty. If people are indeed using their Internet connections to commit unlawful acts, there is no clear reason why graduated approaches to dealing with the perpetrators should be intrinsically unjust or should unduly interfere with basic human rights. If Internet sites are wholly devoted to copyright infringement, then it does not seem unreasonable to seek to close them down. However, the apparent move towards criminalisation for infringement even when it is not for commercial purposes is chilling.

The issue is how these approaches are developed and implemented, and how the legitimate rights of all affected parties are balanced, and how they are *perceived* to be balanced by civil society. Different parties are bound to feel that their rights should predominate, but a reasonable accommodation has to be found between the extremes. If the balance heavily favours commercial interests, and there are no alternative legitimate sources of content which are attractive to consumers, measures will be resisted. If the design and implementation of enforcement measures are too heavily weighted towards economic efficiency at the expense of due process, then human rights are damaged. All aspects of the statutory graduated approaches in place raise concerns both in terms of copyright law and human rights. There is serious concern over the fairness of the notification, sanction and appeals processes. It is in the best interests of all stakeholders in society that measures aimed at online copyright infringement are proportionate and fair and that adequate checks and balances are present. Whether the sanction is connection termination, site blocking or other measures, there should a careful approach to prevent innocents being caught up in sanctions imposed on the guilty, or the rule of law being effectively circumvented in the interests of private interests. This is why the inclusion of a safeguard against false accusations of infringement in American proposals is interesting as this would help to protect individuals.

Two main justifications have been given for the approaches that have been introduced to support the legitimate interests of rights owners. One is about preventing interference with the commercial exploitation of intellectual property and the other one is to encourage creativity and innovation. It is possible to argue that this state of affairs has come about because of a lack of innovation in business models on the part of the industries, i.e., the industries should

not be waiting until an effective solution is found to unauthorised sharing of digital content. The industries should be exploring how they can meet the needs of their potential customers. If rights owners see their works are cultural commodities, they should be prepared to meet market needs and offer cultural products that consumers want to purchase. Apart from the criticism of three strikes approaches on the grounds of fairness and effectiveness, there is also the issue of cost. The French Culture Minister has recently complained that the cost of Hadopi is not justified and that it has failed to sufficiently encourage the development of legal content. Rights holders can argue that the perceived value of intangible goods could be altered through education. However, it could also be through embracing the technologies and network services used by the market and making the pricing and payment mechanisms more attractive to potential customers. It has to be through finding ways to adapt to the way the market wishes to consume copyright works. Where intellectual property is a valuable economic commodity, it is likely that the desire to control its exploitation will remain strong. Developing measures to enforce copyright that are not wholly compatible with citizen's rights is, at least, ethically questionable and may not be successful in the longer term. There are alternative approaches that could at least be explored, including levies on storage devices or ISP fees, although these approaches also raise ethical questions. Allowing purely non-commercial sharing and making it easier to use legitimate sources of copyright material is perhaps currently a step too far for rights holders, but it might be a better long-term approach than further alienating consumers through laws that they perceive as unfair and disproportionate.

References

[1] Meyer, T. Graduated response in France: the clash of copyright and the Internet. *Journal of Information Policy* 2012; 2: 107-127.
[2] See Smith, D and Taylor, M. File sharing: modern developments. *Computer and Telecommunications Law Review* 2010; 16: 176-177 for an accessible introduction to modern file-sharing technologies.
[3] For a recent overview of the usage of prominent file hosting services see Mahanti, A *et al*. Characterizing the file hosting ecosystem: a view from the edge. *Performance Evaluation* 2011; 68: 1085-1102.
[4] For example see Corporate Records (http://corporaterecords.co.uk/whycorporate), which allows artists to retain control of how they market themselves and their material and to retain 80% of the price paid by customers.
[5] Hargreaves, I. *Digital opportunity: a review of intellectual property and growth: an independent report*, p. 18, http://www.ipo.gov.uk/ipreview-finalreport.pdf (2011, accessed August 2012).
[6] Intellectual Property Office. *Prevention and cure: the UK IP crime strategy 2011*. Newport: IPO http://www.ipo.gov.uk/ipcrimestrategy2011.pdf, (2011, accessed March 2012).
[7] Danaher, B. *et al*. *The effect of graduated response anti-piracy laws on music sales: evidence from an event study in France*, p. p. 5, http://dx.doi.org/10.2139/ssrn.1989240 (2012, accessed July 2012).
[8] Open Rights Group. *Evidence please*, http://www.openrightsgroup.org/blog/2011/the-need-for-evidence (2011, accessed March 2012).
[8] Wilson, D. *What filesharing studies really say – conclusions and links*, http://www.zeropaid.com/news/100921/what-filesharing-studies-really-say-conclusions-and-links/ (2012, accessed August 2012).
[9] Hunt, R, *et al*. *Copycats? Digital consumers in the online age.* London: SABIP, 2009.
[10] O'Flynn, T. File sharing: a holistic approach to the problem. *Entertainment Law Review* 2006; 17: 219-222.
[11] *Copyright, Designs and Patents Act* 1988, ch. 48, s. 17.
[12] *Copyright, Designs and Patents Act* 1988, ch. 48, s. 16(3).
[13] *Copyright, Designs and Patents Act* 1988, ch. 48, s. 20(2)(b).
[14] *Copyright, Designs and Patents Act* 1988, ch. 48, s. 29
[15] *Copyright, Designs and Patents Act* 1988, ch. 48, ss. 77 & 80.
[16] Gillen, M. File-sharing and individual civil liberty in the United Kingdom: a question of substantial abuse? *Entertainment Law Review 2006*; 17: 7-14.
[17] *A&M Records v. Napster, Inc*. 239 F. 3d 1004.
[18] *Metro-Goldwyn-Meyer Studios, Inc., et al. v. Grokster, Ltd, et al*. 545 U.S. 913.
[19] *Universal Music Australia Pty Ltd v. Sharman License Holdings Ltd (Sharman)* [2005] F.C.A. 1242.
[20] *Public Prosecutor v. Neil* Unreported April 17 (2009 (TR(Swe)).
[21] For example, *Capitol Records, Inc. v. Thomas*, 579 F.Supp.2d 1210(D. Minn. 2008) and *Sony BMG Music Entertainment v. Tenenbaum* Unreported July 14 (2009 (D (US)).
[22] *Solicitors Disciplinary Tribunal and Brian Laurence Miller and David Joel Gore* (10619-10)

[23] *Solicitors Disciplinary Tribunal and Andrew Jonathan Crossley* (10726-11).
[24] Challis, B. 'May rubber stamps student's extradition'. *1709 Blog* *http://the1709blog.blogspot.co.uk/2012/03/may-rubber-stamps-students-extradition.html, (2012, accessed March 2012).*
[25] *Scarlet Extended SA v Societé Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM)* (C-70/10) [2012] E.C.D.R. 4
[26] *Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) v Netlog NV*(C-360/10).
[27] See http://www.riaa.com/faq.php.
[28] *Digital Britain Final Report* CM7650. London: BIS & DCMS, 2009.
[29] Ofcom. *Online infringement of copyright and the Digital Economy Act 2010: draft initial obligations code*. Ofcom, 2010.
[30] *Loi no 2009-669 du juin 2009 favorisant la diffusion et la protection de la creation sur internet* NOR: MCCX0811238L.
[31] *Copyright (New Technologies) Amendment Act 2008* and *Copyright (Infringing File Sharing) Amendment Amendment Act 2011*.
[32] *Communications Act 2003*, ch. 21, ss. 124K, as inserted by the *Digital Economy Act 2010*, ch. 24, s. 13.
[33] *Communications Act 2003*, ch. 21, ss. 124A3, as inserted by the *Digital Economy Act 2010*, c. 24, s. 3.
[34] Ofcom. *Online Infringement of Copyright and the Digital Economy Act 2010:* notice of Ofcom's proposal to make by order a code for regulating the initial obligations, p. 38. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf (2012, accessed August 2012).
[35] *Roadshow Films Pty Ltd & Ors v iiNet Ltd* [2011] FCAFC 23 & [2012] HCA 16.
[36] Ofcom. *Online Infringement of Copyright and the Digital Economy Act 2010:* notice of Ofcom's proposal to make by order a code for regulating the initial obligations, p. 44.
[37] Hadopi. *Rapport d'activité 2010*. Hadopi, 2011, p.43.
[38] *Communications Act 2003*, ch. 21, ss. 124K, as inserted by the *Digital Economy Act 2010*, ch. 24s. 13.
[39] *Copyright (Infringing File Sharing) Amendment Bill*, 119-1, s. 7.
[40] *Digital Economy Act 2010*, ch. 24, s. 13.
[41] Ofcom. *Online Infringement of Copyright and the Digital Economy Act 2010:* notice of Ofcom's proposal to make by order a code for regulating the initial obligations, p. 68. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf (2012, accessed August 2012).
[42] *Communications Act 2003*, ch. 21, ss. 124K(11), as inserted by the Digital Economy Act 2010, ch. 24, s. 13.
[43] *Communications Act 2003*, ch. 21, ss. 124K(9)(a)(2), as inserted by the *Digital Economy Act 2010*, ch. 24, s. 13.
[44] *Communications Act 2003*, ch. 21, ss. 124K(5) & (6), as inserted by the *Digital Economy Act 2010*, ch. 24, s. 13.
[45] Department for Culture, Media and Sport. *Next steps for implementation of the Digital Economy Act*. DCMS, 2011. http://www.culture.gov.uk/images/publications/Next-steps-for-implementation-of-the-Digital-Economy-Act.pdf (2011, accessed March 2012).
[46] *Digital Economy Act 2010*, ch. 24, s. 17.
[47] *Digital Economy Act 2010*, ch. 24, s. 17(5).
[48] Ofcom. *Site blocking'to reduce online copyright infringement: a review of sections 17 and 18 of the Digital Economy Act* http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf (2011, accessed March 2012).
[49] *Twentieth Century Fox Film Corporation & Ors v British Telecommunications Plc* [2011] EWHC 2714 (Ch) (26 October 2011).
[50] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 26 (CH) and [2012] EWHC 1152 (CH).
[51] *Spain's anti-piracy law may already be obsolete* http://www.reuters.com/article/2012/03/26/net-us-spain-piracy-idUSBRE82P0JV20120326 (2011, accessed March 2012).
[52] *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011* S.968.
[53] *Stop Online Piracy Act* H.R. 2361.
[54] Department for Culture, Media and Sport. *The Government's response to "A Future For British Film: it begins with the audience..."* CM8355 http://www.official-documents.gov.uk/document/cm83/8355/8355.pdf (2012, accessed May 2012).

[55] Anti-Counterfeiting Trade Agreement http://www.international.gc.ca/trade-agreements-accords-commerciaux/assets/pdfs/acta-crc_apr15-2011_eng.pdf (2011, accessed May 2012).
[56] *European Data Protection Superviser. Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America* www.edps.europa.eu/.../site/.../Opinions/.../12-04-24_ACTA_EN.pdf (2012, accessed May 2012).
[57] Korff, D. and Brown, I. *Opinion on the compatibility of the Anti-Counterfeiting Trade Agreement (ACTA) with the European Convention on Human Rights & the EU Charter of Fundamental Rights*. http://rfc.act-on-acta.eu/fundamental-rights (2011, accessed August 2012).
[58] *European Parliament legislative resolution of 4 July 2012 on the draft Council decision on the conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America (12195/2011 – C7-0027/2012 – 2011/0167(NLE))* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0287&language=EN&ring=A7-2012-0204 (2012, accessed August 2012).
[59] Most recently *R. (on the application of British Telecommunications Plc) v Secretary of State for Business, Innovation and Skills Court of Appeal (Civil Division*) [2012] EWCA Civ 232.
[60] *Décision n° 2009-580 DC du 10 juin 2009 Loi favorisant la diffusion et la protection de la création sur internet* http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html (2009, accessed August 2012).
[61] Manenti, B. Aurélie Filippetti: "Je vais réduire les credits de l"Hadopi". *The Nouvel Observateur* 2012; 1 August (2012, accessed August 2012).
[62] Working Group on Internet Governance. Report from the Working Group on Internet http://www.itu.int/wsis/docs2/pc3/html/off5/index.html (2005, accessed May 2012).
[63] World Summit on the Information Society. Declaration of principles. http://www.itu.int/wsis/docs/geneva/official/dop.html (2003, accessed May 2012).
[64] United Nations. What is good governance? http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/gg/governance.asp (2012, accessed May 2012).
[65] Internet Society. Internet Society Board of Trustees Expresses Concern over Online Copyright Enforcement Strategies (2012, accessed May 2012).
[66] Universal Declaration of Human Rights (UDHR) http://www.un.org/en/documents/udhr/ (accessed May 2012).
[67] European Convention of Human Rights.
[68] Moiny, J-P. Are Internet protocol addresses personal data? The fight against online copyright infringement. *Computer Law & Security Review* 2011; 27: 348-361.
[69] *The Article 29 Working Party Opinion 4/2007 on the concept of personal data* 01248/07/EN WP 136.
[70] *Directive 95/46 On the protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' Official Journal of the European Union L, 281 (23/11/1995)*, Art. 6. Articles 2(a) and (b) define the term personal data.
[71] *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* L201, 2002-07-31, pp. 37 – 47.
[72] *Directive 95/46 On the protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' Official Journal of the European Union L, 281 (23/11/1995)*, Art. 7(b).
[73] *Directive 95/46 On the protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' Official Journal of the European Union L, 281 (23/11/1995)*, Art. 7(c)
[74] The *European Convention on Human Rights*, Art. 8(2) provides that the right to privacy could be overridden to protect the rights of others or the economic well being of a country.
[75] For example see Smith, J and Brimstead, K, European Community: copyright – data privacy does not trump copyright protection. *European Intellectual Property Review* 2008; 30(6); 39-40 and Vincents, O.B. When rights clash online: the tracking of P2P copyright infringements vs. The EC Personal Data Directive. *International Journal of Law and Information Technology* 2007; 16(3): 270-296.
[76] *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB* C461/10.

[77] *R (British Telecommunications Plc) v BPI (British Recorded Music Industry) Ltd and others* [2012] EWCA Civ 232, 6 March 2012.
[78] Suprema Corte di Cassazione, III Sezione penale, Sentenza 9 gennaio 2007, n. 149.
[79] Bundesverfassungsgericht, 11 March 2008, BVerfG, 1 BvR 256/07 and Bundesverfassungsgericht, 2 March 2010, BVerfG, 1 BvR 256/08.
[80] Copyright (Infringing File Sharing) Amendment Amendment Act 2011, s. 122J(3).
[81] Copyright (Infringing File Sharing) Amendment Amendment Act 2011, s. 122O(1).
[82] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). *Official Journal* L 178, 17.7.2000, 1–16.
[83] 17 USC § 512 *Limitations on liability relating to material online*.
[84] Directive 2002/58 on Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Official Journal of the European Union L, 201 (31/7/2002), Art. 15(1), p. 46.
[85] Ofcom in its 2010 *Online Infringement of Copyright and the Digital Economy Act 2010: draft initial obligations code,* made an attempt to clarify the status of such entities. Only the largest, fixed network operators will initially qualify as ISPs, though the Act permits the inclusion of all ISPs within its remit. Due to the lack of precision in the drafting of the Act, providers of freely accessible Wifi connections may qualify as subscribers, and if so, will have to find ways to prevent the connections being used for infringements and require some sort of registration to identify third party infringers.
[86] European Commission. *European Parliament Approves EU Telecoms Reform but Adds 1 Amendment: Commission Reaction* MEMO/09/219 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/219 (2009, accessed May 2012).
[87] Copyright (Infringing File Sharing) Amendment Amendment Act 2011.

