ROLE AND RESPONSIBILITY OF INTERNET INTERMEDIARIES IN THE FIELD OF COPYRIGHT AND RELATED RIGHTS

prepared by
Lilian Edwards, Professor of E-Governance, University of Strathclyde

I. OUTLINE AND INTRODUCTION TO PROBLEM

This report is divided into eleven sections.

Sections I and II look at the historical background to the development of regimes of immunity, limited liability or "safe harbor" for online intermediaries, from the early days of the commercial Internet, drawing on the report prepared for WIPO in 2005 by Edwards and Waelde. Early pressures on Internet service providers (ISPs) and hosts who feared being held responsible for multiple types of unwelcome content authored by third parties (including not just copyright infringing material but also illegal and harmful material such as pornography, hate speech and defamatory content) led to the promulgation of the two main global models, the EC Electronic Commerce Directive (ECD), and the US Digital Millennium Copyright Act (DMCA). These instituted a bright line, with some caveats, of no liability for intermediaries unless they received actual notice or became aware of facts or circumstances indicating illegal content or activity. This led to general voluntary participation by intermediaries in notice and take down (NTD) even where not mandated by law. In this model, prior monitoring was not expected of intermediaries.

Sections III and IV look at the global scene and the leading US and EU regimes in more detail, in particular noting the problems remaining with NTD paradigms in relation to potential chilling of free speech due to lack of public oversight of possible wrongful demands for take down of content; and the unhelpful uncertainty as to the extent of immunities for new linking intermediaries such as search engines.

Section V looks at the economic and technical developments in peer to peer (P2P) filesharing which lead to IP rightsholders looking beyond NTD for protection from the downturn in industry revenues, and turning towards suing P2P intermediaries such as torrent sites which enabled users to share files without permission, and to suing users themselves in volume litigation. In particular, different generations of P2P technologies are separately described.

Section VI discusses the jurisprudence which has developed over the last decade in lawsuits against P2P intermediaries such as Napster, Grokster et al, and concludes that although there have been legal victories in this domain; they have been somewhat Pyrrhic, with filesharing relatively undaunted. Lawsuits against users have similarly turned out to be counter productive, paving the way for new approaches in the form of "graduated response".

Section VII examines the various global models for graduated response, focusing in particular on laws passed in the UK, France, South Korea and elsewhere, and lawsuits imposing such a regime on users in Ireland. To found a discussion of the impact on human rights, a summary is given of the technical methods used by private P2P investigation agencies to identify file sharers using systems such as Dtecnet, Audible Magic's Copysense and Global File Registry. "Notice and notice" and "notice and disconnection" (or suspension) are both analyzed. A detailed analysis is given of both the advantages asserted for graduated response by the content industries, including speed, cheapness, effectiveness and educational value, and the problems so far identified with graduated response as respects users, rightholders, intermediaries and the public interest. These problems include impacts on due process, possibilities of error, impact on fundamental rights of privacy, freedom of speech and access to the Internet and "unintended consequences" e.g. impact on those supplying free open wireless access to the Internet.

This section also canvasses whether graduated response may breach the pre-existing regimes of intermediary immunities noted in sections III and IV as well as other existing laws such as EU data protection laws. Finally, it attempts to outline a framework for deciding when or whether graduated response regimes can be proportional to reducing the harms caused by unlawful filesharing.

Section VIII looks further at the solutions of content filtering or website blocking which are sometimes seen as part of graduated response. Global jurisprudence and laws are surveyed and some problems with filtering highlighted which also affect the general proportionality assessment of graduated response.

Section IX recognizes that some hosts such as video streaming sites or cloud storage sites have also become identified by content industries as part of the copyright infringement problem, and addresses recent significant case law in both the US and EU as to whether the "traditional" immunity regimes described in sections II and III should continue to apply to these sites, and on what terms. In particular, the fight over whether intermediaries are required to move from mere duties of NTD to prior filtering is examined in the context of the US *YouTube* and EC *eBay*, *Google Adwords and SABAM* cases.

Section X looks at what new business models have developed to enable monetization of digital music services, and what voluntary initiatives are being undertaken by the ISP and host industries to prevent unlawful filesharing.

Section XI attempts to draw some lessons learned from the above and to outline some possible research questions and issues for the future.

II. INTRODUCTION: THEMES AND ISSUES

Internet content is distributed, hosted and located by online intermediaries, whose part in the entire enterprise of the information society is thus vital. Content or services often carry with them legal liability, which may be civil or criminal e.g. obscene, defamatory, racist content. Most saliently, for the purposes of this report, it may infringe the copyright of the rightsholder, if the host, publisher, reader or listener has made an unauthorized copy or breached other recognized rights under copyright law. It is important throughout this report however to keep in mind that the issue of how to regulate the liability of online intermediaries for copyright infringement has to be situated in the wider debate around their liability for other types of illegal or actionable activity or content.

Online intermediary liability has become increasingly controversial in relation to copyright material as a result of two key developments: the rise in unauthorized downloading of digital music, film and video since the beginning of the P2P revolution; and the arrival of "Web 2.0" interactive user generated or mediated content (UGC or UMC – see section IX) sites such as eBay, YouTube, Facebook, etc. Both of these phenomena will be explored in depth below.

Historical development and general background to policy issues

The problem of the liability of Internet intermediaries for content authored by, or activities carried out by, third parties – known at first as the issue of "ISP liability", but now of considerably wider scope – was one of the earliest problems in the cyberspace

environment to worry the emerging Internet industry and demand the serious attention of lawyers[1]. Early cases mainly originated in the United States and focused on the liability of the first ISPs such as AOL or CompuServe for hosting, transmitting, or publishing material that was in some way criminally or civilly actionable: notably libelous, defamatory or pornographic content. A few early cases dealt with liability of ISPs for hosting copyright infringing works e.g. texts of the Church of Scientology.

The different policy issues raised by different classifications of authorship, responsibility and editorial control across different types of content were largely not teased out systematically in the early jurisprudence, leading to widely differing regimes being imposed both across different legal systems, and within the same legal system but in differing scenarios depending often on what analogy was selected e.g. "publisher," "newsstand," "common carrier".

From the mid 1990s, this lack of harmonization in the emerging case law lead to calls from industry for some form of rescuing certainty in the form of special statutory regimes giving immunity from liability – or in US terminology, "safe harbors". In Europe, the liability regime debate came to be seen less as tied to different types of content—libel, pornography, material infringing copyright—and more as a holistic problem of whether intermediaries on the Internet should in general be made responsible for the content they made accessible to the public, and more importantly, whether they could in practice take any steps to deal with such responsibility and avoid risk. In the US, however, as we shall see below special rules did evolve for different types of content. Both the EU and US models have since become global model regimes in this area (section IV below).

At the same time, the issue of liability for content became a major worry not just for the relatively small traditional ISP community, but also for a wider spectrum of Internet hosts, e.g., universities, traditional media organizations going 'digital' (e.g. the BBC, the Times), software providers such as Microsoft or Sun, libraries and archives, chatrooms and 'weblog' sites, individuals setting up personal Web 'home pages' and the emerging social networking sites —and also affected a wider range of Internet communications intermediaries than traditional ISPs, such as Internet backbone providers, cable companies, and mobile phone communications providers.

The early sharp distinction drawn between Internet Access Providers (IAPs) - who merely provided 'fundamental communications services such as access, information storage etc,' and ISPs, who provided 'some additional service which facilitates a transaction between end users, e.g. identifying one of the parties, providing search facilities etc'[2] became less and less meaningful as the ISP sector expanded during the boom years of the Internet to provide portal services giving access to large amounts of both in-house and third party produced content. Simultaneously, providers of what might be seen as 'pure' telecommunications services, like mobile phone companies, also became deeply involved in both the 'content business' and in providing 'value added' services such as locational data handling. The scene was further muddied more recently by the arrival of novel and important online intermediaries such as notably, search engines, auction sites,

[1] *Cubby v CompuServe* 766 F Supp 135 (SDNY, 1991), for example was one of the earliest cyberlaw cases of any kind to be decided, in 1991, and concerned ISP liability for a user's libel hosted on a CompuServe forum. A Dutch prosecution of an ISP for hosting copyright material was also reported in 1991, see DTL Oosterbaan, *et al*, 'eCommerce 2003: Netherlands' in *Getting the Deal Through: eCommerce 2003 in 25 Jurisdictions Worldwide* (Law Business Research Ltd, 2003).

[2] C Reed, *Internet Law: Text and Materials* (Butterworths, 2000) ch 4, p 78.

aggregators and comparison sites, and the mature social networking sites. All this had important implications for the development of an online intermediary liability regime which was practical, uniform, acceptable to industry and yet protective of both consumer and citizen needs.

Policy factors and the development of the "limited liability" paradigm

The ISP's and host's case for immunity from content liability around the world, which heavily informed the development of limited liability regimes such as the US copyright statute, DMCA and ECD arts 12 to 15, rested mainly at the time on three factors:

1. lack of effective legal or actual control;
2. the inequity of imposing liability upon a mere intermediary ("shooting the messenger"), and;
3. in Europe especially, consequences for the public interest if unlimited liability was, nonetheless, imposed.

1. *Factual impracticality and legal restraints.* On the first point, ISPs argued that they could not manually check the legality of all the material which passed through their server, without impossible amounts of delay and expense, nor was it desirable, or possibly legal, for them to do so without invading the privacy and confidentiality of their subscribers[3]. Their aim was thus ideally legally to be classified not as publishers who carried the risk of the content they made available to the public but as common carriers, akin to the postal service and phone companies in the US, i.e. institutions which carry no liability for content carried but do owe duties of confidentiality[4].
In the 2000 turning point of the *France vs. Yahoo!* case, however, the French court, presented with the defense that it was technically impossible for Yahoo! US to block access to 'all persons from France' to pages on its site selling Nazi memorabilia items, passed on the question of whether automated filtering of requests from a particular *location was feasible,* to a technical sub-committee to investigate. They reported back that, in fact, Yahoo! had the capacity (already used to serve up adverts in the relevant language to users from whatever country of origin) to identify and thus block access to 90% of French citizens.[5] Accordingly, Yahoo! was instructed to block access. This decision was unusual in some senses in that it related to location-based rather than content-based blocking (since Yahoo! already manually classified the *types* of items for sale on its site). However, in cases of pure automated content classification, the view widely held was that online intermediaries could not yet successfully automate the filtering of unwanted material and remain in business. Furthermore, contrary to conventional

[3] BT Internet estimated in 1999 that just to effectively monitor news-group traffic alone, they would have to hire 1500 new employees working 24 hours a day. See *WIPO Workshop on Service Provider Liability*, Geneva, 9 and 10 December 1999, paper by Janet Henderson, Rights Strategy Manager, BT Internet. One's mind boggles to think what the figure would be today.
[4] In fact the US courts took a middle way in two early decisions. See discussions in *Cubby v CompuServe* 766 F Supp 135 (SDNY, 1991) and *Stratton Oakmont Inc v Prodigy Services* LEXIS 229 (NY Sup Ct, Nassau Co., 1995). The former held in US law that the early ISP fitted best into the model of distributor rather than a carrier; the latter that an ISP which took some editorial decisions might nonetheless still be classed as a publisher with full liability for content published.
[5] See *LICRA et UEJF vs Yahoo! Inc and Yahoo France,* (20 November 2000, Tribunal de Grande Instance de Paris, Superior Court of Paris) p14.

publishers, ISPs and hosts were exposed to risk as a result of content authored by parties with whom they often had no contractual relationship.[6]

2. *Equity.* Secondly, ISPs argued that they were mere messengers and not content providers, and thus that it would be inequitable to hold them liable.[7] The model typically contemplated at the time was probably that of a subscriber, business or domestic, who used his ISP, or an online host like Geocities or Hotmail, to store his web pages, documents or emails; perhaps also of a university or school where large numbers of students stored files on central servers for free. In such a scenario, the host is easy to see as both morally "innocent" and factually devoid of actual or constructive knowledge of illegal or unwelcome content, unless specific notice is given. This perception of ISPs and hosts as "innocent" was however combated early on by the music and audiovisual industries, whose business model was already under threat by 2000 from online piracy. In particular, the former President of the Motion Picture Industry Association of America, Jack Valenti, successfully headed an initiative against ISPs in the hearings prior to the passing of the US DMCA to prevent them being granted total immunity in respect of downloadable infringing content[8].

3. Unwanted economic consequences. Finally the ISP industry argued that their emergent business could not withstand the burden of full liability for content authored by others. Since the promotion of e-commerce and the information society depended on a reliable and expanding Internet infrastructure, an immunity regime was in the public interest. Without it, the ISP industry might be rendered uneconomic. In Europe this argument was even stronger as the US online industry already had a head start, and it was feared unlimited liability on EC online intermediaries would encourage them to migrate to more sympathetic jurisdictions.

Against these pleas, however, was the strong state interest in ISPs, as the only effective gatekeepers, taking up the role of 'cleaning up the Internet', *i.e.*, ridding it of pornography, spam, libel and other forms of undesirable content. This was also, somewhat later, the role sought for ISPs by the content industries.

By the year 2000 or so, arguably a rough compromise had emerged in both Europe and the United States among the various stakeholders. ISPs should in principle be guaranteed freedom from liability for content authored by third parties, *so long as* they were prepared to cooperate when asked to remove or block access to identified illegal or infringing content. Such an immunity or "safe harbor," was implemented in Europe in the ECD, and in the United States, in the 1998 DMCA (as respects copyright infringing material only). These regimes were to prove of critical importance in allowing the growth of the innovation, e-commerce and fledgling user generated content (UGC) industries.

---

[6] Conventional publishers, such as newspapers or book publishers could limit their risk contractually, by, for example, issuing acceptability guidelines to its employees, or putting indemnity clauses into contracts with freelancers.

[7] See adoption of this metaphor in G Sutter, 'Don't Shoot the Messenger? The UK and Online Intermediary Liability' (2003) 17 *Intl Rev L, Computers and Technology* 73.

[8] See in particular On-Line Copyright Liability Limitation Act and WIPO Copyright Treaties Implementation Act: Hearing on HR 2280 and HR 2281 Before the House Judiciary Committee, Courts and Intellectual Property Subcommittee, 105th Cong (1997) (statement of Jack Valenti, President, Motion Picture Industry Association of America). Famously Valenti described downloading as the ISP industry's "dirty little secret", claiming that around 80% of ISP bandwidth was devoted to P2P traffic.

III. GLOBAL REGIMES OF "SAFE HARBORS" OR ISP/INTERMEDIARY IMMUNITIES

Model legal frameworks for Internet intermediaries have thus developed taking two different approaches: (i) "horizontal" regulation that deals with the liability of intermediaries across all types of content, such as the ECD, or (ii) "vertical" regulation which lays down rules for special domains (copyright, protection of children, personal data, counterfeiting, domain names, online gambling, etc). Examples of the latter include the US Internet gambling law, the UK Defamation Act 1996, S 1, the US DMCA and the French '*Code monétaire et financier*' for online fraud with a payment card.

USA: In the US, two separate regimes of immunities were created for ISPs and hosts, one relating to all types of liability material except for intellectual property (IP) and the other relating to liability for material infringing copyright. The first regime is found in s 230(c) of the Communications Decency Act (CDA) which provides total immunity in respect of all kinds of liability bar that relating to IP[9], so long as the content in question was provided by a party other than the service provider. The second regime, found in the DMCA, Title 512, exempts online intermediaries of various types from liability in relation to copyright infringement by means of a set of "safe harbors," but only on certain terms, such as the disclosure of the identity of infringers on request, subscription to a detailed code of practice relating to notice, 'take-down' and 'put-back', and the banning of identified repeat infringers from access. The regime is described in detail below.

EU: In Europe, a harmonized "horizontal" regime exists in the ECD, covering liability for all kinds of content, except gambling and privacy/data protection, which are exempted. The ECD regime is described in detail below, but it should be noted that the Commission is currently consulting on reform of the Directive including arts 12 to 15[10].

The global scene: Similar rules are found in many other developed and emergent economy countries. In some countries, following the US model, the rules on intermediary immunity for infringing material are dealt with separately from other types of content liability. China, for example, in its Regulation on Protection of the Right to Network Dissemination of Information of 2006, exempts "network service providers", including search and linking providers, from liability for hosting IP infringing material on certain terms, similar to those of the US DMCA[11]. The Republic of Korea regulates liability of online intermediaries copyright under the Korean laws 'Act on Promotion of Information and Communications Network Utilization and Information Protection(…)', as amended in 2002, and the Korean 'Copyright Act of April 2009,' under which "online service providers" are exempted from liability provided they take down illegal content on notice if it is deemed to be harmful or copyright infringing. Online intermediaries may post a response if they disagree with the notification.

India, however, has a generic regime more along the lines of the ECD model. It introduced "for the avoidance of doubt" a wide provision in its IT Act 2000 that "no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him

---

[9] See detailed discussion of the very wide scope of this immunity in Lemley M "Rationalizing Safe Harbors" [2007] 6 J. On Telecomms and High Tech L 101, at 102-105.

[10] See Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), closed November 5 2010, at http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

[11] See http://www.chinaitlaw.org/?p1=print&p2=060717003346.

if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention". This mainly related to the cybercrime offences created by the Act. The IT Amendment Act 2008 refined the section to correspond more closely to the DMCA/ECD model of near-total immunity for mere conduits and notice and take down for hosts.

Many developing countries still have no rules but tend to regard the DMCA and ECD as potential models.

IV. THE LEADING MODEL REGIMES

A. The European E-Commerce Directive (ECD)

ISSPs – definition

Articles 12 to 15 of the ECD introduced throughout Europe a harmonized regime on the liability of online intermediaries[12]. The regime affects 'ISSPs': *i.e.*, 'information society services providers' or, as the title of Section 4 of the ECD also calls them, 'intermediary service providers'[13]. An 'information society service' is defined as 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service[14]. 'Recipient of a service' is defined as 'any natural or legal person who uses an information society service'.

Thus, broadly, the ECD intermediary service provider liability regime covers not only the traditional ISP sector, but also a much wider range of actors including hosting services, e-commerce merchants, social network sites, cloud computing services, mobile providers, etc. There are a number of key exceptions to what can be defined as an ISSP. First, since an information society service must be offered 'at the individual request of the recipient', TV and radio broadcasters do not fall within the remit of the ECD liability regime, although sites which offer individually on-demand services such as video-on-demand or email are included[15].

Secondly, there is the issue that the ISSP must provide a service "normally provided for remuneration". Recital 18 of the ECD notes explicitly that although a service may be free to the recipient, the provider of that service may still be an ISSP if the service broadly forms part of an 'economic activity': so, arguably, this can include providers of non-commercial services on-line, such as the delivery of e-government services by state departments, if the state will be making economic gains out of the activity (*e.g.*, if they are cutting costs by putting service delivery on line). Given that one of the dominant successful models of e-business is to give away a product or service but then make money out of it in lateral ways, most notably in the search engine and social networking markets, it would not make sense for the ECD definition of an ISSP to be interpreted

---

[12] 2000/31/EC, passed 8 June 2000.
[13] Art 2(b), ECD. These providers can be natural or juristic persons.
[14] Art 2(a) of the ECD refers back to the definition in Art 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The definition is discussed further in Recs 17 and 18 of the ECD. In particular spammers and other 'providers of commercial communications' are included as providers of information society services. Art 2(d), ECD.
[15] See further Rec 18, ECD.

restrictively.[16] The European Court of Justice (ECJ) has now given guidance that the Google "Adwords" referencing service falls, under certain conditions, within the remit of the hosting exemption of the ECD i.e. is an ISSP benefiting from Art 14[17]. However this does conclusively not settle the matter of whether Google in its role as a cost-free provider of *search links* qualifies as an ISSP (the absence of linking liability immunity within the ECD is also discussed further below).

Thirdly, the ECD also excludes certain activities from its remit entirely, including taxation, competition law, and the activities of notaries and gambling. Liability for privacy or data protection breaches is also, somewhat surprisingly, exempted from the ECD (see the controversial Italian criminal case of *Italy v Google)*[18]. It is possible this may be corrected in the current reform process of the EC Data Protection Directive[19]. Thus, online intermediaries in these domains do not fall within the ISSP immunity regime.

B. The substantive rules

EU and the ECD

The ECD, as noted above, takes a horizontal approach to ISP liability. Furthermore, rather than giving a blanket immunity to ISSPs in all circumstances, as the US CDA section 230(c) does (see below), its approach is to separately address the various functions of ISSPs.

Where ISSPs act as a '*mere conduit'*— i.e., merely transmitting content originated by and destined for other parties—the ECD, Art 12, regards them as basically absolved from all liability as regards that content. To maintain immunity, the ISP must not initiate the transmission, select the receiver of the transmission or modify the information contained in the transmission[20].

Where ISPs *cache* material, they will not be liable for it subject to the same conditions as in Art 12[21]. Caching is a ubiquitous technical process whereby local copies of remote web pages are made by hosts when requested, in order to speed up delivery of those pages on subsequent request to speed up the Web for all users. Immunity is also subject to the ISSP taking down cached copies once they obtain actual knowledge that the original

---

[16] A UK court upheld the view albeit *obiter* that Google the search engine qualified as an information society service provider in *Metropolitan v Designtechnica* [2009] EWHC 1765 (QB). See also obiter discussion affirming this view in *Bunt v Tilley* [2006] EWHC 407 (QB) paras 43-45. Note also that a French court has found Wikipedia, the free online encyclopedia to be deserving of ISSP immunity: see OUT-Law news report of 6/11/2007, at http://www.outlaw. com/page-8615.

[17] *Google France v Louis Vuitton, etc, conjoined cases,* Judgment of the Court, Grand Chamber, 23 March 2010, Joined Cases C-236/08 to C-238/08.

[18] See *OUT-LAW News*, 3 March 2010 at http://www.out-law.com/page-10805.

[19] See initial proposal, *A comprehensive approach on personal data protection in the European Union*, 4 November 2010, at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[20] Art 12. Transmission includes automatic, intermediate, and transient storage. Presumably 'information' excludes header information which ISPs routinely and automatically add to through traffic they forward. Such header information is vital to the routing of packets through the Internet to their destination, but does not form part of the message information actually read by the recipient.

[21] Art 13, ECD actually refers in full to "*automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of that service.*"

source of the information has been removed or access to it disabled, or removal or blocking of access has been ordered by a competent court or authority.

The main controversy in the EC regime has centered on the *hosting* provisions in Art 14, which deals with circumstances where ISSPs host or store more than transiently content originated by third parties. Under Article 14, ISSPs are exempt from criminal liability in respect of the "storage" of information provided by a recipient of their services, so long as they have no 'actual knowledge' of 'illegal activity or information'; and are immune from civil liability so long as they have no such actual knowledge *and* are not aware of 'facts and circumstances from which the illegal activity or information is apparent'.

Art 15 provides furthermore that EC member states are not to impose on ISSPs "a general obligation actively to seek facts or circumstances indicating illegality". On the other hand, Art 14(2) expressly preserves the right of parties to seek injunctive relief to "terminate or prevent an infringement" and in practice, this is increasingly (if controversially) invoked as a route by which prior monitoring or filtering may be imposed on ISSPs in Europe by court order despite the apparent intent of Art 15 to restrain such (see further below, especially section VIII). Note that recital 48 provides that it is still possible for states to require ISSPs '*to apply duties of care which can reasonably be expected from them and which is specified by national law, in order to detect and prevent certain types of illegal activities*.' However it has been normally assumed that such 'duties of care'[22] mean those imposed by criminal or public law e.g. aid in investigation of crime or security matters, not as extending to duties under private law, e.g., to help prevent copyright infringement - since that would negate the point of Article 15 and indeed Art 14 generally.

Even if a host receives notice of offending content, it can avoid liability if it takes down or blocks access to that content "*expeditiously*". This imports the well known "notice and take down" or "NTD" regime. What exactly "expeditiously" means is a source of uncertainty around the ECD regime, especially for small ISPs and platforms. No guidance is given in the Directive as to what 'expeditious' means and whether it allows enough time to, e.g. check facts, consult an in house lawyer, find an external lawyer or request counsel's opinion. This vagueness can clearly be oppressive to defendants who wish to clarify their position before taking down. In large ISSPs, it may take some time for a take-down request to find the appropriate employee, or for the appropriate page to be located on a large website (a problem aggravated by the lack of a statutory form of notice); while in small ISSPs it may be difficult to identify an employee responsible, especially in a non profit making or volunteer organization; and how these indoor management issues affect 'expedience' remains unclear. National implementations of the ECD tend, unfortunately, to provide no further guidance than the Directive[23].

Article 14, furthermore, seems to imply that once notice has been given and the expedient period of grace expired, liability is strict even if takedown presents technical or administrative problems. A better alternative might be, as the German Multimedia Act provides, for liability to arise only after the ISSP has failed to take some kind of 'reasonable steps'. Reed suggests similarly that once an ISSP has received a takedown

[22] See e.g. R Bagshaw, 'Downloading Torts: An English Introduction to On-Line Torts' in H Snijders and S Weatherill, *E-Commerce Law* (Kluwer, 2003).

[23] Member states can of course clarify the time for expeditious take down in their own laws e.g. the UK Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007, prescribe that take down, of
terror-related content only, must take place within two days.

notice, its duty should not be an absolute requirement to remove but merely to "to do what is reasonable to prevent further communication of that notified content"[24].

United States – CDA and DMCA

In 1996, Congress passed the Communications Decency Act (CDA) in an effort to prevent minors from accessing undesirably adult speech online. While most of the CDA was struck down as unconstitutional, s 230(c) remained in force and grants total immunity to any "interactive service provider" in respect of content provided by a third party. The section has been interpreted broadly, to apply to many types of "publication tort," including defamation, privacy, negligent misstatement and most recently, soliciting prostitution by advertising, but criminal content is excluded. Notably, it has been repeatedly upheld to grant immunity, even where notice to take down is served on the service provider and even if they then fail or refuse to remove it.

Copyright liability is however exempted from s 230(c) and instead dealt with by the regime for online intermediaries created in the DMCA in 1998. The DMCA creates a limited liability regime much more akin to the ECD than the total immunity of the CDA s 230(c). As with the ECD, different functions carried out by intermediaries are given immunities known as "safe harbors": as with the ECD these include "mere conduit", caching and hosting, but the DMCA goes further and also includes "linking tools", which include search engines and hyper linkers (e.g. price aggregators or comparison sites). Because those classes were fixed in the statute in 1998, their application to later-developed technologies such as P2P intermediaries has been raised but rejected by the US courts (see below). The DMCA safe harbors apply only if the service provider establishes, publicizes, and implements both a NTD system for removing content when copyright owners complain, and a system for identifying "repeat infringers" and removing them from the system. The DMCA also requires hosts to accommodate technical protection measures (TPMs). The DMCA (like the ECD, and unlike the CDA) also allows suit for injunctive relief against an intermediary.

C. General concerns with notice and takedown paradigms

Freedom of speech and privatized censorship

Many have claimed that NTD regimes can exert a potential chilling effect on freedom of speech. Research seems to support the proposition that in the interest of avoiding litigation or risk, ISPs and hosts are sometimes inclined to remove or block access to notified content, without investigating it in detail. They are thus arguably pushed into colluding on what has been termed 'privatized censorship' even though they do not have the authority of a court, or always any knowledge of specific relevant areas of law, such as fair use or libel law[25]. In research carried out at Oxford known as the 'Mystery Shopper' test a major ISP in the United Kingdom was asked to take down a web page alleged to be a pirate copy.[26] In fact the web page contained an extract from Mill's 'On Liberty', published in 1869 and long in the public domain. Nonetheless the webpage was removed

[24] See Reed C, "Policies for Internet Immunity", (2009) 19(6) Computers and Law 20.
[25] See discussion in C Ahlert, C Marsden and C Yung, 'How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation' ('*Mystery Shopper*') cited at http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf.
[26] Ibid.

without demur.[27] The Oxford researchers concluded from this and other examples that '*the current regulatory settlement has created an environment in which the incentive to take down content from the Internet is higher than the potential costs of not taking it down*'[28]. Looking at the roughly similar copyright NTD regime of the DMCA, Urban and Quilter found that almost a third of takedown requests made by rightsholders were apparently flawed or unjustified, and that over half the demands for link removal came from competitor companies.[29]

The project analyzed all the take down notices (876 in totals) received by the search engine Google between 2002 and 2005 and subsequently posted on the Chilling Effects website[30]. 30% of take down notices received raised "obvious" queries as to validity, which a court would have been bound to consider before granting an injunctive remedy. These included defenses for fair use, claims over public domain material, and notices in unclear form. The authors commented:

"The surprising number of questionable takedowns we observed, taken in conjunction with the ex ante removal of content, the minimal remedies for abuse of process, and the lack of knowledge about the counter notice procedures, suggest that few are well served by [the NTD process]".

In the ongoing consultation on reform of the ECD, Art 19, a global civil society group for freedom of expression has argued strongly there should be no take down without intervention of judicial oversight[31]. Few EC countries currently provide for such on a mandatory basis though some e.g. Belgium do require an official such as a prosecutor to agree to removal of criminal content.

One factor that might deter an ISSP from taking down might be the fear that unfounded takedown would lead to a claim for breach of contract from the content provider. In the US DMCA, when an ISSP takes down in good faith, it is protected from any liability arising. No such protection exists in the ECD (although as the Directive is a minimum harmonization, there is no reason why states cannot introduce such protection). It seems likely, though, that European ISSPs still regard default take down on demand as their safest and easiest option. Acceptable use clauses in subscriber contracts can probably control the risk of breach of contract, and consumer-oriented ISSPs may also rely on the inertia of consumers in relation to litigation. By contrast the risk of liability for e.g. obscene

---

[27] Similar results were found in a similar experiment carried out subsequently by Sjoera Nas at Bits of Freedom, a digital human rights group based in the Netherlands. Nas, posing as copyright owner, asked 10 Dutch ISPs to remove works by a Dutch writer who died in 1860 and hence was in the public domain. 7 providers took down the text without apparently checking it out at all; one failed to respond to the complaint; one examined the text complained of and noted it was in the public domain (xs4all, a small ISP with a history of digital rights activism) and one forwarded the complaint to the website owner. Her 'takedown hit rate' was thus 70%.

[28] *Mystery Shopper*, above n 25, at 12.

[29] Urban J and Quilter L, Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act: Summary Report, available at http://mylaw.usc.edu/documents/512Rep-ExecSum_out.pdf.

[30] See 'Chilling Effects Clearinghouse' at http://www.chillingeffects.org/, a joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, and George Washington School of Law clinics. The site hosts take down notices voluntarily submitted by private parties and participating ISPs and sites such as Google.

[31] See Art 19 press release, 9 November 2010, at http://www.article19.org/pdfs/press/european-commission-freedom-of-expression-needs-better-protection-in-digital.pdf.

material or copyright infringement is less easy to shift and is more likely to be pursued by state agencies such as police.

The DMCA builds in other safeguards to discourage arbitrary NTD. Any takedown notice *must* be notified to the content provider, who then has the opportunity to protest that the material should not be removed, in which case it must be 'put back' by the ISP. If the original notifier then continues to dispute the legality of the content, and the content provider to assert it, the argument must be taken to the courts. While dispute is in progress, the ISP is given 'safe harbor' to keep the content up, free from liability, even if in the end a court does decide the content was illicit or actionable. This system of notices and counter-notices largely builds on a common understanding between rightholders and intermediaries, and represents a serious attempt to provide a balanced solution. By contrast, nothing in the EC regime requires notification to the site whose content is taken down, and this would be a matter for each state's legislation or most often, for each ISSP's internal procedures and subscriber contracts. The uncertain requirement of 'expedient' take-down in the ECD (see above), lacking the DMCA's safeguards, only encourages EU ISSPs further to take down now, and investigate later, if at all.

The DMCA also has strict rules that the person demanding take down must properly identify themselves as the rights-holder with locus to demand take down (using digital signature identification if requesting take down by email) and specifies details enabling offending content to be easily located. Both rules discourage fraudulent, unauthorized or over-broad complaints and help the recipient of the notice to be able to practically comply. Furthermore there are serious penalties for any person making a false allegation as to infringement (s 512 (f)) which have been enforced in the US courts[32]. These DMCA rules in principle seem beneficial to any copyright NTD regime and have an obvious deterrent function in regard of eventual misuse of the system.

Search engines and linking liability

Search engines, such as Google, Bing, Baidu and others have become crucial to the navigation and management of Internet resources. There is no global consensus however as to whether search engines should benefit from the safe harbors or immunities given to "traditional" online intermediaries. Search engines as their *raison d'être* create links to material over which the search engine has neither legal nor de facto control, nor, in practice, any human knowledge (since the web spidering systems are entirely automated) and yet there is a constant risk of some kind of liability arising, including under some theory of authorizing copyright infringement.

The US DMCA under its head "locational tools" expressly grants immunity under certain conditions where a link is made to infringing material.[33] In Europe, by contrast, there is no explicit category of immunity. "Hosting" as dealt with in Article 14, requires "storage", itself undefined in the ECD, which seems to imply that merely making a hyper-link to content cannot constitute 'hosting'—therefore any liability which may arise in relation to a hyper-link under national law is not excluded by Article 14. Very few cases in Europe have as yet actually created any problems by ascribing liability to search engines for making links however[34] (arguably one of the few such examples being the Belgian copyright case of

[32] See *Online Policy Group v. Diebold*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).
[33] S 512 (d) Information Location Tools.
[34] See e.g. Spanish, Swiss and French decisions all exculpating Google as responsible for defamation by virtue of linking to such text, discussed in the English case *Metropolitan International*

[Footnote continued on next page]

Copiepresse)[35]. As noted below, the ECJ has looked at the liability of Google as a *host* in *Google v LVMH*[36] but not yet at Google as a linking intermediary. The question of linking liability in the EC thus remains a matter for the domestic law of each member state. Although the EC Commission was specifically instructed to investigate linking liability on an ongoing basis by Article 21(2) of the ECD, so far, only a few states have chosen to create special linking immunities, creating cross-Europe disharmony.[37]

Linking is of ever greater significance as the Internet becomes manageable only via search engines and other linking intermediaries e.g., tagging sites like Digg[38] and delic.io.us. Since the drafting of the ECD, aggregators have also become important online intermediaries— sites which aggregate content from a variety of linked sites so that, say, a user can read the headlines and a few lines from multiple news sites conveniently on one page, or compare prices from a range of providers for utilities like gas or water, or read multiple blogs on one page (so-called RSS readers). What all such aggregators are doing is in essence making links to a wide variety of 'upstream' content over which they have no editorial control, and where they may or may not have technical control to remove individual items, depending on how the software code is implemented. Aggregator sites, alongside search engines and tagging sites are generally seen as a public good in terms of promoting access to knowledge, information management, consumer choice and competition[39]. This is one area where there is broad consensus, except perhaps in the online news industry[40], that search engines and other linkers need the comfort of a certain level of certainty and protection from legal risk, and it would seem distinctly desirable for model global guidelines to be produced on the liability of search engines and hyper linkers.

V. GOING BEYOND NOTICE AND TAKEDOWN – WHY?

The new online intermediaries and new ways to enable or assist copyright infringement

P2P intermediaries and hosts for infringing files

We noted above, that in the time since the last report on this subject was commissioned by WIPO from the current author Edwards, along with Waelde, in 2005, the problems shaping the question of online intermediary liability for copyright infringement have

---

[Footnote continued from previous page]

School v Designtechnica [2009] EWHC 1765(QB) at paras 97ff. The English court also found Google not liable for linking to a defamatory "snippet".

[35] *Copiepresse v Google*, [2007] ECDR 5, Brussels Court of First Instance (TGI), 13 February 2007.

[36] Case C-236/08. See discussion at n 17 supra.

[37] See UK *Consultation document on the electronic commerce directive: the liability of hyperlinkers, location tool services and content aggregators - Government response and summary of responses*, DTI, December 2006.

[38] See the controversy in 2007 over whether Digg were legally responsible for taking down on notice tags made by its users, linking to sites featuring a digital encryption key, which AACS were attempting to suppress since it assisted in DVD piracy. As *Boing-Boing* reported (May 2 2007, at http://www.boingboing.net/2007/05/02/digg-users-revolt-ov.html) "Digg's users revolted at this stricture, and saw to it that every single item on the front page of Digg contained the forbidden number".

[39] See e.g. Pasquale F, "Copyright in an Era of Information Overload: Towards the Privileging of Categorisers" (2007) 60 Vand. L Rev 135.

[40] See *Copiepresse* case, supra n 35.

changed dramatically. First and most obviously, the problem of infringing P2P filesharing, although already regarded as severe in 2005, appears, according to industry reports, to have vastly increased. Secondly, infringing music, video, film and even e-book content is also widely available for download from hosting intermediaries, many originally based around the idea of users uploading content which may be their own UGC but which have evolved also to host copyright infringing content. Such "web 2.0" online intermediaries include video streaming sites such as YouTube, Megavideo and DailyMotion.

Infringing content may also be directly available for download, in open or, frequently, encrypted form, from host or "cloud" intermediaries whose primary business is hosting, not social networking or UGC. These may be reputable businesses such as some cloud computing sites e.g. Dropbox, Amazon Web Services, or may have an approach which seems to be predominantly based on infringing material. In the course of the UK Digital Economy Bill debates these latter were termed "cyberlockers" and it was alleged by ministers that around 20% of infringing content was shared from such sites. Many such sites are based in foreign jurisdictions where they are hard to track down, or frequently move server when investigated; some hosting countries are regarded as "law havens". The BPI claimed in December 2009 that the use of foreign unlicensed MP3 sites among British adults grew 47% in the last 6 months of 2009, and that MP3 search engines, as well as blogs and message boards linking to "online hoards of music" were also becomingly increasingly prevalent[41].

The question thus arises whether special duties should be imposed on (or immunities from liability removed from) such online intermediaries, in order to protect the legal rights and business interests of rightsholders. We look at the possible form such duties might take relating to P2P filesharing, with a particular focus on graduated response regimes, in sections V to VII below.

In section VIII, we consider the use of legal regimes which require ISPs and hosts to filter content and block websites, which can be used both to limit access to sites facilitating P2P filesharing, and also to block access to sites hosting infringing content.

In section IX, we examine in more detail the question of whether particular hosts, such as video streaming and social networking sites, should be required to take steps to filter out infringing uploaded content.

Peer to peer (P2P)

There is considerable industry-supplied evidence that the advent of P2P technologies has created a massive increase in copyright infringement, which in turn threatens the health of the traditional digital content based industries, such as the music, film, video and gaming industries, with the publishing industry also affected. For example, in one much-quoted statistic, the International Federation of the Phonographic Industry (IFPI) estimated that in 2008, 40 billion files were shared online unlawfully and as a result 95% of all music downloads in that year were unlicensed[42]. The OECD also estimated in 2007 in the context of a major study of non-digital counterfeiting, that the consumption of pirated digital goods was "widespread"[43].

---

[41] See "BPI: Filesharers finding alternatives to P2P", PCPro.co.uk, 18 December 2009.
[42] IFPI, DIGITAL MUSIC REPORT 2009: NEW BUSINESS MODELS FOR A CHANGING ENVIRONMENT (2009), *available at* http://www.ifpi.org/content/library/DMR2009-real.pdf.
[43] OECD, *Economic Impact of Counterfeiting and Privacy*, 2007 at http://www.oecd.org.

Such assertions are not, however, uncontested. Those who counter the evidence for the impact of filesharing on content industry revenues often raise the following points: (i) every unlawful download cannot be regarded as a lost legal sale, given the idea of "try before you buy" and the fact that downloading may merely be replacing radio in this function; (ii) that downloading may in fact act as advertising or marketing for the legal content sectors, with some surveys showing high consumers of infringing downloads are also high consumers of legal music; (iii) some downloads may be of material not available legally and thus not replacing sales, e.g. deleted back catalogue; (iv) there is some doubt as to the methodologies and accuracies of the key surveys in the field[44]; and (v) even apart from dubieties over the figures on filesharing itself, decline in music industry revenues may be at least partly due to factors other than P2P filesharing, including the growth of alternative consumer goods on which to spend income[45], a loss of innovation in the music and film markets, and the decline of "blip" profits caused by the windfall effect of the format transfer from vinyl to CD in the 90s[46]. It is not the place of this report to adjudicate on the empirical evidence for and against the extent of infringing filesharing and, more importantly, its economic impact; but such controversy is nonetheless relevant when, as we will below, we come to look at what legal solutions are appropriate and proportionate to solving the problems faced by the content industries.

Early litigation in the P2P wars focused on the detail of copyright legislation rather than the more general rules on immunity or "safe harbors" surveyed, but did to some extent consider if immunities applicable to traditional online hosts or distributors, such as ISPs, could or should be applied to P2P intermediaries. (We will speak here both specifically of certain P2P actors such as clients, torrent sites, etc; and generically of these as "P2P intermediaries"). P2P intermediaries do not themselves typically host files of any kind which infringe copyright (cf, early "simple download" sites such as MP3.com, where the site itself was a host and clearly a primary infringer of copyright). Instead, P2P intermediaries usually enable users who have downloaded P2P software to then *inter se* unlawfully swap and share files containing works protected by copyright. Conceptually, such sites are best seen as "pointing to" infringing material since they do not directly host it, nor transmit it to peers. There are three or four clear generations of P2P systems and each has generated different legal issues and interpretations.

The first generation P2P intermediary, on its own website, provided a *centralized index* to all the files stored and available for upload on the various users' individual computers. This centralized model, which initially provided the most speedy and efficient search facilities for users, was that used by the now defunct pre-commercial Napster site, later found liable in the US courts for contributory and vicarious infringement of copyright (see below, section VI).

The second generation, which was developed both for greater robustness but also to avoid legal liability after *Napster*, has no such centralized index. Each user instead maintains an index only of those files stored on his or on her own machine. A user searching for a particular file obtains a desired file by sending out a request which is

---

[44] See e.g. Goldacre B "Illegal downloads and dodgy figures", *Guardian*, 5 June 2009 at http://www.guardian.co.uk/commentisfree/2009/jun/05/ben-goldacre-bad-science-music-downloads, rejecting figures quoted for impact on the UK economy.

[45] See figures and graph available at http://www.guardian.co.uk/news/datablog/2009/jun/09/games-dvd-music-downloads-piracy.

[46] See general discussion in Piacentin R R **"**Unlawful? Innovative? Unstoppable? A Comparative Analysis of the Potential Legal Liability Facing P2P End-Users in the United States, United Kingdom and Canada" (2006) 14 IJLIT 195.

passed from user to user of the P2P software in question, until it is met with a positive response, after which the file download is negotiated by the software directly between the user who has the file and the user who made the request. This decentralized model is that used by P2P services descended from Gnutella such as KaZAa and Grokster, which in their turn became the subject of lawsuits to more or lesser degrees of success depending on the jurisdiction (see also below). Systems still in use using this protocol include Ares and eDonkey, both still popular in Latin America though little present now in United States and Europe[47]. Some systems such as the recently defunct Limewire[48] enabled users' access to filesharing via both P2P and BitTorrent (see below).
A third approach which is merely a variation on the above, is that although there is still no centralized index, a number of user computers ("supernodes") act as servers hosting sub-indexes, thereby speeding up search times. Such "supernodes" can be seen conceptually as "sub-Napsters".

A fourth approach, or third generation, which is now the dominant player in most Westernized markets except Latin America[49] is the "BitTorrent" (BT) approach or protocol, originally devised by Bram Cohen in 2001. Although Cohen's own company, BitTorrent Inc, makes one client available, there are numerous other clients available running the protocol. In the BitTorrent protocol, files are not shared as one file but instead divided into small parts (bits) which can be individually uploaded and downloaded, enabling hundreds of thousands of users to very efficiently share even very large files such as HD movie and video files (or large legal files such as Linux operating system upgrades, or BBC iPlayer TV programmes). BT thus combines the decentralized approach of second generation P2P with the enabling of very fast downloading. It is a complicated protocol to analyze in legal context, involving several parties: the site which provides the client software; the site which provides "torrent" files which help locate other users who hold all or parts of the file which a user seeks to download; the tracker site which monitors the users contributing to the file transfer and passes their data to the client software; and the "swarm", one or more users (often in their thousands) also using the BitTorrent protocol, who join in uploading parts of the file sought (usually because they have themselves previously downloaded it).

In common BT parlance, a user providing upload access to a file is a "seeder", and one seeking to download it is a "leecher". "Torrent" files themselves in principle do not host any copyright content, but merely point the would-be downloader towards users who are likely to be able to supply such content (or parts of it). It is noticeable that this is not dissimilar to the role played by search engines such as Google which also point searchers towards files hosted by other users, while failing to host any such content themselves (or only for short periods, or only in small fragments) – we will return to this point in the discussion on the legal liability of P2P intermediaries below. An excellent slightly more

[47] eDonkey was in fact closed down as a client site under pressure from US courts in 2006: see "RIAA drops the dead eDonkey", OUT-Law News, 14 September 2006 at http://www.out-law.com/page-7299.
[48] See "LimeWire shut down by Federal Court", *Guardian*, 27 October 2010 at http://www.guardian.co.uk/technology/2010/oct/27/limewire-shut-down.
[49] See "BitTorrent still dominates global Internet traffic", Torrent Freak, 27 October 2010 at http://torrentfreak.com/bittorrent-still-dominates-global-internet-traffic-101026/ revealing that although in most of the world, BitTorrent now dominates, in Latin America P2P traffic of the second generation still forms the majority traffic with Ares the most used client.

poetic description of how the BitTorrent protocol operates can be found in a recent Australian case, *Roadshow Films Pty Ltd v iiNet Limited*[50].

"70. To use the rather colorful imagery that internet piracy conjures up in a highly imperfect analogy, the file being shared in the swarm is the treasure, the BitTorrent client is the ship, the torrent file is the treasure map, The Pirate Bay provides treasure maps free of charge and the tracker is the wise old man that needs to be consulted to understand the treasure map.

71. Whilst such an analogy grossly oversimplifies the situation it will suffice for present purposes. It demonstrates that all of the constituent parts of the BitTorrent protocol must work together before a person can access the file sought. In this judgment the Court will refer to all the constituent parts together as the 'BitTorrent system'.

72. Such analogy also demonstrates that a number of deliberate steps are required to be taken by a person to bring about the means to infringe the applicants' copyright. The person must download a BitTorrent client like Vuze, seek out torrent files related to copyright material from websites, and download those torrent files and open them in their BitTorrent client. Thereafter, the person must maintain connection to the internet for as long as is necessary to download all the pieces. The length of this downloading process will depend on the size of the file, the number of peers in the swarm and the speed of those peers' internet connections."

It is important to note that BT is merely a protocol; like all P2P systems from Napster on, it can be used to share non-infringing files as well as infringing material (and as the examples above show, often is). Another key point to note is that the BT approach, unlike earlier P2P systems, only works efficiently if all or at least most of the users are both uploaders and downloaders, and accordingly software is mainly designed so it is the default to do both simultaneously (although there are ways to avoid this). This can be significant both for strategies of law enforcement, as campaigns of action against users have mainly concentrated on suing key repeat uploaders, rather on the millions of downloaders; and for the legal defenses of users in some civilian legal systems such as France, where downloading for private non-commercial purposes of a certain number of copies is a legal exception to copyright. Finally it may also be significant for legal characterization that, as files are made available in small pieces, no one user can be identified as supplying (making available) the file as a whole to any other user: it comes, as the judge explained in *Iinet*, from the "swarm".

Litigation relating to this newest generation of P2P has so far centered to date, for reasons of both imputed culpability and practicality when faced with millions of infringers, on suing high volume uploaders for making available (a globalised infringement under international copyright law) copyright works without permission, and where that has seemed ineffective, on suing torrent sites such as the notorious Pirate Bay (which themselves provide the pointer to tracker sites). Suing the creators of the client software, given its multiple uses, legal and non-legal; the lack of a direct revenue stream related to infringement; and the fact that many of the authors had academic or theoretical purposes

[50] [2010] FCA 24 available at http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCA/2010/24.html. See further details on how BitTorrent works at paras 56-73, and a good commentary on the decision at http://www.technollama.co.uk/landmark-isp-liability-case-decided-in-australia. iiNet was appealed in February 2010, but the first instance judgment upheld, see http://www.austlii.edu.au/au/cases/cth/FCAFC/2011/23.html.

in mind when they designed such systems, has been rare. However there has been a prosecution of the inventor of Winny P2P in Japan on criminal charges -this was however reversed on appeal[51]. More recent approaches such as "graduated response" shift attempts to enforce copyright from concentrating on the serious uploaders to the downloading population as a whole, by adopting non-court based enforcement methods which arguably scale better and cost less than court-based processes (see discussion, sections VII and VIII).

Many variations on BT have evolved, to meet both technical goals and the goal of avoiding legal detection of copyright infringement. Notably, a number of systems now exist running the BT protocol which also in various ways encrypt the content shared, or hide the IP addresses of the users sharing files. Some of the most prominent of such systems are Freenet[52] and Tor[53], the latter of which was created explicitly in pursuance of freedom of speech goals by the EFF to enable sharing of files without interception by authoritarian regimes. Neither system has become widely used by "ordinary" filesharers as the anonymisation of content nor does identity have the side effect of making the software slow and fiddly to use. In Japan however, encrypted P2P systems such as Winny and its more recent variant Share[54], running on much higher speed consumer broadband than is common in the West, are already in widespread use. It is likely that if placed under legal pressure by systems such as graduated response, Western uptake of encrypted P2P will become much more common, especially as next generation high speed broadband is also rolled out in the West[55].

Finally P2P systems where access is limited to known parties or those they introduce are also increasingly in use. In such "darknets", users manually establish connections with nodes run by people they know. Darknet typically needs more effort to set up but a node only has trusted nodes as peers. Again, it has been predicted that as more efforts are made to identify anonymous filesharers and apply sanctions, darknets, which evade detection methods, will be increasingly used by hardcore infringers[56].

VI. P2P: EARLY LEGAL STRATEGIES OF CONTROL

Suing P2P intermediaries

In the 2005 forerunner of this report, Edwards and Waelde reported in depth on the then relatively novel advent of P2P-related litigation. Five years on it is estimated that more than 35,000 lawsuits have been launched against individual filesharers in the US alone[57]

---

[51] See http://joi.ito.com/weblog/2006/12/17/winny-comments.html and http://yro.slashdot.org/story/09/10/09/0033200/Japanese-Ruling-Against-Winny-Dev-Overturned-On-Appeal.

[52] See R Roemer, "The Digital Evolution: Freenet and the Future of Copyright on the Internet" 2002 UCLA J.L. & Tech. 5 at http://www.lawtechjournal.com/articles/2002/05_021229_roemer.php.

[53] See http://www.torproject.org/.

[54] See http://en.wikipedia.org/wiki/Share_.

[55] Note the estimate of 20% of downloading taking place via encrypted P2P in Europe accepted in expert testimony in one 2010 Irish case, see *infra* n 96.

[56] See "Why the Pirate Bay Verdict Doesn't Matter" *Billboard*, April 16, 2009, at http://www.billboard.biz/bbbiz/content_display/industry/e3i9d7aa37d46e1460bf43ebe5148049570 and "Darknets and the future of P2P investigators", *Ars Technica*, March 5 2009, at http://arstechnica.com/tech-policy/news/2009/03/the-new-version-of-p2p.ars.

[57] See von Lohmann F, *RIAA vs The People Turns from Lawsuits to 3 Strikes*, 19 December 2008, at http://www.eff.org/deeplinks/2008/12/riaa-v-people-turns-lawsuits-3-strikes.

and hundreds if not thousands of lawsuits have also been aimed in multiple jurisdictions at P2P intermediary sites, from *Napster* on. Yet P2P filesharing persists, and efforts to thwart it have moved from primarily litigation based strategies, where individual users, P2P intermediaries and torrent sites are sued, to approaches involving the use of ISP co-operation ("graduated response" et al). Although the end of P2P litigation is by no means in sight, it is in some cases now of less practical interest than in 2005, and so will be dealt with in less detail in this report than in its predecessor.

Napster and Grokster

The first major case on liability of a P2P intermediary, *A&M Records* v *Napster*[58] was decided in favor of the music industry by the US 9th Circuit Court of Appeals in 2001. As noted above, Napster hosted a centralized index of all files available via the system; any user request for a particular song or other work was routed via this centralized index. Napster did not however host any infringing copies nor did it directly make any such copies; the primary infringers were thus solely the peers who used the system to share files *inter se*. The question therefore, as in most such subsequent cases, was whether Napster could be brought within the grasp of some theory of *secondary* liability, including contributory or vicarious liability, in US terminology. (Other jurisdictions have used concepts such as authorization[59] and acquiescence.)

Napster sought to avoid the imposition of contributory liability by arguing that its software was capable of substantial non infringing uses (swapping of files which were not protected by copyright and/or to which the copyright owners had consented). This argument was drawn from the leading case of *Sony Corp. v. Universal City Studios v Sony Corporation of America*[60] where the US Supreme Court had to consider whether Sony was vicariously or contributory liable for infringements carried out by users of the Betamax video recorder it manufactured. The court in *Sony*, finding it not liable as secondary infringers, drew on the "staple article of commerce" doctrine taken from patent law and held that *"The sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non infringing uses".*

The Ninth Circuit rejected this *Sony* defense on the facts of *Napster*, largely on the grounds that Napster had a greater degree of knowledge of the primary infringements than had *Sony*. Because Napster provided the centralized index, Napster, unlike Sony, had actual, not just constructive, knowledge of specific infringing materials. Where there was actual knowledge, it was irrelevant that the product was capable of substantial non infringing uses.[61] On vicarious liability, the court also found Napster liable, opining that Napster not only enjoyed a financial benefit - *'financial benefit exists where the availability of infringing material 'acts as a draw' for customers…Napster's future revenue is directly dependent upon increases in user base'* - but also that Napster had the right and ability to supervise the infringing conduct by blocking users' access to its service.

---

[58] *A&M Records, Inc v, Napster Inc*, 239 F3d 1004 (9th Cir, 2001)

[59] See e.g. in England and Wales, the discussion of authorization and a "Usenet indexing system" in *Twentieth Century Fox v Newzbin* [2010] EWHC 608; discussion of the same in Australian law in *Cooper v Universal Music Australia* [2006] FCAFC 187 and *Roadshow Films v iiNet Ltd*, latter discussed supra n 50. Note that in *Newzbin*, the Usenet indexing site was found liable as primary infringer for making available as well as authorizing its users to infringe.

[60] 480 F supp 429 (C.D Cal 1979) rev'd 659 F 2d 963 (9th Cir 198d1) rev'd 464 US 417 (1984).

[61] *Napster 2.* 239 F 3d at 1021.

Significantly, attempts by Napster to plead the safe harbors for intermediaries established by the DMCA both for hosts and for "mere conduits" were thoroughly rejected by the first instance court. Patel J[62] held that as Napster had been found to satisfy the objective test for constructive knowledge (Napster had reason to know about infringement by third parties) that put to an end to the *'defendant's persistent attempts to invoke the protection of the Digital Millennium Copyright Act, 17 U.S.C. s 512 as this subsection expressly excludes from protection any defendant who has an actual knowledge that the material or activity is infringing'* [63]or '*is aware of facts or circumstances from which infringing activity is apparent'*.[64] This finding was later slightly narrowed by the appeal court but not significantly enough to help Napster.

After this victory for the music industry in Napster (which led to its bankruptcy and disappearance in its illicit form), as noted above, a second generation of P2P emerged which was almost entirely decentralized: no actual knowledge could be easily ascribed to the P2P intermediary as they no longer held a central index of all files available to be shared. This change of architecture leads to the defendants in M*GM v Grokster* initially scoring a win at District and then Appeal Court[65] level. Since the software they distributed was, it was agreed, "capable of substantial non-infringing uses" then contributory liability could not be imposed without proof of actual, not just constructive, knowledge. In practical terms, even if a rightsholder had pointed to a file on a Grokster user's computer and said "remove it ", Grokster itself could have done nothing. Accordingly, Grokster was found not to be liable.

On appeal to the Supreme Court*[66]* however, Grokster finally lost because a new doctrine was evolved in US copyright law, of "inducing" copyright infringement. The court held that "*one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.*" There was considerable evidence that Grokster knew its users were using their software to infringe copyright; that they had advertised themselves as an heir to Napster, and thus built an audience and a business model on infringement. Accordingly the Court unanimously concurred that Grokster could be held liable for inducing copyright infringement, although there remained considerable dissensus over the impact of the *Grokster* case on the *Sony* doctrine of substantial non-infringing uses. Effectively however, the Supreme Court decision killed, in US law at least, the decentralized P2P model as a clever way of avoiding being pinned with contributory liability for peer infringements.

After Grokster

Despite this apparent track record of success, the music industry's victories in *Napster*[67] and *Grokster* have turned out to be somewhat pyrrhic[68]. The "inducement" theory of *Grokster* did indeed enable more US music industry victories, most recently in relation to

---

[62] 114 F.Supp.2d 896.
[63] DMCA s 512(d)(1)(A).
[64] DMCA s 512(d)(1)(B).
[65] 380 F 3d 1154 (9th Cir 2004).
[66] *MGM v Grokster* 545 U.S. 913 (2005).
[67] And also the intervening case of *In Re Aimster* 334 F.3d 643, 67 USPQ2d 1233, where the court refused to believe that a Napster-like system had protected itself from gaining actual knowledge by encrypting its central index and thus making itself "wilfully blind".
[68] Bridy, A, "*Why Pirates (Still) Won't Behave: Regulating P2P in the Decade After Napster"* (2009) 40 RUTGERS L.J. 565.

P2P site Limewire[69] which was closed down by permanent injunction in October 2010 following defeat on the merits six months earlier. Similarly in *Columbia Pictures Industries, Inc. v. Fung*[70] the court found overwhelming evidence of inducement and used it to close down a BitTorrent tracker site. Notably, the *Fung* court also held that this type of site too could not qualify for the DMCA safe harbors. The court stated that "*inducement liability and the DMCA safe harbors are inherently contradictory*," particularly since inducement liability is based on "*active bad faith conduct aimed at promoting infringement*" while the statutory safe harbors are based on "*passive good faith conduct aimed at operating a legitimate internet business.*[71]" In some cases the mere threat of court action following *Grokster* has been enough to close down sites: for example, eDonkey, a prominent P2P site responsible for around a quarter of P2P traffic in 2004, was sued by Arista and other record labels for £30m in 2006 and subsequently settled and closed down[72].

So why have these court victories not won the war against P2P (as they evidently have not)? A number of reasons have contributed. First, modern decentralized protocols of the BitTorrent generation and later make it very difficult to find a critical central chokepoint intermediary to sue, as was true in the days of Napster. Even if the client site is closed down, as was the case with Limewire recently, legacy users of the system can go on swapping files between each other indefinitely, unless they are forced in some way to upgrade to a new version which prevents them e.g. by installing filters which disable access to non-legal content[73].

Secondly, while Napster was a proprietary technology, BitTorrent is an open source protocol. This means that clones and variations on it are constantly springing up. Even if current BitTorrent clients are taken down, new ones can arise with very little effort.

Thirdly, the problem is no longer just or even mainly a US one but an international one. Since the transmission of the actual shared file is peer to peer, the site providing both client software, and, for the BitTorrent protocol, the torrent files, can both be situated outside a particular nation-state jurisdiction without it particularly discomforting the filesharer. In other words, although victories might have been won to some extent in the US courts, the music industry still finds itself fighting a war against sites increasingly situated in every country of the world, where the courts may or may not go along with the same theories as have been successful in the US, and where enforcement of injunctions may be difficult in practical terms even if obtained. In Spain, for example, an appeals court found that a BitTorrent site merely provided an index of links, did not host infringing content on its own site and did not have a commercial purpose and thus did not commit any criminal offense under Spanish copyright law[74]. Even where the courts have agreed, as in the US, that P2P intermediary sites are infringing copyright (as they often, though

---

[69] On Limewire, see n 48 supra. See also *Arista Records LLC v. Usenet.com, Inc.*, 633 F.Supp.2d 124 (S.D.N.Y. 2009) where inducement was one of the grounds on which liability was found, although the site in question was an actual host of infringing copies rather than a "pure" P2P intermediary.

[70] No. 06-05578 (C.D. Cal. Dec. 21, 2009).

[71] Idem at 43.

[72] See n 47 supra and discussion in Bridy, supra n 68 at n 132.

[73] See e.g. "US court demands stronger copyright filters for Morpheus", 17 October 2007 at http://www.out-law.com/page-8557.

[74] See European Digital Rights, "Spain: Indexing torrent files is not copyright infringement," EDRI-gram (Sept. 24, 2008) at http://www.edri.org/edrigram/number6.18/link-torrents-not-infringement.

not always, have[75]) there are still usually sites still available in other countries, including some "law havens" where action from law enforcement authorities is unlikely to be swift[76]. Fighting multiple, legally complicated and controversial cases abroad has also proven to be both time consuming and very expensive. Meanwhile moving a P2P torrent site abroad is as easy as moving data files to a new server; resulting in typically a brief hiatus for users, rather than a permanent closedown.

Suing torrent sites

The Pirate Bay saga is a good example of all this. Modern third generation P2P networks, as noted above, depend on intermediary sites, which host files known as "torrents", such as the well-known Pirate Bay[77]. Clearly there is an argument to be made, though a controversial one, that torrent hosts may also be contributory or secondary infringers of copyright, or inducers of infringement; and in 2009, the Swedish courts found that the operators of the Pirate Bay site had criminally infringed Swedish copyright law, and sentenced them to a year in jail and a £2.4million fine.[78]

The defendants argued that the Pirate Bay merely provided links to offending files, and were doing nothing different from respectable search engines like Google. If search engines have a claim to safe harbors or immunities, as discussed above in the last section, should torrent sites not also benefit from these[79]? The Swedish court found however that the Pirate Bay was very different from Google, both in terms of its owners' "awareness of illegality", and their acts. The judge found that:[80]

"...all the defendants were aware that a large number of the website's users were engaged in the unlawful disposal of copyright-protected material. By providing a website

[75] Wikipedia records a litany of court-sanctioned raids on and take downs of torrent and associated P2P sites in various countries including Sweden, Slovenia and Finland, see http://en.wikipedia.org/wiki/Legal_issues_with_BitTorrent; although note that some of these would have been after preliminary injunctions rather than the product of a fully argued legal case. In Holland, one significant victory was when the Dutch court found in August 2009 against Mininova, a prominent torrent site, which subsequently closed down unable to meet court requirements to remove infringing torrents: see http://www.theregister.co.uk/2009/08/26/mininova_loses_lawsuit/. There has also been international dissensus relating to court action against ISPs asking them to block access to P2P sites like torrent sites. In Denmark, in May 2010, the Danish Supreme Court upheld an injunction against a major ISP requiring it to block access to the Pirate Bay. Similar injunctions were upheld by the Supreme Court of Italy in December 2009. In Norway however a request for such an injunction was rejected by the courts, as was also the case in Australia and recently, Ireland. We discuss this issue of requiring ISPs to block websites as opposed to the liability of P2P intermediaries themselves in detail below at section VIII of this report.

[76] See "Internet pirates find "bulletproof" havens for illegal filesharing", *Guardian*, 5 January 2010 at http://www.guardian.co.uk/technology/2010/jan/05/internet-piracy-bulletproof.

[77] See http://thepiratebay.org/.

[78] *Sony and Ors v Neij*, Stockholm District Court, Division 5, Unit 52, VERDICT B 13301-06, 17 April 2009 handed down in Stockholm, Case no B 13301-06. Unofficial English translation commissioned by the IFPI, available at http://www.ifpi.org/content/library/Pirate-Bay-verdict-English-translation.pdf. On appeal by the defendants in November 2010, the judgment was upheld: see http://www.bbc.co.uk/news/technology-11847200.

[79] See amusingly, http://www.thepirategoogle.com/, a site deliberately created to demonstrate that: "The intention of this site is to demonstrate the double standard that was exemplified in the recent Pirate Bay Trial. Sites such as Google offer much the same functionality as The Pirate Bay and other Bit Torrent sites but are not targeted by media conglomerates such as the IFPI as they have the political and legal clout to defend themselves unlike these small independent sites."

[80] Unofficial English translation used.

with advanced search functions and easy uploading and downloading facilities, and by putting individual file-sharers in touch with one other through the tracker linked to the site, the operation run via The Pirate Bay has, in the opinion of the District Court, facilitated and, consequently, aided and abetted these offences."

Furthermore in terms of financial complicity, the Pirate Bay operators were not, as often portrayed, merely high-spirited anarchists, but, the court found, generating sizeable revenue from advertising on the site. The written evidence confirmed that at least 1,200,000 Swedish crowns had been paid to the defendants for advertising space on their site.[81] Significantly in comparison to Google, furthermore, the majority of the files the Pirate Bay linked to were protected by copyright, implying that their business model was indeed substantially based on infringement.

The ECD exemptions for online hosts, as incorporated into Swedish law, were plead for the Pirate Bay, but rejected, just as the DMCA immunities for mere conduit and location tool had been similarly rejected in the United States in the *Napster* and *Grokster* decisions. Since the Pirate Bay posted takedown letters sent in by copyright owners on their own site to ridicule, the court had no problem holding they had actual knowledge of copyright infringement but had failed to take down. Thus in this case the court could, perhaps unusually for the future, rely on actual notice, without having to look for constructive knowledge. But the plethora of evidence available here, of complicity with infringing users, business models obviously built on illegality, notice of illegality ignored, plus failure to co-operate with law enforcement or industry enforcers, will most likely not be present in such an easily demonstrable way all in future cases. (Sites such as the now defunct Limewire, for example, overtly required users to click to agree that they would not infringe copyright before allowing them to share files[82].)

What happened after the Pirate Bay lost is however perhaps the most salient part of the story. Despite of the celebrated victory, and a subsequent victory in the appeal courts, the Pirate Bay site is still up. This is not just because of delay caused by the appeal process. In the past the Pirate bay has moved its servers to other countries including the Netherlands to avoid police action, threatened to buy an island ("Sealand") to establish as its own legal jurisdiction, and according to the site TorrentFreak is now considering if the servers could be mounted in space on a satellite[83]. Even without such extreme measures, the difficulties of physically closing down one, let alone dozens, of highly mobile torrent sites[84] become apparent.

As Bridy puts it:

"In the final analysis, the industry's high profile legal victories against P2P network operators have not amounted to a durable or comprehensive network-level solution to the problem of P2P piracy. For every network operator that has been sued out of existence, another has come along : exit Napster, Aimster and Grokster; enter Azureus, LimeWire

---

[81] Although this did not match the claim made in the course of the trial that the Pirate Bay site made 10 million Swedish crowns in revenue during one year. See report at EDRI-Gram, 11 March 2009, at http://www.edri.org/edri-gram/number7.5/pirate-bay-trial.

[82] Courts seem however increasingly willing to disregard such statements as merely "cosmetic" in face of other contextual evidence of knowledge: see e.g. *Newzbin*, supra n 59 at paras 65ff.

[83] See *Torrentfreak*, 10 October 2010, at http://torrentfreak.com/pirate-parties-plan-to-shoot-torrent-site-into-orbit-101020/.

[84] TorrentFreak also provides a list of "25 other torrent sites you might like to use while the Pirate Bay is down" – see http://torrentfreak.com/top-25-most-popular-torrent-sites-of-2009-091213/.

and Shareaza. Hydra-like, they just keep coming back. And for some, as sites like the Pirate Bay demonstrate, flouting copyright law is the point"[85].

Suing users

Co-existent with the years of litigation described above against P2P intermediaries, has been a sustained campaign of civil action against P2P users as primary infringers, particularly in the US, led by the record and film trade bodies, the RIAA and the MPAA. The aims of such action were both to deter users from infringing by scare tactics, and also as an educational tool, to try to alter norms that filesharing was common and acceptable behavior. In other countries, such as the UK, suing users has been seen as something of a last resort because of the damage it causes to public relations; nonetheless volume litigation (or rather, the threat of it) is also now being conducted in the UK, though mainly on the instructions of the computer games, and adult films copyright industries, rather than music and "mainstream" film companies. In 2008, however, the RIAA famously declared that they would no longer depend on suing users as their primary weapon in the fight against filesharing but would turn instead towards seeking ISP co-operation as the best way forward[86]. Why was this? Suing users has proved counter productive on a number of counts, creating something of a Public Relation disaster[87]. First, the process is prone to error,[88] producing well known cases where dead people or grandmothers innocent of technology received lawyer's letters.[89] Secondly, penalties imposed, especially punitive statutory damages available in the US in civil copyright cases, or in some jurisdictions, even criminal sentences, were often seen as disproportionate to the infraction (e.g. a three months jail sentence given to Hong Kong Special Administrative Region of China filesharer for uploading three movies).[90] Thirdly, the emphasis on suing P2P filesharers distracted energy and attention from pursuing obvious large scale commercial IP infringers e.g. counterfeiters of physical goods such as pirate CDs. Fourthly, and perhaps worst, volume litigation against users has become publicly regarded as a form of legally-sanctioned blackmail or racketeering. Recipients of letters threatening legal action over filesharing rarely if ever fight the case to court, no matter what the merits of the case are, especially if the damages demanded are kept relatively low and the potential legal costs and risk seem very high. In the UK, one firm of lawyers conducting volume litigation against filesharers, Davenport Lyons, was formally reported to, and is now under investigation by, the solicitor's disciplinary body for "bullying" behavior,[91] and was

---

[85] Bridy supra n 68, at 589.

[86] SEE ANDERSON N, "NO MORE LAWSUITS: ISPS TO WORK WITH RIAA, CUT OFF P2P USERS," 19 DECEMBER 2008, AT HTTP://ARSTECHNICA.COM/TECH-POLICY/NEWS/2008/12/NO-MORE-LAWSUITS-ISPS-TO-WORK-WITH-RIAA-CUT-OFF-P2P-USERS.ARS.

[87] On this see generally Yu P, "The Graduated Response", (2010), *62 Florida Law Review,* draft paper available at SSRN at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1579782.

[88] We discuss below in more detail at n 96 and text following how filesharers are identified by IP address and what problems of error can arise.

[89] See Yu, supra n 87, at 16-17.

[90] *Chan Nai Ming v HKSR* [2007] 3 HKC 255 (CFA). In the US, see the widely reported case of Jammie Thomas-Rasset, who after several appeals was ordered to pay $1.5 million in statutory damages for downloading and sharing 24 songs – see http://copyrightsandcampaigns.blogspot.com/2010/11/third-thomas-rasset-verdict-15-million.html.

[91] SEE WILLIAMS C "MAJOR LAW FIRM DROPS FILESHARING THREATS", *THE REGISTER*, 12 MAY 2009, AT HTTP://WWW.THEREGISTER.CO.UK/2009/05/12/DAVENPORT_LYONS_ACS_LAW/.

subsequently trenchantly criticized in Parliament; another firm, ACS-Law, which picked up much of the same work after Davenport Lyons ceased operations, has recently been involved in a serious data breach where personal and highly sensitive data it collected about filesharers was released to the public following a DDOS attack combined with its own inadequate security.[92] In short as *Rolling Stone* magazine put it, suing users has made the content industries "the most hated industry since the tobacco industry"[93].

VII. NEW APPROACHES AND "ISP CO-OPERATION": GRADUATED RESPONSE

As noted above, since 2008, the music and other IP industries have thus turned away from the unsuccessful and counter productive campaign of litigation against users and, to some extent, P2P sites, and turned to the more indirect strategy of seeking "ISP co-operation". In particular this co-operation (whether achieved by voluntary agreement, or through exertion of legal or state pressure) takes two forms.

One, the industry seeks to have ISPs play an active role in regulating the behavior of their users and applying sanctions to them when they are alleged to have infringed copyright. The actions ISPs are asked to take range from sending warnings to users, to monitoring traffic to and from users, to slowing their traffic or denying individual users access to certain websites; and as a last resort, entirely disconnecting the user from Internet access. These policies under the general head of "graduated response" are discussed below. Secondly, rightsholders seek to have ISPs block access to certain websites, such as torrent sites or "cyber lockers", which they allege are vital to the continuation of unlawful filesharing. The crux of the current debates around copyright infringement and intermediary liability is whether it is both right, practical and cost effective for ISPs (and other intermediaries such as universities, or search engines) to have such duties placed upon them; and what the consequences of such regimes are for the public interest, for creators, for commercial prosperity and for the fundamental freedoms of Internet users.

Such regimes of "co-operation" can be achieved in at least three ways. First, the intermediaries involved may voluntarily agree to participate, for whatever reasons, without legal pressure from state or courts. This has been true of some leading US ISPs. Secondly, participation may be imposed as the result of private court action led by industry bodies or rightsholders (as has happened in *inter alia* Belgium, Ireland, Italy, and Denmark).[94] Thirdly, co-operation may be imposed by legislation, as has happened recently in France, UK, Republic of Korea, and Chile, and has been introduced but for the moment suspended in New Zealand. In some cases, the lines between these three

---

[92] See BBC News report, 28 September 2010 at http://www.bbc.co.uk/news/technology-11418970. Subsequently, ACS-Law were involved in proceedings which revealed they had written to around 10,000 alleged unlawful downloaders of adult films on behalf of a firm called Media C.A.T, threatening action unless £500 was paid. ACS-Law were eventually told by the court to drop the cases they had outstanding against alleged filesharers because there was a threat of "of working real injustice" (*Media C.A.T. Ltd. v A* [2010] EWPCC 17) and were also ordered to pay the court costs involved because of their "chaotic" behavior. According to research reported in the *Guardian* (http://www.guardian.co.uk/technology/2010/oct/05/acs-law-filesharing-copyright-claims), ACS-Law had kept 40% of sums gathered this way, a higher share than artists received which was typically 20-30%.

[93] Steve Knopper, *RIAA□s Gaze Turns from Users to ISPs in Piracy Fight*, ROLLING STONE, Dec. 19, 2009, at http://www.rollingstone.com/rockdaily/index.php/2008/12/19/riaas-gaze-turns-from-users-to-isps-in-piracy-fight/.

[94] See n 75 supra, and section VIII.

paradigms are blurred, or a voluntary stage may give way to a mandatory legislative stage if voluntary self-regulation fails.

The OECD, in a recent comprehensive report on online intermediary liability[95], identified four different models for ISP co-operation: "notice and takedown", which we have already discussed above in section 4; "notice and notice"; "notice and disconnection" or graduated response; and "filtering", which involves either (i) requiring ISPs to block access to websites implicated in copyright infringement, or (ii) examining Internet traffic in transit to subscribers of the ISP to see if it is infringing content (monitoring or "deep packet inspection") which may then lead to certain traffic (or certain sites) being filtered or blocked. We will examine "notice and notice" and graduated response in this section, and filtering in section VIII.

First, however, we will explain how alleged filesharers are typically identified by rightsholders (or their agents) so that notice of suspected infringements can be given to them by ISPs, or court orders sought for their identification. Such notice forms an essential part of both "notice and notice" and graduated response. The identification process is usually outsourced to private investigation companies, using various proprietary technologies, some of which will be described in brief below. The details of the process are vital for later analyzing *inter alia* if the privacy of the alleged filesharer is guaranteed, if evidence gathered is likely to be reliable and if the processes are cost-efficient and can scale to very large numbers of file sharers.

Detecting and identifying filesharers

Two recent cases have helpfully given us a great deal of information about the techniques used to identify filesharers by P2P detection agencies,the Irish case of *EMI v UPC*[96] and the Australian case of *Roadshow v iiNet.*[97] Here we draw on the testimony presented there as well as journalistic discussion in other media. In *EMI v UPC*, the judge outlined how a system called Dtecnet operated, which is employed extensively by rightsholders to identify P2P filesharers.

"DtecNet searches peer-to-peer networks for files being uploaded which are subject to copyright. On finding such a file, DtecNet requests the file. This is then transmitted to, and copied, by DtecNet's computer. It is integral to this process that basic information about the uploader from whom the work is being transmitted is obtained. The examples produced in Court show that the user's pseudonym and the IP address of the user appears together with the relevant time, date and identification of the copyright material. As part of this process, if the IP address was registered to an Irish internet service provider, Dtecnet identified how many sound recordings were being made available by that user on P2P software... I am satisfied from the evidence that the process is highly accurate. The activity log further transcribes the activity whereby the evidence is secured in a reliable format."[98]

Notwithstanding the judge's confidence in Dtecnet, he went on to admit that there are a number of well known ways to compromise its accuracy. First, proxy IP addresses can be

[95] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, draft report in preparation, 29 September 2010, paras 205ff (hereafter "OECD 2010 report").
[96] *EMI v UPC*, Irish High Court, 11 October 2010, [2009 no 5472 P] available at http://www.scribd.com/doc/39104491/EMI-v-UPC.
[97] Supra n 50.
[98] *EMI v UPC* at para 34.

used. Alternately, another computer can be used as proxy server (*UPC*, para 35). Secondly, P2P downloaders can use encryption. Although evidence was given in *UPC* that the encryption problem could be overcome (para 36), it was also admitted that around 20% of filesharing in Europe is now encrypted (para 28).

A second investigatory system discussed in *EMI* is Global File Registry (paras 38ff). This system uses a database of copyright music tracks supplied by the rightsholders (four million tracks) to identify by deep packet inspection (DPI) when a subscriber of an ISP is attempting to download a copyright track. If a track is matched, then the download is interrupted and if possible, the user is offered a link to purchase a legal version of the file, thus preserving rightsholder revenues. According to the judge in EMI, *"privacy is never infringed as the system simply reads numbers which identify the illicit nature of the transmission. The recording companies can never go through Global File Registry or any other system, discover who it is that is infringing their copyright materials. Only the internet service provider on being notified of an infringement through Dtecnet can find that out."*

Although the court regarded Global File Registry as having "*obvious advantages*" a clear problem exists as to the extent of the copyright tracks database needed to make it work. However the judge found it was not necessary to "*upload the entire discography of modern civilization deterring through interruption and diversion, the most widely shared musical tracks at a particular time is highly effective"*. In fact, the real remaining problem was that as technology currently stands, the system could not yet scale to meet the needs of an ISP with hundreds of thousands of subscribers.

Finally *EMI* discussed a third investigatory solution, CopySense, produced by Audible Magic, which was described as being used on the University of Florida campus to deter P2P filesharing. (It is also endorsed by the RIAA[99] and used *inter alia* by a social network specializing in music, MySpace). Like the system above, CopySense uses a database of some 3.7 million copyright works against which attempted downloads from P2P networks are matched. Unlike Global File Registry, however, it merely creates a violation notice when a match is made, which then restricts the user's access to the Internet – in other words, it acts as a form of instant notice and disconnection in respect of illegal P2P traffic. After such match had been made, the University or Florida, in the evidence given, then imposed a system of graduated response whereby successive violations lead to longer and longer suspensions from the college network until on the third violation the student was invited to a disciplinary tribunal. Again problems existed with scaling this type of solution from a university campus of c 50,000 students to an ISP with 150,000 users. It was also noted that the reported high effectiveness of the graduated response sanctions in the campus context depended on the ultimate possible sanction of expulsion from the university. On privacy, implications were reported to be similar to those in the Dtecnet system.

The judicial accounts in *EMI* (and also in *iiNet*, where Dtecnet was also used) show that effective technologies to collect the IP addresses of filesharers on P2P networks do exist, even if there are currently difficulties with scaling them to meet the needs of large modern ISPs with substantial client bases, and with making copyright work databases up to date and inclusive. Some groups have however been less sanguine about both the accuracy of these technologies, and the lack of associated privacy invasions. The Electronic Frontier Foundation, e.g., note two easy ways to spoof Audible Magic in their working

[99] See EFF report at http://w2.eff.org/share/audible_magic.php.

paper, similar to those cited in *EMI v UPC*[100]. More crucially the privacy implications at least for European data protection regimes are not without concern. We discuss this further at text after n 161, below.

"Notice and notice"

The idea of "notice and notice" is that an ISP receives notifications that its subscriber is alleged to be infringing copyright, and passes those warnings on to that subscriber. Notifications are usually received either from individual rightsholders or, more commonly, their trade bodies. They in turn acquire the IP addresses notified to ISPs via their agents, such as Dtecnet, using the techniques described above. No further action is required of the ISP. The point of the programme is part educational and part deterrent: to convince filesharers that they cannot hide from legal detection and thus to persuade them to turn to legal methods of obtaining music. Arguably it implies the existence of a back-up system of coercion ("stick") whether this is litigation against users, criminal prosecutions by the state or an eventual imposed "graduated response" regime. The ISP will take a given IP address and use it with other information such as timestamp to internally identify the subscriber, to whom warnings ("strikes") can then be forwarded. The identity of the alleged infringer is thus not necessarily disclosed to the rightsholder. The process of notification of alleged infringements, identification of users (which is near impossible to completely automate) and sending out warnings is costly, especially for smaller ISPs, and how such costs should be allocated between ISPs and rightsholders is a major controversy.

In Canada, such a programme has been in place since 2001 on a voluntary basis[101]. All the major Canadian carriers including Bell Canada, Telus and Rogers participate in the programme. The number of complaints received from rightsholders and thus passed on has grown considerably over time, and the industries making use of the scheme include software, music and film. Costs of sending out warnings to subscribers are born by ISPs and costs of notification by rightsholders, though in many cases such notification is automated and thus relatively cheap. Industry Canada in 2006 estimated the cost of one notification to be $11.73 CAN for large ISPs but as much as $23.73 CAN for smaller ISPs. Costs overall thus probably run into tens of millions of dollars. Canada is currently considering codifying the system and setting a maximum fee for rightsholder to pay per notification.

Finland is considering legislation for notice and notice, as of August 2010. IFPI Finland however questioned if the draft legislation would be effective given Finland's July 1, 2010 declaration that broadband access is a right for all citizens (discussed below). It was also questioned if new legislation was appropriate given total sales of music in Finland actually rose by 4.2% in first half of 2010.[102]

In the UK, a "notice and notice" regime of a sort was adopted voluntarily by the six major UK ISPs in 2008 in a limited period exercise preceding the introduction of more stringent modes of compulsion in the Digital Economy Bill (which became law in 2010)[103]. The idea was to trial notice and notice to see if it deterred filesharing or if it would then be necessary to move on to more stringent methods such as notice and disconnection.

---

[100] Ibid.
[101] See OECD 2010 report, paras 224ff in draft.
[102] See IFPI response to consultation by Finnish government on copyright reform in May 2010 (supplied by WIPO).
[103] See http://www.berr.gov.uk/files/file47139.pdf.

Unfortunately however, the legislation allowing for such was introduced before any detailed empirical results from the trials was made public, rendering the experiment fairly futile. "Stage 1" (ss 3-8) of the Digital Economy Act 2010 ("initial obligations") implements in hard law the model of notice and notice. Although the Act is now in force, notification and warnings are still not "live" since subsidiary regulations need to be approved. However "stage 2" of the Digital Economy Act ("technical measures", in ss 9-17) which allows for graduated response, is explicitly not to be introduced without clear evidence accepted by both Houses of Parliament that it is necessary to go further than warnings[104]. The new Chilean legislation[105] similarly seems to envisage a period of warnings before moving on to full graduated response.

The US is unusual in that there seems to have been relatively little governmental pressure placed on ISPs to take action or face compulsory legislation. This may be because of the high premium placed by US courts on freedom of expression in the Internet environment and the history of courts striking down legislation which seemed likely to impact on it. Nonetheless, since 2009, many US ISPs have participated in a voluntary notice and notice programme. One ISP estimated that it had sent 2 million such notices.[106] AT&T has developed an Automatic Customer Notification Service and argues the programme is effective in deterring filesharing.[107]

Despite the AT&T experience, there is no clear evidence so far establishing if such warning programmes alone are or are not sufficient to reduce filesharing. Studies have been contradictory: one in 2008 found that 7 out of 10 people said they would stop unlawfully downloading if they received a warning from their ISP,[108] but another UK study in 2009 found only 33% would stop after a warning.[109] Much seems predicated on the technical sophistication of the user (e.g. their confidence they can hide their IP address using a virtual private network, or similar), their belief that harsher sanctions may follow warnings, their risk taking characteristics (notably, the young are not easily deterred by possible future consequences) and whether legal alternatives are satisfactory and available, a topic discussed below at section X.

"Notice and disconnection" or graduated response

The regimes described in this section were pioneered by the French government as a policy of "graduated response", also known internationally as "three strikes and you're out".[110] The model follows up on "notice and notice" with the "stick" that after a designated number of warnings ("strikes") certain coercive sanctions are required to be applied by the ISP. In the leading French model, often known after the authority placed in charge as "HADOPI"[111], the number of warnings is indeed three, but this is not necessarily the case.

---

[104] DEA 2010, s 8.
[105] See "Chile breaks new ground in regulating IP liability", *WIPO Magazine*, 3/2010, June 2010.
[106] OECD 2010 report, fn 229 in draft.
[107] Comments of AT&T, reported in OECD Report 2010, n 211 in draft.
[108] Study by Digital Entertainment Survey, 2008, cited in http://arstechnica.com/tech-policy/news/2009/06/stern-letters-from-isps-not-enough-to-stop-p2p-use-after-all.ars.
[109] Cited in ibid.
[110] The first notices or "strikes" were finally sent out under HADOPI on September 21, 2010, over a year after the law originally passed (see http://www.techdirt.com/articles/20100921/14423311097/hadopi-begins-issuing-tens-of-thousands-of-notices-for-infringement-in-france.shtml).

[111] French *Loi Olivennes*, or "HADOPI" law, passed on second attempt by the French legislature on 13 May 2009. For a critical examination, see Geiger, C), "Honorable Attempt but (ultimately)

[Footnote continued on next page]

Similarly "notice and disconnection" implies that the only sanction is complete loss of Internet access, whereas in most implementations this is in fact seen as a last resort. Yu[112] accordingly prefers the term "graduated response", which will be adopted hereafter.

The French model has been significantly promoted by the IP industries throughout the globe and legislation has now been passed installing it or similar in the UK,[113] Republic of Korea[114], Taiwan Province of China,[115] Chile[116] and New Zealand.[117] Hong Kong Special Administrative Region of China[118] has begun the process of legislating in this direction but not yet decided whether to proceed with it. Many other significant economies such as Japan are also considering whether to go down this route[119]. Some countries however such as Germany[120] have clearly come out in opposition to graduated response, as has the European Parliament since April 2008[121], citing fears as to the effect on freedom of speech, privacy and due process. In Spain[122], as discussed below, in the face of much judicial and public controversy, legislation has been introduced allowing for website blocking[123], but not for user disconnections.

[Footnote continued from previous page]

Disproportionately Offensive against Peer-to-peer on the Internet (HADOPI) – A Critical Analysis of the Recent Anti-Filesharing Legislation in France" (2011) IIC 1 (in press).

[112] Yu P "The Graduated Response", supra n 87.

[113] UK Digital Economy Act 2010, ss 3-18. Note that the DEA provides a list of possible responses, including traffic slowing (throttling) and filtering, with "suspension" of the account (so far of uncertain duration) to be used as a last resort for repeat infringers.

[114] See details at http://hurips.blogspot.com/2010/03/three-strikes-rule-sleeping-for-seven.html. The legislation was passed in July 2009. "The South Korean regime provides that under Article 133*bis* of the Korea Copyright Act, the minister in charge may, after deliberation by the Copyright Commission, order an ISP to take measures to suspend for a period of no more than 6 months an account provided by the corresponding ISP for a user when the user has been warned at least three times by the Minister in connection with unauthorized reproduction or transmission of the copyright infringing material." See statistics as to actions taken under the South Korean regime at http://hurips.blogspot.com/search/label/Three%20Strikes%20Rule. Note also that the Korean Copyright Commission may recommend, but not demand, the suspension of a user account on less than three strikes. By end July 2010, a year after the system was introduced, no individual subscriber had yet been suspended.

[115] See *Taiwan International Intellectual Property Alliance 2010 Special Report on Copright Protection and Enforcement*, 18 February 2010 at http://www.iipa.com/rbc/2010/2010SPEC301TAIWAN.pdf. Legislation was adopted April 2009 to implement "graduated response". However regulations made in November 2009 dealt only with notice and counter-notice, and have not yet prescribed how ISPs are to go further than this. The report indicates unwillingness by ISPs to negotiate a code of conduct on this for fear of losing safe harbors from liability.

[116] Supra n 105.

[117] New Zealand Copyright Act 1994, ss 92A and B as amended in 2009 (amendments frozen indefinitely following public opposition –see http://www.nbr.co.nz/article/entire-copyright-act-be-scrapped-101820).

[118] See IFPI briefing note, "ISP Co-operation", July 2010.

[119] Information derived from IFPI note, "ISP Co-operation – Update", July 2010.

[120] See http://arstechnica.com/tech-policy/news/2009/02/germany-walks-away-from-three-strikes-internet-policy.ars, 6 February 2009.

[121] See e.g. http://www.iptegrity.com/index.php?option=com_content&task=view&id=173&Itemid=9.

[122] See 'Three-Strike' Off Anti-Piracy Agenda in Spain", June 22, 2009 at http://www.billboard.biz/bbbiz/content_display/industry/e3i8071e0d9c25cb6b876d3771fb7e3d102.

[123] See "Spain Fast Tracks P2P Site Shutdowns", Torrent Freak, 8 January 2010 at http://torrentfreak.com/spain-fast-tracks-p2p-site-shutdowns-100108/.

In terms of hard EC legislation, the Telecoms Framework reforms passed in October 2009[124], although strictly not about copyright law at all but about telecommunications regulation, were widely believed to have been designed in part to lay a possible foundation for EC member states to introduce or justify graduated response laws[125]. In response however, an amendment known as the "Internet Freedom" clause was added with the support of the European Parliament, which now states that

3a. Measures taken by Member States regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.

"Any of these measures regarding end-users' access to or use of service and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are *appropriate, proportionate and necessary* within a democratic society, and their implementation shall be subject to *adequate procedural safeguards* in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of *presumption of innocence and the right to privacy*. A *prior fair and impartial procedure* shall be guaranteed, including the right to be heard of the person or persons concerned subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to an *effective and timely judicial review* shall be guaranteed." [126] [italics added]

This provision must be transposed into all EU states by May 2011. Note that although the sentiments of due process are strongly expressed, in practical terms this provision guarantees only the right to access to the courts on appeal ("review") not *before* warnings are notified, or even possibly before measures such as disconnection are implemented. Accordingly it appears currently that both HADOPI (albeit as modified by the French Constitutional Court) and the UK DEA may pass the "Internet Freedom" test.

As noted above, graduated response may also be imposed without legislation. In Ireland, a variety of media companies sued Eircom, a leading Irish ISP, for culpability in copyright infringement by its subscribers. Eircom settled in January 2009, and as a result agreed to impose a system whereby they would suspend the account of the subscriber after three warnings as a sanction for breach of the subscriber contract. Eircom agreed initially to process complaints involving c 50 IP addresses per week, as a pilot to test if the process

---

[124] See unofficial consolidated version at http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

[125] See report commissioned by Open Rights Group, Bradshaw S and Edwards L "Analysis of Recent Amendments to the EC Telecoms Package: Do They Provide a Legal Basis in Europe for 'Three Strikes and You're Out' Anti Filesharing Laws?," 12 November 2008 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1300662.

[126] See report at http://arstechnica.com/tech-policy/news/2009/11/eu-adopts-internet-freedom-provision-on-net-cut-offs.ars and discussion at http://www.laquadrature.net/wiki/Telecoms_Package_Amendment138_compromise_20091105. A critique of what was earlier known as "amendment 138" can also be found at Edwards L and Bradshaw S, supra n 125.

worked satisfactorily. The agreement was confirmed as legal in terms of data protection law by the Irish High Court in April 2010[127]. However in October 2010, when a similar media consortium sued a further Irish ISP, UPC[128], the same judge found against the plaintiffs and held that despite considerable dislike of piracy, under Irish copyright law he had no power to order UPC, as plaintiffs sought, to block certain sites such as the Pirate Bay, nor to monitor and filter the traffic received by its subscribers. *EMI v UPC* leaves the *Eircom* settlement in a state of some uncertainty as of the time of writing, and it is also not clear if content industries will launch suits against further Irish ISPs.

Finally, subject to local laws, an ISP may choose to voluntarily implement a graduated response scheme. Indeed, this is often done by internal university regulations on many campuses where the university acts as ISP for students. It is likely that some of the US ISPs which voluntarily adopted "notice and notice" schemes have followed up repeated warnings with threats or actually terminating user accounts on repeated infraction[129].

Advantages of graduated response

A number of advantages are claimed for graduated response systems. Many of these spring from a first assertion by the content, and especially, music industry that they cannot simply sit back and let revenues fall, and that conventional forms of enforcement of IP rights have failed, or if not yet at failure point, are unpractical or unhelpful. This primary argument is, if accepted, the axiomatic basis for many others, but acceptance would require a close examination of economic evidence which is outside the remit of this legal, not economic, report[130]. *If* accepted as axiom, it follows that "three strikes" has a number of connected advantages for rightsholders.

First, and above all, graduated response is seen as effective, speedy and cheap compared to court based justice. Strowel, a much quoted expert, has noted that it is to filesharing what the UDRP has been to cybersquatting: a speedy and effective procedure, with limited costs, focusing on straightforward infringement involving basic facts, rather than more nuanced cases involving e.g. copyright exceptions[131]. Graduated response is seen as a more effective deterrent than recourse to the courts. For example, the UK's introduction of the Digital Economy Act was predicated on the assertion in the Impact Assessment that 70% of filesharers would stop illicit sharing of music after one or two warnings. The French system was also introduced in the explicit belief it was both effective and proportionate. Both the UK and French systems have now been validated by

---

[127] *EMI v Eircom* [2010] IEHC 108.
[128] *EMI (Ireland) Ltd et al v UPC*, supra n 96.
[129] See OECD 2010 report, n 221 in draft; note AT&T claim they will not disconnect subscribers without court order merely on multiple allegations of infringement.
[130] The figure in the UK Impact assessment, for example, was questioned in the judicial review of the Act – see BIS DEA 2010, Impact Assessments, April 2010, at http://interactive.bis.gov.uk/digitalbritain/wp-content/uploads/2010/04/Digital-Economy-Act-IAs-final.pdf and infra n 132. The judge accepted that the figure was based on a survey carried out in 2008, while another survey in 2009 showed that only 33% of users would stop infringing if there was a threat of sanctions such as disconnection (para 255). Although the review resulted in failure for the claimants, this was not because the Impact Assessment was held to be accurate, but because the judge's concern was whether Parliament had acted reasonably in believing the estimates with which it was presented (para 256). His overall view was that "some of the alleged costs were little more than guesswork" (para 262).
[131] See Strowel A ,"Internet Piracy as a Wake Up Call for Copyright Law Makers – Is the "Graduated Response" A Good Reply?"(2009) 1 WIPO J. 75 at 77-80. See discussion at n 185 and text following of the alleged cheapness of the system, however.

their national courts as a proportional response to the problem of filesharing[132].

Second, it is unpleasant and unhelpful for the content industries to be forced to sue their own customer base. Graduated response is, in particular, seen as less punitive and alienating of the customer base, given the emotive history in the US of copyright suits involving disproportionately massive and punitive copyright damages[133]. In EU and other countries where such punitive damages are not available for civil claims, however, this argument has less weight.

Thirdly, graduated response is seen as educational in a way ordinary court based legal sanctions are not. By giving a number of warnings before "sentence" is passed, the filesharer is, it is alleged, encouraged to reform, with penance not punishment the aim, and in aggregate, the hope is that a social norm currently extant in the youth demographic where filesharing is encouraged, will be replaced with one where it is frowned upon as amoral behavior[134]. A further development is that graduated response systems, it is hoped, can encourage the user to migrate to legal online filesharing services (at least, where the product they seek is available in this way). The Recording Industry of New Zealand's Chief Executive, speaking to support the proposed NZ graduated response law, also emphasized that warnings have the advantage of not being retrospective. "There will no move to seek redress for past illegal behavior, only a request that the user does not break the law in future"[135]. For this reason, it is specified in the UK draft Initial Obligations Code to the DEA that a warning has a "shelf life" of only a year and cannot count as a strike thereafter. Without such a safeguard, threats of suspension etc could hang over the user like a "digital guillotine"[136] for most their life.

Fourthly, even if a small hard core of recidivists remains who are immune to persuasion and education, and not deterred by the fear of disconnection and other sanctions, they will find downloading progressively harder as the number of uploaders "seeding" P2P networks diminishes.[137] In any case it is often asserted that the aim of graduated response is not to stamp out P2P filesharing, but merely to reduce it in its unlawful form to a level where the content industries can survive in their current form, and artists receive a reasonable return on their creativity and labor sufficient to incentivize further cultural production.

Fifthly, it is argued that users, too, benefit from graduated response solutions. Following on from the third point above, Anderson notes that, unlike in court based suits, they are

---

[132] The French system was passed by the Cour Constitutionnel after changes were made following an earlier finding it infringed basic due process rights. The UK system was also challenged as disproportionate having reference to the EU Charter of Rights, general principles of EC law and the ECHR, but this argument was rejected by the judge in the judicial review of the DEA: see *R v BT/Talk Talk, [2011] EWHC 1021 (Admin), 20/4/2011.* An appeal may well follow. (Hereafter "DEA judicial review" - this case was reported as this report was finalised so although attempts have been made to include salient points, it cannot be referred to in detail.)

[133] See Anderson N "IFPI: "Three strikes" efforts hit worldwide home run." At http://arstechnica.com/tech-policy/news/2008/08/ifpi-three-strikes-efforts-hit-worldwide-home-run.ars.

[134] See Yu, n 87 at 1381.

[135] See Smith C, "Why NZ needs graduated response now", July 2010 at http://www.ifpi.org/content/library/Campbell_Smith_100730.pdf.

[136] See Patry W, infra n 162 at 14.

[137] Yu, supra n 87, at 1382.

presented with multiple chances to stop filesharing before suffering any sanction.[138] He along with Sookman and Glover[139] also emphasize that graduated response is respectful of user privacy in a way that may be superior to court based justice, and that "graduated response systems are not intended to be anti-consumer or heavy handed"[140]. Whereas a court suit will invariably start with the identity of the filesharer being sought and revealed to the rightsholder plaintiff, in graduated response, the personal details of the alleged filesharer need not be shared with rightsholder or law enforcement bodies. Only the ISP can connect the filesharer's name to the alleged infringement since it is they who pass the warnings on[141].

Anderson also emphasizes that the protection offered by graduated response will encourage music unions such as the RIAA to release more "legal" offerings to online services such as last.fm, iTunes and Amazon, and to be more open to the idea of blanket licensing, all to the benefit of users. It has to be asked though if this is not rather cart before horse: if a comprehensive and competitive market for legal online music services had developed earlier, some argue, than unlawful filesharing would not have been a necessary evil for music lovers. There is a fuller discussion of the role of the market and legal online music services at section X below.

Finally, it is argued that ISPs also benefit from graduated response[142]. Anderson argues that ISPs will gain by the reduction in the use of their bandwidth by P2P filesharers[143]. In practice, with or without graduated response, most ISPs already employ traffic management to reduce or slow traffic to heavy downloaders, but Anderson argues that some (US) ISPs are limited in what they can do in this direction by local limits on network discrimination imposed by telecoms regulators (see e.g. the FCC Comcast[144] decision in the US). For them, graduated response will be a "tremendous new tool"[145]. The worth of this argument depends on what attitude is taken towards net neutrality: a heated and controversial subject at the best of times, beyond the remit of this report, and with obvious differences in views again between the US and EU. It should be noted that ISPs have largely, despite these cited advantages, been opposed to graduated response schemes, mainly on grounds of costs (see below at n 185 and following text) – notably, the UK DEA judicial review claim was brought by two major ISPs, BT and TalkTalk. Although the

---

[138] Anderson, supra. It should be noted however that as the vast majority of accusations of filesharing are settled rather than going to court, this distinction between the two systems is not entirely plain. Note also the discussion below of the accuracy of allegations of filesharing, both in court based justice and in graduated response.

[139] See Sookman B and Glover D "Graduated response and copyright; an idea that is right for the times", *Times*, January 20 2010, at http://www.barrysookman.com/2010/01/20/graduated-response-and-copyright-an-idea-that-is-right-for-the-times/.

[140] Ibid.

[141] Note however concerns expressed that ISPs are often not well regulated environments and that databases of alleged user infractions may be subject to hacking or other security breach, either deliberately or accidentally – as was shown vividly in the ACS-Law incident (see n 92 supra). Note also the detailed discussion below in section VIII of how some versions of graduated response involving filtering, monitoring or blocking endanger not only the privacy of users alleged to be filesharers, but of all Internet users, innocent or guilty.

[142] See Anderson N, "No more lawsuits: ISPs to work with RIAA, cut off P2P users" at http://arstechnica.com/tech-policy/news/2008/12/no-more-lawsuits-isps-to-work-with-riaa-cut-off-p2p-users.ars.

[143] See also Yu, supra n 87, at 1385-7.

[144] See http://arstechnica.com/old/content/2008/08/fcc-spanks-comcast-for-p2p-blocking-no-fine-full-disclosure.ars.

[145] Ibid.

judicial review claim largely failed, the ISPs did succeed in securing a reduction (albeit small) in their total contribution to costs, in that they were exempted from sharing the costs of establishing an appeal body to oversee disputed warnings or technical measures[146].

Particular systems have added "carrots" to offset the "stick" of disconnection or suspension, and this may lead to further advantages for users. The main current example is the French
Loi Olivennes, discussed above, where the French government agreed with the media industries a number of concessions in return for graduated response, including the end of non-interoperable DRMs for French music catalogue, a narrower window between the release of media worldwide and their release in the French market, and a commitment to release virtually all French language media product to video on demand. Most remarkably, the French government has in its turn offered not only a reduction in the rate of VAT on cultural goods to the industry, but also made a gift to every *user* who downloads 25 Euros of product from legal online music services of a 25 Euro voucher on top. Reportedly however, very few French users know of this and there has not been much uptake, and it remains uncertain how the 20 Million Euros or so this requires is to be funded[147]. Also, as above, it could be suggested that these market "carrots" should have been made available anyway in a functioning competitive marketplace. Despite these qualms, Jondet asserts that because of this combination of carrot and stick, the French system is the "Rolls-Royce" of graduated response.

One final advantage of graduated response may be that if it is successful, it may become a model for other digital products facing piracy or counterfeiting online. Anderson suggests that graduated response may be adopted by e-book vendors and perhaps even the makers of crochet patterns[148].

Problems with graduated response

Due process and public oversight

A key aspect of graduated response is that sanctions are in principle applied by an automated administrative process rather than via the ordinary courts. Only in this way can it scale to deal with thousands or even millions of filesharers. As a civil infringement, claims as to domestic copyright infringement would normally be processed via the civil courts or tribunals with conventional guarantees of due process. The arguments for graduated response are however that volume litigation against users is a failed strategy, and is counter-productively slow and expensive as well as bad for public relations. Regardless of the worth of these claims, the right to due process guaranteed by various international and domestic human rights instruments, notably the European Convention on Human Rights, Art 6, cannot be disregarded.

Due process embraces issues such as the right to a fair hearing, standards of evidence, presumption of innocence, rights in some cases to legal assistance or financial aid to obtain such, oversight, transparency, accountability and appeals. All of these raise issues in the context of a reutilized bureaucratic process, transacted between rightsholders and

[146] Supra, n 132.
[147] See presentation by Jondet N on the French graduated response system, Scottish-French Association, April 2011, Edinburgh. Jondet's arguments can be found also in working paper form at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1664509.
[148] Supra, n 142.

ISPs, rather than a judicial hearing where the person accused of infringement has rights to a presumption of innocence, to argue their case in person or via legal agent, examine evidence and obtain legal advice. In regimes of graduated response, therefore, it is crucial to know how far a public authority such as a court, tribunal or independent regulator is involved in overseeing the process is fair, and when and how opportunities will arise to seek the intervention of such an authority, or at least, get legal advice.

In the UK Digital Economy Act 2010, sanctions, it seems, will be applied after a number of warnings are sent (the exact benchmark still to be determined in regulations) without, initially at least, any judicial intervention. There is thus no independent check in the early stages on the possibilities that rightsholder or ISPs have made an error either as to fact (e.g., mistaken identification) or of law (e.g., material downloaded was in fact in the public domain, subject to fair dealing, etc). By contrast, the French HADOPI regime, after a history of challenge in the French constitutional courts, now includes at least some judicial oversight from the start, though it is not yet clear how far this will be really effective to safeguard civil rights and due process[149]. The Spanish have also agreed that legislation for blocking of websites (not for disconnection of users) cannot proceed without some kind of prior public or judicial investigation[150]. It is not clear how far there is any intervening adjudication in the South Korean or other relevant systems, although their copyright commission has a role; and of course, where notice and disconnection has been imposed by private action or settlement as in the *Eircom* case, or voluntarily adopted as perhaps on US campuses, there is very unlikely to be a role for public or judicial oversight.

A controversial aspect of the UK DEA experience especially, is that the legislation was passed in principle as an extremely sparse framework, with no detail available concerning timing of and notification of appeals, access to legal aid or advice, standards of evidence, or relevant grounds for appeals (e.g. fact, law, and procedural injustice). Such rules are still being elaborated as of the time of writing for the Initial Obligations Code (IOC) [151] with rules as to the "technical measures" of the Act still yet to be investigated at all. This issue, that "the devil is in the detail", is very likely to recur in future legislation for many countries dealing with such a complex problem, and has already led to leave being granted for a judicial review challenge to the legality of the DEA by Talk Talk, a UK ISP, and other plaintiffs on the grounds (among others) that the Bill failed to meet European law consultation standards, and that the regime may not be a proportionate response to the goal of enforcing IP[152]. For example, in the DEA it currently appears that rights to appeal against "strikes" or warning may be fairly limited until sanctions are eventually applied some while later, which may mean opportunities to combat false or erroneous evidence may be lost, e.g. technical data may have been deleted. This matter was not clear in the primary legislation.

Finally there is a question of what might be called "equality of arms". Under graduated response, typically rightsholders can make allegations as to infringement without redress

---

[149] See http://www.techdirt.com/articles/20100920/11092911078/leaked-report-admits-that-hadopi-first-strike-accusations-won-t-be-reviewed-for-accuracy.shtml.

[150] Indeed as of 21 December 2010, it seems website blocking in Spain is at least temporarily on hold altogether: see http://www.zeropaid.com/news/91654/us-pressure-backfires-as-site-blocking-is-voted-down-in-spain/.

[151] Draft Initial Obligations Code to the DEA, published by Ofcom 28 May 2010, can be found at http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/.

[152] *Application by BT plc and Talk Talk Telecoms Group v Secretary of State for BIS*, Statement of fact and grounds available at http://www.talktalkblog.co.uk/download/sfg-final.pdf; decision to grant leave not officially reported except on proportionality ground; see news report, *Guardian* , 10 November 2010 at http://www.guardian.co.uk/technology/2010/nov/10/bt-talktalk-digital-economy-act.

if they have made an error (whether through malice or negligence or not). In the US DMCA, as noted above, provision is built in for penalties where a rightsholder makes false notifications of copyright infringement as part of NTD, and such penalties also exist in UK law for abusive trade mark claims. Such a parallel provision might also be appropriate for notice and disconnection given the severity of the sanction on an innocent user.

Error

Standards of evidence are a general problem in a graduated response regime. Everything depends on the quality of the processes by which (a) IP addresses are harvested (see above, *Detecting and identifying filesharers*) and (b) by which they are then matched to the names of subscribers of an ISP. The Online Rights Group (ORG) in their response to the draft Initial Obligations Code to the UK DEA 2010, argued that standards of data handling and evidence collection are of "*utmost importance. If the means of obtaining evidence and the standard of evidence on which copyright infringement reports are based is not robust, potentially thousands of subscribers will be [penalized] even though no credible evidence has been established*" [153]
Practice on how filesharers are identified varies across different private companies and different countries. Researchers at the University of Washington showed that one approach to identifying file sharers commonly employed in the US (i.e. record the IP address of anyone who appears to be offering a specified file on Bit Torrent, and then use it to identify user) was deeply flawed. The researchers joined torrents to monitor them, but neither downloaded nor uploaded any copyright work, and still received legal notices accusing them of infringing[154]. In Europe, the approach has generally been more careful. Monitoring companies ask for files and also actually fetch sections of the shared file, so they can then confirm that they are indeed part of a copyrighted work. This raises another issue that by so doing, the monitoring companies may themselves be breaking the law, unless they have clear permission from rightsholders to download – an issue discussed in *iiNet*[155]. If criminal charges are involved, there might also be evidential issues such as whether it is appropriate for private companies to do this investigation.

A number of technical errors can then occur at the identification stage, when the ISP is asked to match data given to named subscriber. Timestamps may be inaccurate, records may be incomplete, humans may make transcription errors and so on. In the view of Richard Clayton, a security expert at the Cambridge Computer Lab, "Most of the time this will work just fine, but occasionally it will all go pear-shaped"[156]. One key point is that if IP addresses are widely spoofed to avoid detection, then innocent persons assigned such a spoofed IP address by their ISP are likely to find themselves wrongly accused of filesharing. Finally if filesharing is conducted via mobile networks, as is increasingly

---

[153] Online Rights Group *Response to Consultation on Online Infringement of Copyright and the DEA2010,* 30 July 2010, at http://www.openrightsgroup.org/assets/files/pdfs/ORG_initial_obligations_code_response_2.pdf.
[154] See "Tracking the trackers: Investigating P2P Copyright Enforcement" at http://dmca.cs.washington.edu/. In one famous incident during this research, a printer attached to a P2P network, with its own IP address, was sent a cease and desist letter. Interestingly, the US courts have just declined to make a subpoena order against an ISP to identify an alleged filesharer on the basis that an IP address is not a person: see http://torrentfreak.com/ip-address-not-a-person-bittorrent-case-judge-says-110503/, 3 May 2011.
[155] At paras 326 ff.
[156] Private email, November 2010, and see http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html and evidence given by Richard Clayton to the DEA judicial review on behalf of Open Rights Group, intervening, see http://www.openrightsgroup.org/assets/JK1RC.pdf.

possible, then collecting the IP address alone is not enough for identification, and this problem may occur on fixed lines too, with the move from IP v 4 to IP v 6[157].

Even if both data collection and IP address matching are error free, it is quite possible for evidence of infringing drawn solely from IP addresses to be misleading. Erroneous allegations may be made that a subscriber A was downloading because his wireless network is being used by another party B "piggybacking" on it – either because, as is often the case, the wireless router has not been secured through ignorance or inertia, or because its security has been hacked. Similarly a subscriber A's computer may be infected with malware causing it to be controlled remotely (as a "zombie" or "bot") and used to download (or upload) for the bot controller B unknown to A. Finally, of course, IP addresses only identify the subscriber and not the person who actually used the Internet connection at that physical address. Illicit downloading might actually have been done by a child in residence, a friend visiting, or a variety of people with access (e.g. cleaners, tradesmen) especially when a wireless network is in place, and yet in each case the incriminating IP address would belong to the person who was the official subscriber to the account, regardless of their level of knowledge or legal or factual control over the actual infringer. It is by no means clear that in most legal systems a parent is habitually held responsible for a child in either civil or criminal law (let alone a child's friends), so a statutory or judicial change of this nature seems to require particular justification[158].

It is also worrying that many administrators, policemen and judges will not always understand these technical niceties of arguments about IP addresses, data collection protocols and computer insecurity. In the debates in the UK House of Lords on the Digital Economy Act, e.g. Lord Young said the following:

"Clearly, it will be important that the appeals body set up by the code should be capable of determining whether a copyright infringement notice has been properly generated, so it will require some technical knowledge and expertise of, for example - I stress the importance of this - whether an infringement has occurred; whether the time and date stamp is accurate; whether the IP address was correctly captured and recorded; whether it has been properly handled by the ISP; and whether the subscriber has been properly identified from the IP address and the time and date stamp provided. As I have said on a number of occasions, that means an audit trail, a validated evidence base, not incomplete information. No system is infallible, but we are talking about serious evidence that can be technically validated and proved and that has to be chronologically correct".[159]

Yet further issues exist as to the security of the data on which warnings or allegations are based, when it is held in the hands of either the rightsholder or its agent, or the ISP. It is easy for example for an employee of an ISP to undetectably tamper with such evidence. Non malicious security lapses are also an issue. In the UK, there has been considerable concern following an incident in September 2010 involving the law firm ACS-Law which, acting as legal agent for various rightsholders, acquired via court orders from ISPs, sensitive personal data allegedly identifying certain persons as filesharers (including in some cases, as downloaders of pornographic films). A combination of a DDOS attack by

---

[157] See further http://www.lightbluetouchpaper.org/2010/01/14/mobile-internet-access-data-retention-not/.

[158] Of course it may be the child (say, above 18 and the household accountholder) who is held responsible for the parent's downloading; an even less typical scenario for vicarious responsibility.

[159] See Hansard, HL Deb, 20 January 2010, c1026), at http://www.theyworkforyou.com/lords/?id=2010-01-20a.1009.3&s=evidence+speaker%3A13450#g1026.3.

anonymous actors, and apparent poor security practices by ACS-Law disclosed this data to the world, with as yet uncertain personal, economic and legal consequences[160].

It is crucial therefore that any system which gathers evidence to generate copyright infringement warnings must be robust, accurate and transparent to public and expert technical audit. Such standards will be hard to maintain and scrutinize given the anticipated scale of graduated response if it is to have a serious deterrent effect. Patry warns that

"Faced with the receipt of hundreds of thousands or millions of such notices under graduated response, ISPs will simply pass the notices along to customers who will be presumed guilty. there is no guarantee or even reason to believe ISPs' customers will be able to get service restored due to errors or that they will have the ability to prove their use was lawful as fair use"[161].

Fundamental rights: privacy

We noted above how data, such as IP addresses and types of files requested, is harvested by systems such as Dtecnet and Audible Magic's CopySense. Although the judge in *EMI v UPC* defended these systems as not privacy invasive (above, n 128), this claim has been questioned by a number of commentators. Under the EC Data Protection Directive (DPD) stringent restrictions are placed on those ("data controllers") who control the processing of "personal data". Whether IP addresses collected in the context of P2P investigations are "personal data" is thus vital to deciding if the DP regime's safeguards are invoked.

Under Art 2 of the DPD, personal data includes "any information relating to an identified or identifiable natural person (data subject)". Peter Hustinx, the European Data Protection Supervisor, and the Art 29 Working Party, which provides guidance on interpreting DP law across Europe[162], have both strongly taken the position that since "*an IP address serves as an identification number which allows finding out the name of the subscriber to whom such IP address has been assigned*", it is clearly "*relating to*" the activities of an identifiable individual (the holder of the IP address), and thus must generally be considered personal data[163].

Even in the UK, which is regarded as having implemented a weak version of the DPD in this regard, IP addresses will be considered to be "personal data" if they are data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, *or is likely to come into the possession of*, the data controller [emphasis added]. Thus even under a UK style interpretation (which has also been espoused by companies like Google[164]) in assessing

---

[160] See http://www.bbc.co.uk/news/technology-11418970 and supra n 92.
[161] Patry W, *Moral Panics and the Copyright Wars* (OUP, 2009) at 13.
[162] See e.g. Art 29 Working Committee *Opinion 4/2007 on the concept of personal data*, 20 June 2007, WP 136.
[163] See e.g. 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) at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf.
[164] See "Are IP Addresses "Personal Data"?", Peter Fleischer's blog (Chief Privacy Officer of Google), February 5 2007. The view that IP addresses used to identify filesharers should be regarded as personal data was seemingly accepted by all sides in the DEA judicial review (para 157).

the DP implications of a system like Dtecnet, it would have to be considered if it was likely that a living person could be identified from the data held by rightsholders (IP address etc) *taken with* other data *likely* to come into their possession. Given the widespread availability of mandatory court orders to obtain personal details from ISPs once an IP address is known, as well as the possibility of voluntary arrangements (as in *Eircom*), "likeliness" cannot be dismissed. Accordingly, it has to be considered if the collection of IP addresses, presumably typically without the consent of the data subjects, is legal under DP law, *if* IP addresses are assumed to be personal data, or potentially to become personal data at some point in the detection, matching and notification process[165].

Consent is, of course, not the only ground that can justify the processing of personal data; other grounds exist, and processing can be legitimate if it is in the data processor's "legitimate interests", so long as there is not "prejudice to the rights and freedoms or legitimate interests" of the data subject[166]. That final sub clause however may be troubling to a European court[167] and in particular in *Promusicae v Telefonica*[168], the European Court of Justice has already emphasized those privacy rights of data subjects do not necessarily defer to rights of property such as those being asserted by copyright holders via the Infosoc and other copyright related Directives.

Finally, processing might be justified without consent on the grounds of detection and prevention of crime (which exempts controllers from many, though not all, parts of the DP regime). However not all copyright infringement, of course, involves criminal charges, nor do all EC countries allow private parties, rather than public law enforcement agencies, to plead this exemption – Italy e.g. has already refused to allow private P2P detection agencies to take advantage of this exemption[169].

What becomes clear is that despite the repeated assertions of Justice Charlton in not only *EMI v Eircom,* discussed above, but also *EMI v UPC,* that privacy is not compromised by IP address harvesting and identification methods, in fact across different jurisdictions, this issue seems to be controversial. In Germany, for example, following the Constitutional Court's rejection of the harvesting of personal data for the purpose of investigating civil wrongs[170], the government apparently rejected the idea of legislating for graduated response on the grounds that it would unreasonably infringe the privacy of citizens[171].

Rules relating to interception of communications may also be relevant. IP address harvesting and packet sniffing may potentially be accused in EU states of being illegal interception under arts 5 and 6 of the Privacy and Electronic Communications Directive

---

[165] See generally Coudet F and Werkers E "In the Aftermath of the Promusicae Case – How to Strike the Balance?" (2010) 18 IJLIT 50.
[166] DPD, Art 7.
[167] In Italy, a court has already found that the processing of IP addresses by a private company acting as agents for rightsholders was illegal, since it could not be based on any legitimate grounds under the Italian DP Act ("Pippermint" case, 28 February 2008, cited by Coudet and Werkers, supra, at n 34.)
[168] *Promusicae v Telefonica* C-275/06 Judgment (OJ) OJ C 64 of 08.03.2008, p.9 in which the court asserted that although copyright enforcement was a goal backed by EC law, it nonetheless did not necessarily overrule the rights to privacy of alleged file-sharers, and instead a balance had to be struck according to human rights jurisprudence. The case itself concerned whether it was legitimate under EC law for a national Spanish court to demand that identifying data be handed over to rightsholders claiming infringement.
[169] See supra n 167.
[170] See German Federal Constitutional Court, 11 March 2008, 1 BvR 256/08.
[171] Supra n 120.

(PECD), which forbid interference with the confidentiality of communications as well as the retention of "traffic data". It is possible that Art 15(1) of the PECD may provide some justification for non compliance with arts 5 and 6, but as the grounds for exemption are limited in essence to national security, investigation and prevention of crime, and investigation of "unauthorized use of the electronic communication system", again it is not clear if civil infringement of copyright would justify derogating from Art 5 or 6. Any such derogation would also have to be "necessary, appropriate and proportionate within a democratic society", a familiar formulation to balance state interest against fundamental rights in European jurisprudence. Coudert and Werkers argue[172] that the effect of *Promusicae* may be that Art 15(1) can be widened to allow derogations from arts 5 and 6 on the ground of protecting private property rights i.e. copyright, on the last ground cited above, but this remains a grey area.

Finally, this is by no means only an EU issue: Paul Ohm[173] has similarly questioned the legality of surveillance carried out by rightsholders and ISPs under US laws against wiretapping, especially the Electronic Communications Privacy Act (ECPA). Vincents[174] also suggests liability may arise under common law US cases on online trespass such as *Bidder's Edge*[175] and *Hamidi*[176].

Fundamental rights: freedom of speech, access to the Internet

The ultimate sanction in graduated response is usually some form of disconnection from the Internet, although typically of limited time (e.g. "suspension" in the UK DEA 2010; a maximum of a year in HADOPI). Such sanctions can be imposed simply in relation to the connection via one ISP (the approach currently taken by the DEA, for example) or may conceivably involve being placed on some kind of national ISP "blacklist" which would more closely approximate a true ban from the Internet (which is what HADOPI attempts to do). In both cases, but more critically in the latter, issues arise as to whether this now fundamentally impairs in the information era rights of freedom of expression, or more generally, of access to knowledge, or to "essential services". Globally, free speech is protected by Art 19 of the Universal Declaration on Human Rights; and within the European Convention on Human Rights, Art 10, and it is widely acknowledged that access to the Internet – digital inclusion – is now a crucial part of that right. It can be argued that graduated response sanctions, even with a blacklist, do not infringe freedom of expression because they do not cut off all access to the Net: cybercafés may be used, or connections at libraries or schools[177]. But the more restrictions are placed on freedom of digital expression, the harder it will be to see such as legitimate and proportionate to the goal of controlling filesharing, especially if other alternative solutions for the IP industries are possible, such as levies or legal alternatives, as explored below, section X.

---

[172] Supra n 166, p 64.
[173] Ohm P, "The Rise and Fall of Invasive ISP Surveillance", (2009) Univ of Illinois Law Review 1417 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344>.

[174] Vincents O B, "The Tracking of P2P Copyright Infriengements and the EC Personal Data Directive"2008 16 IJLIT 270.
[175] *eBay v Bidder's Edge* 100 F.Supp.2d 1058.
[176] *Intel v Hamidi* 30 Cal.4th 1342.
[177] In discussion during the passage of HADOPI, the French government indicated that although access to the Internet would still be possible via anonymous surfing from cybercafés, these would also be restricted to a whitelist of approved sites, thus removing access to P2P sites.

The issue of freedom of expression also shades into the paradox of closing down access to the Internet to potentially thousands of people, particularly the young, at the same time as many countries are driving to improve access to the Internet in the name of digital inclusion. It is arguable that in the EC Charter of Fundamental Rights, access to the Internet has become a protected right not just under the head of expression, but under Art 36 which guarantees access to "services of general economic interest". Some states, such as Finland[178] and Costa Rica[179], have also recently recognized a right to access to the Internet, and indeed in the case of Finland, to broadband access, in their national law. Again, it can be argued that such a right is of course not absolute, and that access can be withdrawn for breach of both civil and criminal law. But as before, a court, especially the Strasbourg court, would look to see if the restriction on such rights in the interest of copyright enforcement was proportionate and legitimate, and it is notable that even in criminal cases involving pedophiles, withdrawal of Internet access is often seen as too strong a sanction because of its knock on effects both on the rest of household, and on basic economic and social activities such as seeking work, accessing services and education.

Unintended consequences

Graduated response laws will of course in their detail vary from state to state, but one key issue will be what unfortunate side effects are produced. As noted above, one problem will always be that the actual downloader cannot be identified by IP address: merely the machine to which that IP address was assigned by an ISP. Accordingly, in the UK DEA for example, the statute provides that the subscriber is responsible for downloading via that account, even if the actual breach of copyright may have been by another person. This presents particular problems for institutions like universities, schools, libraries or community centers which may give Internet access to a wide range of persons who may then use the facilities to download. If such institutions are held liable as the "subscriber", then the requisite number of warnings for disconnection is likely to accumulate very fast[180]. Their solution may be to restrict access to any kind of P2P traffic – but this will have the effect of blocking access to legitimate content distributed by P2P (such as in the UK, online delivery of BBC TV programmes often used for educational purposes). Such schemes also create substantial uncertainty for reputable institutions like universities and the British Library, which have expressed uncertainty if they are to be classified as an ISP – with expensive duties to deliver warnings – or as a subscriber – with worrying responsibility for infringements which may not be manageable without curtailing their public access and education roles. Demanding every user of a system registers with identifying details, so that warnings can be delivered, may also be contra indicated both for public access interests[181] and for businesses which often use free Wi-Fi as a means to improve casual visitors e.g. pubs, cafes, hotels[182].

The problem is exacerbated even further for such commercial and public institutions – as well as for domestic subscribers – if wireless networks are operated. As noted above, it is

[178] See http://www.bbc.co.uk/news/10461048, 1 July 2010.
[179] See http://www.technollama.co.uk/costa-rican-court-declares-the-internet-as-a-fundamental-right, 2 October 2010.
[180] See e.g. JANET (UK university backbone network provider) response to DEA Initial Obligations code consultation, July 2010, at http://www.ja.net/development/legal-and-regulatory/regulated-activities/related-regulatory-documents/Ofcom-DEA-Code-response.html .
[181] For example, many cities now try to provide open access wi-fi zones in their city centres.
[182] See further Edwards L, *Guardian,* 30 November 2009 at http://www.guardian.co.uk/technology/2009/nov/30/open-wi-fi-digital-economy-bill-government.

often easy to "piggyback" on unsecured Wi-Fi or to hack even secured Wi-Fi. Again, under both the DEA and HADOPI models, it seems a subscriber is in principle held responsible for anyone who uses their wireless network for infringing purposes in terms of the graduated response sanctions, although there may be opportunities down the line to plead that someone else was the actual copyright infringer. However in at least the UK model thus far, it appears such a plea may not be successful without proof that "reasonable steps" were taken to secure a network[183].

Such a defense may still be beyond the capacity of many domestic subscribers who are old or technology-ignorant, especially as wireless routers are typically delivered unsecured; and thus again the aims of the graduated response schemes seem at odds with national drives to get the digitally excluded online. At present within the UK, there seems an acknowledgement that the above problems are intractable and the interim solution has been to apply the DEA only to the 6 largest UK ISPs (i.e. those with over 400,000 subscribers) and thus not to those who provide Internet access on a smaller scale e.g. universities, libraries and providers of wireless networks[184]: this however can only be a stopgap as, otherwise, avoidance will be fairly easy, defeating the purpose of the exercise.

Costs

Finally, graduated response is an expensive business. The UK government has estimated the cost to ISPs as between £290 and £500 million over 10 years[185]. This includes the costs of identifying subscribers, sending notifications, running call centers for answering queries and investing in equipment to manage the system. Initially, total costs are to be shared 75% to industry and 25% to ISPs[186]. This, it is asserted, will produce a saving to the copyright industries of approximately £200 m annually. France has given HADOPI an initial budget of 6.7 million Euros annually and estimates the costs over 2009-2012 at 70 m Euros for ISPs and 100 m Euros for the IP industry[187].

The ISP industry has generally argued for "beneficiary pays" i.e. the full cost of such enforcement should fall on the industries benefiting[188]. While it may conceivably be argued that mainstream consumer ISPs deserve to bear the partial cost of policing infringement, given they benefit financially from packages catering to high broadband use, for some sectors it will be a particularly difficult cost to bear, especially at times of recession. In the UK, for example, it has been estimated that if the University of London alone (which has 135,000 students) were to be brought into the remit of the DEA as an "ISP" then the costs of either entirely blocking P2P traffic – which would be invidious as the university is a high user of legitimate P2P traffic – might approach £8m annually. If all P2P was not blocked, then the appeal process to notifications delivered to universities as

[183] See OFCOM consultation and draft Initial Obligations Code to DEA, 28 May 2011 at http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf , para 7.5 of draft code. A final code should have been issued by end 2010, but has not appeared as of May 2010, having been delayed by the judicial review process.

[184] Ibid, paras 3.6-3.18. Note mobile operators are also excluded, mainly because of difficulties with gathering the evidence more than mere IP address needed to identify someone downloading using a mobile network – see supra n 157.

[185] Supra n 130 at p 68.

[186] See http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response. Note amendments are indicated to this by the DEA judicial review.

[187] OECD 2010 Report, para 239 in draft.

[188] See e.g. http://www.ispa.org.uk/press_office/page_725.html.

providers to students would also be extremely expensive, given an expected one notification per 140 students[189].

Such costs will be passed on by commercial ISPs to their customers, creating an increase in Internet access costs and possible impact on digital inclusion; while for the public sector, such costs may result either in withdrawal of Internet access as a public service (e.g. with free community Wi-Fi) or severe organizational and financial difficulty. The UK's own impact assessments suggest that around 10,000-40,000 people could lose Internet access due to increase in fees and ISPs could lose £2-9m per year[190].

Legal issues

Finally, and perhaps most significantly within Europe, as discussed at length above, under the EC Electronic Commerce Directive, arts 12 to 15, ISPs and hosts are provided with exemption from liability in respect of content they either host or transmit as a 'mere conduit', unless the ISP or host has been given notice of such illegality, in which case they are obliged to take down that material to retain immunity. A 'three strikes law' could seem potentially to breach this immunity. This formed one of the four grounds of judicial review of the UK DEA 2010, which the UK courts agreed to hear in November 2010[191], but the ECD ground was rejected by the court on the basis that Art 12 should be construed "narrowly" and restricted to liability arising directly "as regards" the content transmitted, not merely liability accruing *because* of the content. In respect of Art 15, the judge took the view that in his opinion an ISP's role in graduated response is "essentially passive" and thus no general obligation to *monitor* was being laid on them in breach of Art 15[192].

Assessment

Although graduated response has been heavily promoted all over the world, it has won few friends outside the creators and content industries, brings with it the many serious problems discussed above and cannot yet be said to have proved an effective deterrent to infringing filesharing (although this would be difficult when e.g. the French system has only just gone "live"))[193]. This report cannot canvas the huge amount of words that have been spilt on this topic, on either side: but it appears fair to say that opposition is heartfelt and possibly counter-productive to rightsholder interests when it has generated its own political party which now holds two seats in the European Parliament[194]. Perhaps in response to this hostile public climate, especially in Europe, the latest, and now final and

[189] See "DEAct costs will run into £hundreds of millions – is this a good investment?", 10 November 2010 at http://www.trefor.net/2010/11/10/deact-costs-will-run-into-hundreds-of-millions-is-this-a-good-investment/.
[190] See supra n 130 at p 76.
[191] Ibid.
[192] DEA judicial review, paras 107, 114-116. It is worth noting that the Advocate-General Opinion in *L'Oreal v eBay* 9 December 2010 (1), Case C-324/09 para 136 argues against a narrow interpretation of Art 12.
[193] There is however early evidence that the passing of HADOPI has not discouraged filesharing but merely encouraged migration to alternatives such as streaming sites rather than P2P sites: see http://arstechnica.com/tech-policy/news/2010/03/piracy-up-in-france-after-tough-three-strikes-law-passed.ars. Contrast however James Gannon arguing that legislative interventions in countries like UK and Republic of Korea is improving record company profits : http://jamesgannon.ca/2010/04/30/musics-biggest-hit-in-2009-graduated-response/.
[194] http://en.wikipedia.org/wiki/Category:Pirate_Party_%28Sweden%29_MEPs.

official, draft of ACTA[195] – the multilateral Anti Counterfeiting Trade Agreement which the US has been negotiating under conditions of strict conditions of confidentiality with a number of other states including the EU for several years, on issues including piracy and counterfeiting – seems to have turned its back on imposing graduated response as a mandatory requirement for states party. This had been expected by many onlookers, given evidence from leaks of various prior versions.

Similarly, the Gallo Report, an influential enforcement report which was received by the European Parliament in June 2010[196], does not demand graduated response, but instead seems to concentrate on the need to extend the criminalization of large scale but still non-commercial copyright infringement (a theme also pursued in ACTA). Yu argues that although graduated response has both advantages and drawbacks for users, ISPs and rightsholders, the case for it is not made on four key grounds. Two have been addressed above; the problems with due process and the possible infringement of fundamental rights of free expression and privacy. But she goes on to note that graduated response may not actually be effective in inducing a significant change of social behavior among individual file sharers and that thus it may not be a proportionate response to the problem (see below). Patry similarly notes:

"Graduated response is all stick and no carrot: as such , it can never accomplish its purported goal of encouraging lawful behavior because the industry refuses to respond to the consumer demand, and instead insists on suppressing it, even when third party ISPs are willing to do all the work"[197].

As noted above, it *is* possible to provide a carrot as well as a stick using systems along the lines of Global File Registry described above, which attempt to filter out infringing works and then as an alternative to imposing sanctions, divert the user to a route to downloading legal content. YouTube's Content ID system is another example of how detection systems can be used not to "punish" infringing uploaders and downloaders but rather to create a system which allows rightsholders a new revenue stream. We return to this point in section X, Alternative Approaches, below, after we have addressed the second major strand of activities associated with P2P investigations and graduated response, namely, filtering by ISPs and hosts.

Perhaps the key issue in any assessment of graduated response is the question of proportionality. The basic equation here is that although unlawful filesharing is a problem, the means of stopping it may outweigh the benefits, and infringe on basic rights, especially when there are less harmful means to achieve the same end. The application for judicial review of the UK DEA by BT and Talk Talk asserted that:

"The contested provisions of the DEA 2010 represent a restriction on the free movement of services and/or an interference with the right to privacy and/or the right freely to receive or impart opinions and information. The burden accordingly falls on the UK to present a public policy justification for such measures and to establish that the measures are proportionate to the aim to be achieved."

---

[195] Consolidated Text, "Informal Predecisional/Deliberative Draft", 2 October 2010, at http://trade.ec.europa.eu/doclib/docs/2010/october/tradoc_146699.pdf.

[196] Report on enforcement of intellectual property rights in the internal market (2009/2178(INI)), Committee on Legal Affairs. 3.6.2010.

[197] Patry, supra n 136, at 12.

The courts gave leave for this ground to be explored in November 2010. The statement of grounds argued that the principle of proportionality was offended in the DEA 2010 because:

(i) it risks catching and harming innocent Internet users whose service has been used for illicit purposes by others;

(ii) it will have a chilling effect on Internet use that goes beyond (i) e.g. by impeding organizations offering open Wi-Fi or dissuading individuals who fear not being able to protect their accounts;

(iii) the evidence of costs to industry of £400 million pa from unlawful filesharing presented was unproven and not subject to independent scrutiny and did not take into account key factors such as the fact that removal of access to unlawful content would not guarantee equivalent uptake of legal content;

(iv) the harms to public interests such as the risk of constant monitoring of users, the reputational detriment to users alleged to be infringers and the possible curtailment of access in public places had not been taken account of in full or in part;

(v) less restrictive means of achieving a reduction in unlawful filesharing were available e.g. education; recourse to the ordinary civil courts; greater use of NTD procedures; uses of "notice and notice" (especially as the trialing of this prior to the passing of the DEA 2010 had not resulted in any empirical analysis of its success or failure). It was also noticed that there had not yet been time in Europe to observe if the changes brought in by the IPRE Directive would make a significant impact on commercial scale copyright infringement thus restoring industry revenues.

(vi) The restrictions on privacy and freedom of expression entailed by the measures could not be justified as in the public interest.

In the end the judicial review court also rejected the proportionality argument, but in fact gave it little more than a cursory hearing. It appears that the court might have felt somehow constrained by the limits of a judicial review case (rather than say human rights or constitutional proceedings) where strong weight had to be given to the belief that Parliament in legislating had already carefully weighed up the balance between industry needs and user rights and freedoms (paras 210-218). Furthermore the court emphasized it was premature to assess proportionality when the delegated rules to bring the Act into force had not yet been made, and only barely decided to consider hearing the ground on the basis that just about "enough [was] known at this stage about the fundamental regulatory structure of the DEA" (para 205). It seems therefore that a future challenge to proportionality when the Act was actually operating might well go differently, and commentators have suggested the challenge was made too early for a chance of success.

At ECJ level as already noted, different views have been emphasized. The *Promusicae* case placed a heavy emphasis on proportionality when balancing protection of copyright property rights against other interests such as user privacy rights, and stated explicitly that copyright, even if recognized as a human right, did not necessarily trump privacy. The Advocate-General's opinion in *SABAM (*discussed in detail at n 211 below and text following*)*, also seems to strongly take the view that enforcement means to protect copyright are not acceptable where they involve blanket invasion of the privacy rights of all users, innocent and infringing, as is inevitable in current content filtering and monitoring.

The Council of Europe has recommended that if filtering technologies (discussed below, section VIII) are to be used, limitations on fundamental rights must be proportional and appropriate to the purposes of the filtering[198]. Peter Hustinx, the European Data Protection Supervisor, has been particularly unhappy (in his opinion on negotiations over ACTA) over the possible impact both of generalized monitoring of Internet activities, including those of "*millions of law-abiding Internet users*", and the effects of disconnecting users from the Internet given it "*plays a central role in almost all aspects of modern life… thus cutting individuals off from work, culture, eGovernment applications etc"*[199].

Outside Europe, commentators have also doubted the proportionality of graduated response, with, in the US, particular emphasis on the disproportionate impact on free speech. Yu argues that "*a cost-benefit analysis should take into account both the local conditions and the challenges in quantifying such costs as harm to free speech, free press, privacy and other civil liberties"*[200].

If the introduction of graduated response is allowed or imposed (whether by voluntary or forced co-operation by ISPs as well as by legislation) Yu asserts that seven basic principles must be built in:

- Independent review of allegations of infringement, which should be judicial except in cases of those already convicted of infringement in a court of law;

- Education and rehabilitative benefits must be taken seriously;

- Reasonable alternative access to the Internet must be available for those whose accounts are suspended;

- Collateral damage (unintended consequences) must be minimized e.g. suspension of Internet access should not also result in loss of tied phone or cable services; downloading by children should not result in loss of access to parents;

- The graduated response system must be proportional and consider other important societal interests such as free speech, free press, and privacy;

- The graduated response should be flexible and allow those alleged to have infringed to show they had reasons to believe they were not doing wrong, not just limited to strict "fair use";

- Internet disconnection should be a last resort, and blacklists which might bar a suspended user from all forms of Internet access should be barred;

The draft 2010 OECD report which looked generally at online intermediaries and liability, in its special section therein on copyright, also made several key points:

- Quantitative information on the costs of copyright infringement on the Internet and the long-term effectiveness of remedies, compared to their costs, is limited, and more should be done to measure the effectiveness and costs of notice forwarding, notice and

---

[198] See *Recommendation on freedom of expression and information with regard to Internet filters*, 26 March 2008 at https://wcd.coe.int/ViewDoc.jsp?id=1266285&Site=CM.
[199] Supra n 164.
[200] See also Yu P, "The International Enclosure Movement" (2007) 82 Ind. L.J. 827.

take down, and graduated response in jurisdictions were such schemes has already been implemented;

- NTD regimes in many jurisdictions appear workable and balanced however do not deal with all the realities of cross border and P2P infringement;

- Research is needed to see if "notice and notice" regimes are effective without needing to go further to regimes involving disconnection or other sanctions.
- Copyright infringement should be officially determined "to the greatest extent possible" before imposing sanctions, and consideration should be given to developing an "expedited adjudication process" for allegations of infringement;

- Further research into the equities of sharing of the costs of implementing graduated response schemes between rightsholders, ISPs and the state/for social benefit is required;

- Private or voluntary arrangements for graduated response run the risk of putting intermediaries at risk of legal liability, and may not be fully protective of user rights;

- International agreements might be an important way to create consensus globally in this area but such negotiations should be open and transparent and provide for input from all relevant stakeholders.

VIII. FILTERING AND WEBSITE BLOCKING

Since it began to become apparent that neither suing P2P sites nor users would be a magic bullet to bring about the end of unlawful filesharing, much attention has been paid by rightsholders to the possibility of asking ISPs to act as filters to reduce online infringement. There are currently two main approaches here.

One is to ask (or to sue) the ISP so that they block certain websites to all their subscribers, which might be either P2P intermediaries such as torrent sites, or actual hosts of infringing material. This will be called "*website blocking*".

Secondly, the ISP can be asked to monitor for and then filter out certain *types* of traffic coming to its subscribers e.g. using certain protocols i.e. P2P traffic; or matching certain constraints e.g. notified copyright works. This will be called "*content filtering*".

A third approach, connected to the first, is to ask the sites that translate URLs and thus direct Internet traffic – the Domain Name System (DNS) routers - to block resolution of the domain names notified as used by alleged piracy sites. This approach ("*domain name blocking*"), which has so far mainly been publicized by the proposed US Combating Online Infringement and Counterfeits Bill[201] introduced in September 2010 by Senator Leahy, may be unpopular with many states, both because of the over-wide scope for censorship where entire domains are blocked[202], and because of its considerable scope

[201] See MPAA press release supporting Bill at http://www.mpaa.org/resources/a5118846-763a-46a5-9ad9-18b8a9a6bf63.pdf.
[202] See "Advocacy group slams online-piracy bill as censorship", 22 September 2010 at http://thehill.com/blogs/hillicon-valley/technology/120211-eff-slams-online-piracy-bill-as-censorship.

for tension with the existing domain name Internet governance scheme run by ICANN and the international standards bodies which support it[203].

Suing ISPs and hosts to install filters

In Europe, a large number of national courts have heard cases on filtering to protect and enforce copyright, and decisions have gone both for and against filtering of both types[204]. In Spain[205], Norway[206] and Holland[207], courts have rejected applications against ISPs for filtering, while the German courts have twice rejected claims that hosting sites such as RapidShare should also filter out the files they host[208]. However as noted above, the Italian Supreme Court has required blocking of the Pirate Bay site, and the Danish courts have also required that site be blocked, as well as certain Russian sites.

Website blocking has been imposed by agreement after legal coercion: in the Irish *EMI v Eircom* case discussed above, the settlement reached in that suit required Eircom not only to impose graduated response, but also to block the Pirate Bay website[209].

Notably in the Belgian case of *SABAM v SA Tiscali (Scarlet)*[210], a Belgian ISP was compelled in July 2007 to implement technical measures (content filtering, not just website blocking) in order to prohibit its users from illegally downloading music files. The case is now however under appeal to the ECJ and the questions for that court have been formulated:

"1. Do Directives 2001/29 **[copyright in the information society]** and 2004/48 **[the IP enforcement directive]**, read in conjunction with Directives 95/46 **[on the processing of personal data],** 2000/31 **[the e-commerce directive]** and 2002/58 **[on privacy and electronic communications]** and interpreted with regard to Articles 8 and 10 of the European Convention on Human Rights, allow Member States to authorize a national court, seized in a procedure on the merits and on solely on the basis of the legal provision which holds that "They [the national court] can equally impose a prohibitory injunction on intermediaries whose services are relied upon by a third party to infringe copyright or a neighboring right", to order an ISP to put into place, *vis-à-vis* all of its customers, *in abstracto* and as a preventive measure, at the expense of the ISP and without limitation in time, a system filtering all electronic communications, both incoming and outcoming, passing through its service, in particular by means of peer to peer software, with the aim to identify the circulation on its network of electronic files containing a musical, cinematographic or audiovisual work to which the claimant alleges to enjoy rights and to then block the transfer thereof, either at the request or at the time it is sent?

---

[203] See MacSithigh D, blog post at http://www.lexferenda.com/17112010/coica/.
[204] Supra nn 74,75,78.
[205] See n 123 and "Spanish government endorses an aggressive anti-P2P file-sharing legal amendment", 20 January 2010, at http://theviewfromtheboundary.com.
[206] Supra n 75.
[207] Court of the Hague, 19 July 2010, dismissing request by Brein, a Dutch copyright organisation, for court order for ISP Ziggo to block the Pirate Bay.
[208] "Germany: filtering by keyword is not an obligation for a hosting company", *EDRI-gram*, 28 July 2010.
[209] See *EMI v Eircom*, [2009] IEHC 411, unreported, 24 July 2010, per Charlton J, and supra n 127.
[210] [2007] ECDR 19, District Court of Brussels. English translation available at http://www.cardozoaelj.net/issues/08/case001.pdf. The case was referred to the ECJ and the Advocate-General delivered a preliminary opinion on 14 April 2011 (Case C-70/10, English summary available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf).

2. If question 1 is answered in the positive, do these directives require that the national court, seized to rule over a request for injunctive relief against an intermediary on whose services a third party relies to infringe a copyright, applies the principle of proportionality when it is asked to rule over the efficacy and the dissuasive effect of the requested measure?"[211]

Although the case is yet to be finally heard by the ECJ, the Advocate General gave his preliminary opinion on 14 April 2011. In short, he considered that the installation of a filtering and blocking system would necessarily involve restrictions on the right to respect for the privacy of communications, the right to protection of personal data, and the right to freedom of information, all of which were rights protected under the Charter of Fundamental Rights. Although he accepted such rights were, of course, subject to exceptions, restrictions would be permissible only if adopted on a national legal basis which was accessible, clear and predictable. It could not be held that the obligation on ISPs to install the filtering and blocking system at issue, entirely at their own expense, was laid down expressly, and in clear, precise and predictable terms, in the Belgian statutory provision at issue. Consequently, he concluded that the ECJ should declare that EU law precluded a national court from making an order that an ISP install a filtering system, in respect of all its customers, *in abstracto* and as a preventive measure, entirely at the expense of the ISP and for an unlimited period. If upheld in the final decision, this will be a considerable setback for the desires of the content industries to extend the scope of filtering *ex ante* obligations in Europe.

Outside Europe, there seem to be fewer reported examples of litigation seeking to impose filters on ISPs. One significant setback for the content industry was in the Australian *iiNet* case, supra n 50. In that case Cowdroy J refused to accept that the ISP in question, by not installing filters, had authorized infringement, nor had they sanctioned, approved or acquiesced in it. He distinguished an ISP such as IiNet which provided access to any and all sites, from a P2P client site such as KaZaa (who had lost in previous Australian litigation[212]) where the respondent "intended copyright infringements to occur, and in circumstances where the website and software respectively were deliberately structured to achieve this result." [213]

Legislation for website blocking

Multinational

The EC Telecoms Package passed in December 2009 and noted above, n 124, contains provisions which may allow EC member states to mandate filtering by ISPs and telecommunication providers in relation to obligations to clamp down on copyright infringement, illegal content such as pornography, and possibly also to maintain the security of a network. Whether such obligations would clash with other laws and fundamental rights has been uncertain and controversial.

The latest version of ACTA, released on 15 November 2010, also clearly demands that injunctive relief be available "to prevent infringing goods from entering into the channels of

[211] English translation and interpolations taken from IPKat, 11 February 2010, at http://ipkitten.blogspot.com/2010/02/sabam-v-tiscali-goes-to-ecj-on-isp.html
[212] *Universal Music Australia and ors v Sharman License Holdings* [2005] FCS 1242; (2005) 65 IPR 289.
[213] Ibid, para 14.

commerce" (section 2, Art 2.x) and applies this to the electronic environment in section 5, Art 2.18[214]. It is however stated that such enforcement measures must "preserve fundamental principles, such as freedom of expression, fair process and privacy".

National

In Spain, where the courts had previously rejected blocking of P2P intermediaries, the Sustainable Economy Act was introduced, which sets up a system of judicial investigation of websites where allegations have been made that they are complicit in copyright infringement. The legislation only involves blocking websites, not disconnecting people, and requires a court investigation; even then in Spain, the law does not seem to have broad support from the local judiciary, the ISP industry and public[215].

The UK DEA 2010, discussed in the last section, was unexpectedly amended near the end of its legislative progress to allow a rightsholder to seek a court order under s 17 forcing an ISP to block an entire website ("location on the Internet") if that site was or was likely to be used "for or in connection with an activity that infringes copyright". This was justified on the grounds that c 20% of filesharing, according to industry figures, occurred not via P2P protocols at all but via simple downloading from so called "cyberlocker" sites, i.e. hosts where content was stored, usually in encrypted form. It was uncertain at the time, particularly given the vagueness of the statutory terminology used, if these "locations" were supposed to include only overtly illicit sites, or "dual purpose" sites which host both infringing and non-infringing content, and have many legitimate commercial users, a category which might include DropBox, Google Docs, YouTube, Facebook and numerous cloud computing sites. Further amendments have meant that the details of how s 17 is supposed to operate have been further delayed, as consultation must be undertaken before delegated rules can be made: however it is notable that the legislation now demands that any new rules must take into account if an injunction to block a "location" would be likely to have a disproportionate effect on any person's legitimate interests; and "the importance of freedom of expression" (s 17(5)(d) and (e)).

The future of s 17 is currently uncertain after the newly elected Coalition government announced an enquiry into whether website blocking was practical and desirable in February 2011. Meanwhile the government appears instead to be seeking agreement from the major UK ISPs to undertake filtering of websites associated with piracy on a voluntary basis.

The South Korean graduated response law also allows for ISPs to be ordered to "shut down" a website for no more than 6 months if it has received three warnings for sharing infringing content and not responded. As of January 2010 however, no such order had been made[216].

Assessment

Three key issues arise as to whether filtering, whether imposed by law or by court order, can and should be employed to reduce copyright infringement. First, is it *practicable* for ISPs (or hosts) to implement an order to filter and block content - and if they can, how much will it cost and how reliable will it be? Will it over block and under block? Will it increase the cost of Internet access for users to the point where digital inclusion may be reduced? These questions are at the heart of the *SABAM* opinion discussed above.

---

[214] Final Consolidated Text, released November 15, 2010.
[215] Supra n 74, 153.
[216] See http://hurips.blogspot.com/2010/03/three-strikes-rule-sleeping-for-seven.html.

The second question, which is particularly germane to Europe, is whether it is currently *legal* under instruments such as the ECD to impose such ongoing filtering obligations on ISPs and hosts. Certainly, Art 15 of the EC ECD, as discussed earlier, forbids member states from imposing "a general obligation to monitor". However Art 14(2) does allow a court or administrative authority to require an ISSP to terminate or prevent an infringement, and similar injunctive relief is available specifically in relation to preventing IP infringements, and against intermediaries, under Art 8(3) of the Infosoc Directive[217].

This however takes us to the third question, which is whether filtering can be imposed without imposing restrictions on fundamental rights and freedoms in a way disproportionate to the goal sought to be achieved, i.e., reduction of infringing behavior. We have already partially considered the issue of proportionality in the section above. There is considerable concern that the current state of content filtering technologies necessarily both under blocks and over blocks, e.g. machine filters can compare copyright work A to uploaded work B but they cannot yet and may never be able to understand and implement concepts like "fair use", "private use" or "implied license". Freedom of expression and of information may accordingly be impaired. In older fashioned website filtering by URL or keyword, entire websites might be blocked because of a small section of offending files. For example, the video streaming site YouTube has been attacked by the content industry as a haven for infringement, but one 2007 report showed only 9% of files had been notified as infringing, and even these only generated 6% of all views[218]. Links from a site may also be seen as evidence of infringement with serious consequences e.g. the BBC news website often makes links to sites such as the Pirate Bay to illustrate relevant stories.

Content rather than website filtering can be made more precise by "deep packet inspection"
(DPI) – which allows ISPs and "mere conduits" to not just identify the *type* of packets they are distributing - which is classically how the "end to end" Internet operates - but effectively to look inside them to their actual content[219]. This brings with it issues of blanket monitoring and privacy of users, including those whose activities are wholly legitimate. We have already looked at some DPI tools above – Dtecnet and CopySense by Audible Magic are examples – and noted that they are already controversial in relation to relating to privacy.

Most notably, blanket ISP filtering using DPI is clearly rejected in the ECJ *SABAM* opinion as a disproportionate invasion of privacy. The opinion clearly perceives general future unspecified filtering restrictions as diametrically opposed to fundamental rights such as privacy, personal data protection and freedom of information. It also echoes a trend in ECJ jurisprudence visible in another recent ECJ Advocate-General opinion, *L'Oreal v*

---

[217] Directive on Copyright and related rights in the information society, 2001/29/EC. See also Article 11 of Directive 2004/48/EC (IPRED). Note that, interestingly, this is exactly the power which the Irish judge Charlton J held he did not have in *EMI v UPC*, not because he felt he was restricted by the ECD, the ECHR or the Charter of Rights, but merely because he felt the Irish implementation of the EC copyright Directives was flawed on the matter of injunctions.

[218] See http://technollama.blogspot.com/2007/04/youtubes-content-is-mostly-user.html.

[219] The Canadian Privacy Commissioner has expressed concern over the privacy implications of DPI and produced a collection of essays, available at http://dpi.priv.gc.ca/. See also Ohm P, "The Rise and Fall of Invasive ISP Surveillance" supra n 173, and Yu, supra n 87 at n 10 citing Kevin Werbach's definition of DPI.

eBay (discussed supra n 193) where again, an application requiring eBay to put in place general proactive filtering to prevent future unnamed trademark infringements by unnamed persons, was rejected as too vague in its restrictions on freedom of expression, and hence illegal. Nor could such filtering be imposed if it "*would infringe the rights of innocent users of an electronic marketplace or leave the alleged infringer without due possibilities of opposition and defense"* (para 158).

In respect of the intermediary, practicality was the key. "*What is crucial, of course, is that the intermediary can know with certainty what is required from him, and that the injunction does not impose impossible, disproportionate or illegal duties like a general obligation of monitoring*" (para 181). The only concession made to the trademark holder plaintiffs was that filtering to remove repeat infringers – by for example, closing their accounts – would be allowed as it rested on "actual knowledge" in terms of Art 14 of the ECD.

Between them, these two cases show a clear steer away from court imposition of general filtering to protect IP rights in Europe, and may even place a greater scrutiny on national EU *legislation* mandating filtering – such as the UK DEA, s 17 - as well.

Finally, the question of how far ISPs should interfere with the packets they transmit and receive is also, as Ohm, points out, highly relevant to the question of net neutrality[220], an issue whose definition and policy is being fought over in various venues in the EC and US right now[221]. Since the techniques to look inside packets are usually harnessed to produce the ability to slow traffic or block it entirely, DPI potentially threatens both freedom of expression and privacy simultaneously, as well as net neutrality.

In this context, it should be noted briefly that there are other drivers towards encouraging ISPs to monitor and filter content than IP interests. Filtering is increasingly popular with governments and law enforcement agencies as a legislative and policy tool, as part of the struggle by states to regulate the influx of other types of unwelcome content from the Internet, such as adult and child pornography, hate speech, terrorist and pro-jihad speech, et al. A draft EC Directive, championed by Commissioner Cecilia Malmstrom, recently proposed that ISPs throughout the EU should be required to filter out child pornography, but was blocked by the European Parliament, for the moment anyway, in February 2011[222]. The general move towards using ISP filtering as a public policy tool, may mean that the technologies for more effective, granular, reliable and scalable filtering may indeed be developing, but crucial problems will still remain both in relation to copyright and other types of illegal or offensive content, as discussed above, i.e. privacy, over and under blocking, machine processing of semantically difficult exceptions to hard rules. Meanwhile the legal environment for regulating filtering across different content domains

[220] See, notably, the US FCC decision that Comcast breached its neutrality duties as a telecoms provider by covertly blocking P2P traffic (using DPI) and sending bogus error messages to affected users, notwithstanding Comcast's claim that it was legitimately managing its network to ease traffic congestion. The FCC held that Comcast was entitled to manage traffic, and indeed to block transmissions which violated copyright law, but not to prioritize one protocol over another. See Bridy, supra n 68, at pp 598-599.

[221] See e.g. http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/index_en.htm.

[222] See Proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (29.03.2010) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0094:FI. A compromise agreement was put in place of the rejected mandatory filtering portion of the draft Directive, 14 February 2011, at http://www.edri.org/files/14_feb_blocking_compromises.pdf.

is confusing and underdeveloped, as seen in the battles over the Telecoms Framework and the Child Abuse Directive in the EU, the IP opinions in *SABAM* and *eBay*, and the current net neutrality debates globally. What may well happen is that, as in the UK currently (in relation to pornography as well as pirate websites) states and other agents such as rightsholders may divert their efforts not towards mandated filtering, by publicly accountable methods such as courts and legislation, but towards voluntary agreements with intermediaries which may lack transparency, democratic foundation and safeguards for user rights.

The Council of Europe has suggested a number of safeguards in relation to the use of filters by Internet intermediaries. Although these may have been conceived more with an eye to state or private filtering of illegal content such as pornography, than in the context of copyright, they are still relevant. The Recommendation[223] notes that states should:

- introduce regulations where necessary to prevent the intentional use of filters to restrict access to lawful content

- assess filters both before and during their implementation to ensure their effects are appropriate and proportional and avoid unreasonable blocking of content

- provides for effective means of recourse including suspension of filters where users claim lawful content or access is being blocked.

Global reactions on the proportionality of filtering and website blocking as solutions to unauthorized filesharing tend to be more hostile even than to sanctions such as suspension or disconnection. For an outraged recent example, note the response of one US senator, Ron Wyden, to the US COICA Bill which would mandate domain name blocking:

"*It seems to me that online copyright infringement is a legitimate problem, but it seems to me that COICA as written is the wrong medicine. Deploying this statute to combat online copyright infringement seems almost like using a bunker-busting cluster bomb when what you really need is a precision-guided missile. The collateral damage of this statute could be American innovation, American jobs, and a secure Internet*".[224]

IX. HOSTS OF "USER GENERATED" OR "USER MEDIATED" INFRINGING CONTENT

Hosts of "user generated content" (UGC) like Facebook, MySpace, YouTube, DailyMotion, Photobucket, GoogleDocs, Tumblr and Flickr, to name but a few have seen extraordinary growth and success in the last five years or so. All these sites began as primarily hosting content generated by users or subscribers to the site: e.g. music on MySpace, videos on YouTube, pictures on Flickr, text and pictures on Tumblr, etc. Although many such sites began by offering a free service out of sheer enthusiasm or for aspirational benefit, they have in a mature market, become profit making businesses, and in many cases also become well known loci for IP infringement, with content copyright of third parties e.g. all or part of commercial films, music videos and TV programmes, uploaded by, and then made available to, users. In this sense, they are now better described as "user-mediated content" (UMC) sites than "user generated content" (UGC) sites. They have also in the

[223] Supra n 199.
[224] See http://arstechnica.com/tech-policy/news/2010/11/senator-web-censorship-bill-a-bunker-busting-cluster-bomb.ars.

main developed a business model with revenues arising not from a conventional joining fee or subscription, but more often from advertising (textual, video or audio) delivered alongside content the users seek to access. Accordingly the financial success of the site can be conceptually tied to the commercial appeal of the user-mediated content it hosts. (Many sites now also have a hybrid business model where an alternative to the free ad-supported service is a paying ad-free subscription.)

As such sites have grown extraordinarily (e.g. 35 hours of video uploaded to YouTube per minute[225]) they have become perceived as a problem for IP rights holders, in the field of trade mark as well as copyright, in the same way as, though to a lesser extent than, the more obviously subjectively illicit P2P intermediaries discussed above. The issue thus arises if these sites should retain their claim to the same immunities as traditional intermediaries like ISPs, discussed above in section III, or whether they should be held at least partly responsible for infringing content they host, on grounds of financial benefit therefrom. Such arguments rest to a very large extent on whether it is assumed the intermediary would, or should have known of this infringing content, simply because of its ubiquity, since where actual notice of infringement is served by a rightsholder, these sites usually take down promptly. This takes us to asking whether there are grounds to move from the existing "notice and take down" (NTD) model described above and implemented by the ECD and DMCA, to a model based around "constructive knowledge", with possible new duties for intermediaries of proactive filtering, rather than mere NTD – and as noted above[226], there are difficulties fitting such duties into the existing scheme of especially the ECD, Art 15, which restrains EC states from placing general obligations to monitor content on intermediaries. Without such new duties, content industries are effectively limited either to abiding by NTD as their best remedy, possibly seeking to have such sites blocked by ISPs as havens for infringement (as discussed in the last section) or reaching voluntary arrangements with sites (see section X below).

These issues have so far principally come to a head in two lengthy campaigns of litigation: one by Viacom (and other rightsholder plaintiffs, including the English Football League) against YouTube in the US courts, and the other by various famous trademark holders in the luxury goods sector against eBay as host of listings selling counterfeit goods which tarnish or infringe those marks.

Viacom v Google

In 2007, Viacom sued Google, as owner of YouTube, for failing to police the widespread unauthorized posting of clips there from properties owned by Viacom (such as MTV videos, or TV comedy clips).[227] According to Viacom, at that time 160,000 clips owned by them had been viewed without permission over 1.5 billion times on YouTube, and one billion dollars damages were claimed. YouTube's business model was, it was said, "based on building traffic and selling advertising off of unlicensed content, [and] is clearly illegal". Google responded that take-down notices from Viacom were promptly dealt with and designated content removed. For example, in February 2007, YouTube had taken down 100,000 unauthorized Viacom-owned clips. Viacom's reply was that Google must know in a generalized way of constant widespread infringement, given their own search engine revealed extensive postings of Viacom-owned properties. In fact however external

[225] Supra n 202.
[226] Supra section VII, *Legal Issues*.
[227] See original Complaint, *Viacom International v YouTube*, Inc No 1:2007- CV- 02103 (S.D.N.Y Mar 13, 2007). See case documents at http://news.justia.com/cases/featured/new-york/nysdce/1:2007cv02103/302164/.

studies also showed that infringing content was a relatively small percentage of the content hosted by and viewed on YouTube[228]. As with the *eBay* cases discussed next, Viacom appeared *prima facie* to be looking for YouTube, not them, to shoulder the burden of policing the site by filtering *ex ante,* rather than simply offering NTD.

The matter was complicated by the reality known to both parties that Viacom's properties benefited from an enormous audience on YouTube, far more than might have been attracted to a free or paying download site on Viacom's own websites. Indeed, negotiations between Viacom and YouTube for a blanket license from Viacom for plays of their properties on YouTube had commenced, but broken down. YouTube had already successfully negotiated such licenses for profit-sharing with many other entertainment rightsholders e.g. the BBC. In addition, YouTube were known voluntarily to be developing a content identification technology now known as Content ID, which would help block uploads of infringing videos.

In US law, the DMCA, s 512(c)(i) holds a service provider immune from liability for copyright infringing content if (in words almost identical to the ECD) it does not have actual knowledge of such content, nor is aware of facts and circumstances from which such infringing activity is apparent. As in the ECD, immunity is provided subject to material being taken down or access blocked expeditiously – a condition which YouTube were amply able to demonstrate to the court they met.[229] In June 2010, the US courts decided at first instance that YouTube were indeed entitled to the safe harbor of the DMCA [230] and granted Google's motion for summary judgment.[231] The court stood firm that loss of immunity required "*knowledge of specific and identifiable infringements of particular individual items*" and that "*Mere knowledge of such activity in general is not enough*." They also added that "*General knowledge that infringement is "ubiquitous" does not impose a duty on the service provider to monitor or search its service for infringements"*.

The court considered briefly if under s 512(1)(B) – the DMCA's more detailed equivalent of Art 14(2) of the ECD – YouTube might lose the benefit of the safe harbor if it *"receive[d] a financial benefit directly attributable to the infringing activity in a case in which the service provider has the right and ability to control such activity".* The court held that such a "right and ability to control" must refer to a specific, notified infringement (at 26). In other words, it was not enough for YouTube to lose immunity that they possibly made a financial benefit from displaying ads next to contributed videos, if they had no specific knowledge which of those videos was infringing. The decision is likely to be appealed, but at the moment it will be highly influential in indicating it might be unreasonable to expect UMC

---

[228] On May 1 2007, for example, Viacom announced "It is simply not credible that a company whose mission is to organise the world's information claims that it can't find what's on YouTube" (note ownership of YouTube by Google). See Silicon.co, May 1, 2007, at http://management.silicon.com/government/0,39024677,39166945,00.htm. On the other hand around the same time a Vidmeter survey, for December 2006- March 2007, sampled YouTube take down notices and claimed that only 9.23% of all videos on YouTube were removed on notice of copyright infringement, and views of videos removed made up less than 6% of all YouTube video views. (However of those removed for copyright infringement, 40% did belong to Viacom.) See http://theutubeblog.com/2007/04/05/vidmeter-study-debunks-viacomscopyright- lawsuit/.

[229] See *Viacom International v YouTube Inc* 2010 WL 2532404 (SDNY June 23, 2010) at 23: "In this case it was uncontroverted that when YouTube was given the notices, it removed the material".

[230] Ibid.

[231] See www.nytimes.com/2010/06/24/technology/24google.html?scp=1&sq=YouTube%20viacom&st=cse.

sites to go beyond NTD as a matter of law, where such *ex ante* policing cannot be wholly automated.

EBay and liability for trademark infringement

Although relating to trade marks not copyright, the eBay cases mentioned above are also very relevant. Online auction sites like eBay or PriceMinister are anecdotally well known to have a large number of listings which offer counterfeit goods, infringing or tarnishing famous marks such as Gucci, Tiffany, Jaeger, or Harrods. Such sites usually prescribe that sales of such counterfeit goods are forbidden under their acceptable use policy, and respond rapidly to notices from trade mark holders (e.g. eBay's fast track VeRO scheme), but this alone rarely deters sellers.[232]

Policing such infringements by NTD alone takes significant vigilance by the brand's employees and a more desirable solution for them would be to compel eBay to filter out *ex ante* listings containing infringing trademarks. The typical argument is that eBay must have some degree of knowledge of, and control over, its own listings which generate it commission. Primary liability is difficult to establish. Consequently some famous mark holders have argued that auction sites must have "constructive knowledge" of infringement, rendering them contributory liable.

Another basis of liability might be whether the auction site should be held responsible as authorizing the activities of the user who posts the infringing listing. We have seen above how concepts of authorization in *copyright* law have been used to attack intermediaries such as ISPs and P2P sites. Article 14(2) of the ECD provides that content is not to be treated as originating from a third party if that recipient acts '*under the authority or control of the [ISSP]*'. Any normal legal liability would thus persist if the intermediary was found to be authorizing infringement by its users. The qualifications for such liability have not however been defined so far in case law of the European Court of Justice and are often vague in national laws. As noted above a similar claim, of vicarious liability because of financial gain was rejected in the US in the *Viacom* case.[233]

Cases brought by famous marks across the globe against eBay have produced spectacularly varying results. In *Louis Vuitton Moët Hennessy (LVMH) v eBay*[234], a French court found, despite the immunity provisions of the ECD, that eBay was responsible for failing to prevent the sale of counterfeit luxury goods on their site. eBay was fined £31.5 million and ordered to forbid the sale of some luxury perfumes on its site.[235]

---

[232] See ebay's IP policy for sellers which exclude counterfeit goods, at http://pages.ebay.com/help/policies/intellectual-property-ov.html.

[233] But cf s 230(c) of the CDA, which confers absolute immunity on service providers in publication torts and where there is no exception for agency or authorization. This has had unfortunate effects – see e.g. *Blumenthal v Drudge* 992 F. Supp. 44 (D.D.C. 1998) where Drudge contributed an online gossip column which defamed Blumenthal, and for which AOL paid Drudge a considerable sum, as it drew audiences to their fora. Despite this financial gain by AOL, the US court found that AOL were not responsible for Drudge's defamatory comments and were immune from suit under s 230(c) as this was what Congress had intended to prevent chilling of free speech.

[234] See account at OUT-Law, 1/07/2008, available at http://www.out-law.com/page-9225. The matter was complicated by the fact that it is not clear in French law if eBay falls under the laws applying to "offline" auctions, where liability is different from in ordinary sale of goods law

[235] But note that a Paris court seems to have reached the reverse decision in a very similar action by L'Oreal against eBay in respect of sale of counterfeit perfumes, reported on 15 May 2009 at http://www.guardian.co.uk/technology/2009/may/13/ebay-loreal-court-paris-counterfeit.

By contrast however in the US, eBay, sued by Tiffany, won.[236] The case was argued under the different rules of United States' trade mark and unfair competition law, and without reference to a generalized safe harbor law. The US District Court held that ultimately it was "*the trademark owner's burden to police its mark and companies like eBay cannot be held liable for traders based solely on their generalized knowledge that trademark infringement might be occurring on their websites*". Indeed, this finding was explicitly referred to in *Viacom*.

Meanwhile in Europe, L'Oreal, Hermes and others have also sued eBay in countries such as UK[237], France, Germany, Spain and Belgium[238] It is expected that some or all of these non-harmonious European cases may eventually be resolved by one or more references to the ECJ.
The UK case referred to the ECJ for clarification, *L'Oreal v eBay,* has been the first to arrive at the ECJ, with an Advocate-General's opinion issued December 2010 and the full decision of the ECJ expected soon[239]. As noted in more detail above in the discussion on filtering, as with the US *Viacom* and *eBay* cases, the opinion comes down strongly against placing duties on online auction sites (or "electronic marketplaces") to filter out infringing content in advance, based only on abstract not specific knowledge of infringements by particular users. Indeed the only concession the opinion makes to such notions is in accepting that where infringements have been notified so that an online site is aware of repeat infringers, it is reasonable to ask them to block access to such particular users as likely to infringe again, and even this can be done by the simple expedient of closing their account.

Most interestingly, in relation to hosting liability generally, not just injunctive relief, the *eBay* opinion also rejects the distinction drawn in a previous ECJ reference which had reached the court itself, between "*neutral"* hosting intermediaries who deserve the full benefit of Art 14 immunities, and "*non-neutral*" intermediaries who did not. The Advocate General took the view that the *eBay* case raised issues that were 'more complicated than [those in] *Google France and Google* in many aspects'.

In *Google France v Louis Vuitton, etc* (the first ECJ "AdWords" case, which also concerned intermediary liability for trade mark infringements by third parties, but in the context of a search site providing advertising listings, rather than "electronic marketplaces")[240], the question had been whether Google was liable for trade mark infringement because it allowed third parties to advertise on its site, using trade marks which were owned by competitors. The production of such adverts was fully automated as far as Google was concerned, using the Google Adwords system where clients "buy" certain keywords which then appear in ads displayed to users who include those keywords in searches. The key point was that Google did not stop a competitor to a trade mark holder from "buying" that trademarked word or phrase.

---

[236] *Tiffany (NJ) Inc v eBay,* US District Court of NY, SD Ny, No 04 Civ.4607(RJS).
[237] See *L'Oréal v eBay* [2009] EWHC 1094 (Ch) (22 May 2009). The case is pending as a reference to the ECJ, the questions asked of the ECJ by the English court have been finalised: see http://www.cpaglobal.com/newlegalreview/4213/ecj_reveals_terms_ebay_probe.
[238] Se see OUT-LAW News report, 15/8/2008, at http://www.out-law.com/default.aspx?page=9354.
[239] Supra n 193 and discussed in detail at p 50 of this report.
[240] *Google France v Louis Vuitton, etc, conjoined cases,* Judgment of the Court, Grand Chamber, 23 March 2010, Joined Cases C-236/08 to C-238/08.

The court held (as a separate point from the discussion on primary TM infringement) that Google's Adwords hosting business *was* entitled to claim immunity under Art 14 of the ECD, but only so long as "*Google's role [was] "neutral in the sense that its conduct is merely technical, automatic and passive pointing to a lack of knowledge or control of the data which it stores*."
It was not clear at the time if the word "*neutral*" here - not found in the main text of the ECD but drawn by the Advocate-General from recital 42 of the ECD - imported more restrictions than what Art 14 already says, or merely clarified it. Para 120 of that opinion expanded further that immunity under Art 14 was retained so long as the "*service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored"*. The qualification was crucial in the subsequent *eBay* reference, because L'Oreal argued that eBay was not neutral because eBay instructed its clients in the drafting of their advertisements and monitored the contents of the listings, as well (obviously) as making money (fee or commission) from those listings.

The A-G in *L'Oreal v eBay* however opined that the reference to recital 42 had been mistaken as that concerned "mere conduits" (art 12), not Art 14 hosts. Instead the *Google* court should have looked to recital 46, concerning "storage", which makes no mention of neutrality. He then went on to say (at para 142) that

"*It seems that if the conditions set out in Google France and Google for a hosting provider's liability [i.e. "neutrality"] are confirmed in this case to apply also to electronic marketplaces, an essential element in the development of electronic commerce services of the information society, the objectives of the Directive 2000/31 would be seriously endangered and called into question."*

And at para 146, he added that:

"*As I have explained, 'neutrality' does not appear to be quite the right test under the directive for this question. Indeed, I would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding storage of information uploaded by the users*."

Accordingly the A-G upheld only the letter of Art 14, namely that an intermediary performing the function of host could not be fixed with liability for one of its users without actual notice, and this, combined with "*the requirement of proportionality would in my opinion exclude an injunction against the intermediary to prevent any further infringements of a trade mark***"** (para 181).

On the second question of authorization, or vicarious liability, as conceived of in Art 14(2), the *Google France* court held (para 116) that "*the mere facts that the referencing service is subject to payment, that Google sets the payment terms or that it provides general information to its clients cannot have the effect of depriving Google of the exemptions from liability provided for in Directive 2000/31*." In this respect, the ECJ followed the US court in *Viacom*. Art 14(2) was not referred to in the *eBay* opinion. However the A-G did stress that, whilst eBay is generally exempted from liability for information stored by its clients on its website, it still remains liable for the content of data it communicates as an advertiser to a search engine operator.

The *eBay* opinion, if carried into law by the court, shows a marked reluctance, much more akin to the US courts than those of some European states, notably, France, to impose liability on hosts for user generated content, even where they make money from it. It also

however makes it clear that immunities go with *function* and not with a name for a class of intermediaries: so eBay could escape liability where performing the function of a host, but might still be liable as an advertiser for misleading information. The key arguments seem in the end (as with filtering) to be about practicality and economics, not moral or legal. Who should bear the cost of policing the online sale of counterfeit or copyright infringing material? The most obvious answer is the IP owner, since they most proximately make profits from enforcement activity. The costs of enforcement for online marketplaces are still high enough to drive some out of business if imposed, even though some degree of automation might be possible, and this as the A-G emphasizes, might "seriously endanger" e-commerce, with negative consequences for users and the marketplace alike.

Assessment

In the US *Viacom* case, (and indeed the US *eBay* case) the court basically declined to consider the ulterior motivations or anecdotal knowledge of the hosting intermediary, looking instead at the simple factual point of whether they had fulfilled their obligations to take down on notice and in some cases, remove repeat infringers. Across Europe, cases have gone various ways with very little predictability. In the ECJ *Adwords* case, the position has been more muddied by the use of the world "neutral". The *eBay* opinion if followed by the ECJ would remove the qualification of "neutrality" for hosts, though not it seems, for "mere conduits", cachers, advertising services which involve hosting, and possibly search engines *per se*.

There is an obvious tension here between the copyright P2P intermediary cases surveyed above – where considerable attention has clearly been devoted to the evidence of unlawful intention (see e.g. the US *Grokster*, Swedish *Pirate Bay,* and UK *Newzbin* cases, just as a representative international selection) - and the cases surveyed here involving UGC or UMC hosts, which seem more naturally to fall into the traditional regimes for intermediary immunity, such as the DMCA and ECD, where intention is more or less irrelevant, financial gain related to infringement not in any way conclusive and the real issues are actual notice or at the very least constructive awareness of a particular definite and specific kind (e.g. in respects of multiple repeat infringers). Since these cases lay on the borderline between the c 2000 DMCA/ECD approach, and the post *Napster* cases, they are of great interest.

For legitimate UMC hosting enterprises, subjective factors like intention would make it hard for a lawyer, let alone a small start up entrepreneur to predict in advance their risk; and requirements of *ex ante* filtering would make it difficult to stay in business. The effect could be to deter innovation, by making entrepreneurs reluctant to risk new forms of business model[241]. As has been seen, the web 2.0 boom, in the form of sites like Facebook, eBay, YouTube, Amazon and Google has very much been built on the back of risk management enabled by safe harbors and intermediary immunities.

[241] See report on suit in New York courts, *Ars Technica*, 22 November 2010, at http://arstechnica.com/tech-policy/news/2010/11/mp3tunes-safe-harbor-challenge-a-legal-test-for-cloud-storage.ars against MP3Tunes, self described as a cloud hosting provider but described by plaintiff EMI as an online "music locker". The CEO of MP£Tunes, Michael Robertson said: "This case will define digital media ownership in the 21st century. Can companies assist their consumers in storing thir possessions in the cloud where they can control them? That's the issue at stake."

X. ALTERNATE SOLUTIONS AND VOLUNTARY INITIATIVES

So far we have seen that while litigation strategies to reduce widespread copyright infringement such as suing users, suing P2P intermediaries, suing hosts of infringing content and even suing ISPs have had a degree of legal success in the last decade, they have failed to effectively bring an end to the P2P problem and look unlikely to do so. The newer legal solutions such as enrolling ISPs in graduated response regimes, with possible sanctions of traffic slowing, filtering and eventual suspension or disconnection, are as yet untested in effectiveness, but as detailed above, present together with some advantages also serious problems involving user rights and freedoms and the public interest.

In the report of 2005, we considered alternative solutions than legal action to the problems at hand. In 2010, the need to examine these seems as, or even more, pressing. We begin with what happened to some of the solutions canvassed in 2005 and move on to what seem to be the most promising emergent models in 2010.

Levies

The issue of levies has been on the agenda for a number of years. Levies, whether on hardware, software, physical media such as CDs or on bandwidth provided by ISPs, are widely used in continental Europe to compensate rightsholders for copying allowed by "private use" exemptions in those legal systems. Could, or should a system of levies be instituted to compensate content owners for unlawful filesharing?[242] Such proposals, while supported by many academics, have met with little enthusiasm from the rightsholder industries. For example, William Fisher at the Berkman Centre, Harvard, suggested in 2004[243] that copyright restrictions on sharing music files (though not other types of digital goods) should be removed, files shared freely and the revenues raised by a levy on bandwidth used would be proportionally distributed to rightsholders, using sampling techniques to determine which files were downloaded in what numbers. This would remove the need for technologies such as DRM (see below), allow artists a reasonable revenue stream and allow "semiotic democracy," i.e., the wide circulation of cultural materials as a kind of common good. Appealing as this may be, the content industries have largely opposed the extension of such "alternate compensation" schemes beyond limited cases such as private use or radio play, primarily because they do not maximize market return but only to a flat rate royalty determined by whoever runs the levy scheme[244]. In effect, such levies are compulsory licensing rather than allowing a market economy. Instead, what we have seen since 2001, when iTunes launched, has been the rise of various schemes which combine the idea of being able to consume music as a service for a fee, via various types of digital delivery rather than buying individual copies of files as physical or digital goods, but at a market-set and hence optimized rate.

Digital rights management (DRM)

The most pressing reason for rightsholders to oppose levy schemes in 2005 and earlier was that it was believed filesharing would soon be controlled by DRM systems instead. DRM is a term for access and copy control technologies that can be used by hardware

---

[242] For a number of differing views on levies see generally *Creators' Rights in the Information Society* (ALAI, Budapest, 2003).
[243] *Promises to Keep* (Stanford University Press, 2004).
[244] See further Mehra S, *The iPod Tax: Why the Digital Copyright System of American Law Professors' Dreams Failed in Japan*, Temple University Legal Studies Research Paper No. 2007-27 at http://ssrn.com/abstract=1010246.

manufacturers, publishers, copyright holders and individuals to limit the usage of digital content and devices. Both online music and music sold on physical CDs, it was believed, would be controlled by DRM, so that "ripping" and sharing without permission became difficult or impossible. Tethered platforms such as Apple's iPod where downloading was controlled via iTunes, successfully used such technology to create a market for selling music online without the risk of free copying of such files thereafter. DRM, it was hoped, would create a market where rightsholders could retain control over (and potentially charge for) every use consumers made of products purchased, including reading e-books, listening to music, and playing video content, plus other types of rights (printing, burning, streaming, backing up, sharing, etc). This DRM-assisted model was pioneered by iTunes and subsequently adopted by most online music sites, e.g. the legal version of Napster, each using different (and generally non-interoperable) DRM formats.

DRM however has fallen victim to widespread consumer opposition for a number of reasons[245]. Consumers do not like being unable to transfer music from one proprietary platform to another, nor having restrictions on the electronic version of a book (e.g. able to read it , but not print it, or lend it to a friend) which would not apply to its non electronic but still copyright analog equivalent[246]. When physical platforms become obsolete or break, transferring DRMed content to a new platform may be impossible. Applying DRM to physical media such as CDs proved to be technically difficult, with, in some cases, disastrous results e.g. the Sony BMG rootkit debacle[247], producing a severe consumer backlash. High profile cases were heard globally in which hackers circulated ways to crack various DRM formats around the Internet, and in some cases, were less or more successfully prosecuted under anti-circumvention laws: again, generally to consumer disquiet. Legally, although laws on anti-circumvention were successfully installed globally as a result of Art 11 of the WIPO Copyright Treaty, such laws have also become problematic as the difficulties of maintaining fair use and fair dealing exceptions in the face of DRM become apparent. Rights to circumvent works for public purposes, e.g. to assist the blind in accessing e-books, or to run software on non supported operating systems, have also been disputed in court and elsewhere. This development takes place at the level of national implementation as Article 11 of the WCT neither mandates DRMs nor does it protect technologies restricting acts which are permitted by law, such as under limitations and exceptions.

The end result has been that although DRM is still much used in relation to online music, software, e-book and computer game sales, it has disappeared from physical CDs, is largely circumventable, is "justifiably resented" by consumers (as Bridy puts it) and is arguably not the answer to preventing or even probably reducing mass music filesharing. In some of the major consumer online music shops, it has all but disappeared. Apple, for example, under consumer pressure first launched iTunes Plus, which offered higher quality DRM-free tracks for a higher price than its (then) normal 99c-price tracks with DRM, then in January 2009, announced that iTunes music would become available completely DRM free. Videos and software sold through iTunes continue however to use

---

[245] See further Bridy, supra n 68, at 568-582.

[246] For music, one of the key problems has been inability to copy music bought to simultaneously used multiple platforms, e.g. car, MP3 player, home computer, office; similarly with inability to play games on multiple computers. One key PR disaster related to Microsoft's music player Zune, which when launched did not support files previously purchased from Microsft's own previous DRM-protected music shop : see http://arstechnica.com/microsoft/news/2008/04/drm-sucks-redux-microsoft-to-nuke-msn-music-drm-keys.ars

[247] See discussion by Bruce Schneier, 17 November 2005, at http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html.

DRM.[248] Amazon and WalMart have also shifted to almost entirely DRM free distribution of music.

Legal music filesharing services

If you can't beat 'em, join 'em, goes the saying, and it has long been suggested that the answer to the problem of illegal downloading was not to sue P2P intermediaries into extinction, but to adopt their tactic of using the Internet, and the P2P protocol, as an effective delivery platform within a legal, paying model. Internet delivery of digital music has developed speedily in the last decade in the form of downloading and more recently, streaming particular content, but "legal P2P" for music - where music labels negotiate a blanket licensing deal with an ISP or other service provider so that subscribers can then file share without fear of sanction, by virtue of paying a monthly fee to the service provider - has yet to truly arrive on the market. Two key distribution models have taken root: downloads and streaming; and two business models, subscription and advert-supported (though the two are often combined as "freemium" – see below).

The digital download model was pioneered by Apple's iTunes store which opened in 2001; other successful online music download stores are now operated by many players including Sony and Amazon. An early example of the paying streaming model came from Napster, which having collapsed following the lawsuits described above, was reborn as a legal subscription site providing streaming of a large licensed catalogue of music for a flat monthly fee, and also, for an extra fee, providing downloads.[249]

More recently, free music streaming sites such as Spotify, We7 and last.fm have appeared[250] which pay for themselves with audio, display or text adverts, sometimes alongside the so-called "freemium" model. Such sites aim to provide the key advantages of the illegal infringing model in that, as well as music for free, they provide the convenience, choice and diversity which was lacking from the pre-P2P legal market for music on physical media; for example, being able to buy or listen to one track rather than the whole CD, allowing users to put together their own playlists from different record labels or genres, and being able to access music from multiple platforms e.g. home PC, iPod, work PC, mobile phone, etc. They also add attractive innovative features of their own: e.g. both last.fm and Spotify examine your music choices and those of other subscribers to the site to "recommend" to you more music you might like. (iTunes' Genius application now does the same for iTunes's download store). The streaming subscription model has also been successfully applied to video, TV and film by, most notably, Netflix (which now claims to account for 20% of downstream Internet traffic during peak hours in North American homes)[251].
Most recent has been the rise of bundled music services: selling free or subscription music services bundled with a platform such as your mobile phone (e.g. Nokia's "Comes with Music")[252] or a tablet such as the iPad, or bundled with your ISP subscription, or

[248] See http://en.wikipedia.org/wiki/Digital_rights_management.
[249] See e.g. http://www.napster.co.uk/.
[250] See *Guardian*, 10 December 2009, http://www.guardian.co.uk/media/2009/dec/10/personalised-online-radio-rajar , reporting a rise in uptake of such "personalised online radio services" from 2.9m in the UK in November 2008 to 4.5 million a year later.
[251] See "Will Netflix destroy the Internet?", *Slate*, 2 November 2010 at http://www.slate.com/id/2273314/.
[252] See *Guardian*, 3 October 2008, at http://www.guardian.co.uk/technology/2008/oct/03/nokia.nokia. However Nokia announced in January 2011 that it would be withdrawn from 27 of its 33 markets due to poor consumer uptake

[Footnote continued on next page]

mobile phone network subscription, as a flat rate add-on. Social networks are also beginning to take advantage of their massively popular platforms to work with music stores and sites: see e.g. the recently announced partnership between struggling music social network MySpace and global giant Facebook[253].

There has been much skepticism whether legal subscription online music schemes would pay their way ("you can't compete with free") or alternately, speculation that the *free* advert-supported models, such as basic Spotify, would not be able to make enough profit to survive. (Spotify's announced business plan is indeed to convert its customers from the free model to the paying subscription.) Although it is still early days, and many acclaimed sites involved are yet to move into profit[254], this skepticism seems tentatively ill-founded. One key point is that, as mentioned above, legal services are the "carrot" to the "stick" of graduated response; if the fees for online streaming sites remain low or free and the risk of legal action disappears by using them, this may be very appealing for some sections of the music market e.g. those older than their teens or twenties, with professional reputations to compromise. Statistics abound, but some indications of usage if not always of profit, are very positive. NetFlix, as noted above, now uses more bandwidth in North America than BitTorrent. Spotify has 7 million users in Europe of which 500,000 are paying customers, a high conversion percentage. In Sweden, a tenth of the entire population subscribe to Spotify, many paying 10 Euros a month for the premium service[255]. In a 2009 survey, music industry consultancy Music Ally found that "young users are increasingly switching filesharing activity to legal streaming services" with 65% of teens (ages 14-18) streaming music from sites like Spotify, YouTube and MySpace regularly, and 31% listening to streamed music every day[256].

Most notably, Finland, a market where filesharing has been rife, recently reversed a long pattern of overall decline in music sales with a 4.2% rise in total music sales (physical and digital) , which seems to be primarily related to the growth in bundled services provided by ISPs and mobile phone operators. In particular, while sales of music via mobile downloads actually fell in the first quarter of 2010 by 40%, subscriptions to bundled music subscription services available via mobile rose dramatically and accounted for a total 40%

[Footnote continued from previous page]

and rebranded in 6 developing markets as "Ovi Music Unlimited": http://moconews.net/article/419-nokias-comes-with-music-disappears-in-27-markets/. This failure is suggested to be due to lack of promotion by mobile networks offering competing music services; and on customer dislike of the "stringent" DRM. It was also reportedly fiddly to use, could not be activated in shop of purchase and was only available on a few handsets of the range (see http://www.theregister.co.uk/2011/01/17/nokia_comes_with_music_eol/). Subsequently however Vodafone has offered a bundled service Vodafone Music Unlimited, and 3 have struck a deal with Spotify: see http://www.techradar.com/news/phone-and-communications/mobile-phones/spotify-attacking-nokia-with-new-3-deal-643474.

[253] See *Guardian*, 18 November 2010, at http://www.guardian.co.uk/technology/2010/nov/18/myspace-announces-mashup-facebook-collaboration and see also *Guardian*, 27 April 2010 on links between Spotify, and Facebook and Twitter - http://www.guardian.co.uk/media/pda/2010/apr/27/spotify-facebook.

[254] Though see *Guardian*, 28 April 2010, at http://www.guardian.co.uk/media/2010/apr/28/we7-online-music-service , announcing that We7 had covered costs of licensing with its advertising revenues and was also paying a higher level of royalties to artists and record companies than comparable start up services.

[255] See James Gannon, supra n 194.

[256] "P2P activity drops but young people find other covert ways to share, finds survey" OUT-LAW News, 15 July 2009 at http://www.out-law.com/page-10168.

of digital music revenues. As a result digital music revenues arising from advertising (mainly via Spotify) rose by 68% to 600,000 Euros pa[257].

Experts believe that a promising future scenario is one where music (and other digital) services are cross-subsidized by platform operators or third parties like ISPs: so e.g. Nokia incentivizes you to buy their mobiles by offering a discounted – or "free" - "comes with music" service, or Virgin Media entices you from BT Internet by offering a cheap "all you can eat" legal P2P music service[258] for an extra £5 or £10 on the monthly broadband bill. Similar bundled new models might emerge for other types of digital content than music – e.g. we might see the *New York Times,* who recently launched an Apple iPad app which will be free initially[259], but then (like the London *Times*, paying), offering it free or discounted to certain customers as an incentive to buy both products (the London *Times* iPad app is already available free to those who buy the subscription to the paywalled website).

Revenue sharing for hosts and rightsholders

The cross- subsidization deals posited above are in effect a form of revenue sharing, where the platform operator and the music rightsholders pool resources to produce an attractive consumer product and share the profits, whether they come from sales of platform, ads or subscriptions. Similar new business models involving revenue sharing are also taking root in the social network, hosting, video streaming and mobile app markets.

A key example is YouTube' system Content ID, formerly known as "Claim Your Content", developed at least partly to protect YouTube from allegations of complicity with copyright infringement by its users (see section XI, above). Content ID allows IP rightsholders to submit a copyright video they wish protected to YouTube, who then encode it into a unique hash file, against which user-uploaded videos are compared. If the content to be uploaded matches, then the rightsholder can ask YouTube to reject it entirely, allow it to stay up (perhaps as advertising) or alternately to monetize it by placing ads next to it, with the rightsholder sharing in the revenue. Tim Wu has called this "tolerated use"[260] and it marks a significant diversion from the idea that unlawful content can only be take down or filtered out, to transforming it into a money making prospect. YouTube thus have voluntarily made available a system which combines conventional NTD with a degree of pre-emptive filtering, plus an option for revenue-sharing between platform and rightsholder. This solution however (a) places the onus on the rightsholder to do the first stage of the work of protecting their product, and (b) automates the rest of the process on YouTube's part, making it economically scalable in a way that would be difficult to imagine for non-automated *ex ante* filtering of infringing material (as of November 2010, 35 hours of video are being uploaded to YouTube every minute[261]).

---

[257] IFPI Finland figures, quoted from supra n 102.

[258] Virgin's longstanding attempts to launch legal P2P have so far foundered for lack of agreement on terms with major record labels: see http://www.guardian.co.uk/media/pda/2008/aug/13/ispsnewmusicservicewillpa and "Virgin puts legal P2P plans on ice", The Register, 23 January 2009 at http://www.theregister.co.uk/2009/01/23/virgin_puts_legal_p2p_on_ice.

[259] See http://techcrunch.com/2010/04/02/the-new-york-times-launches-free-ipad-app-for-real-now-paid-app-on-the-way/.

[260] Wu T, "Tolerated Use" (2008) 31 Colum. J.L. & Arts 617.

[261] See http://news.cnet.com/8301-13506_3-20022481-17.html?part=rss&subj=news&tag=2547-1_3-0-20.

Content ID is by no means the only such offering in the field voluntarily adopted by hosts or streaming sites. Audible Magic's system CopySense, for example, works in a similar way by comparing potentially infringing uploads to a database of millions of hashed copyright works but significantly does not offer the option of monetizing rather than blocking the detected unlawful content. It is used by several of the leading upload, hosting and streaming sites including MySpace, DailyMotion and Facebook[262]. Global File Registry, as we saw above does offer the option to divert a user detected trying to download illegal content to a legal alternative site, but seems not to have been widely adopted by the market yet although it is used in Altnet's reboot of KaZaa as a legal service.

There are clearly negative points for some rightsholders in embracing systems like Content ID. They allow the music hosting or streaming site a revenue stream from what might be seen as acquiescence in hosting or making available of infringing works; and exacerbate the loss of prior control by rightsholders over uses of copyright works (e.g. diverting priority access to the works from the rightsholder's own website to another site).

For users, a problem is whether content identification systems, rather like DRM, provide adequate scope for uploaders to take advantage of copyright exceptions, such as fair dealing or parody. In one famous example, a video on fair use and remix culture by copyright guru Lawrence Lessig was rejected by YouTube's automated system, because it contained a short clip of background audio which had not been authorized by the rightsholder. Content ID however now provides a counter-notice procedure (which Lessig successfully used to restore his video) which allows an uploader whose video is rejected to ask for manual reconsideration of the blocking[263].

In 2007, Principles for User Generated Content Services were proposed by a number of copyright owners, which include an obligation on UGC service providers to use "*effective content identification technologies with the goal of eliminating from their services all infringing user-uploaded audio and video content*". Note that the Principles also say that manual intervention *may* be added, and *if* it is, then it should be implemented in a way that "*effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use*.[264]" While NTD is still contemplated by the UGC principles (principles 8 and 9), it is clearly secondary to blocking. DailyMotion and MySpace are signatories to the UGC principles, but notably not YouTube or other major UGC players, and they are not implemented as law in any leading jurisdiction. For the moment, content identification systems seem to have been judicially accepted as a voluntary not mandatory obligation in the US (see *Viacom* decision above) with NTD still the primary *legal* obligation for such hosts.

Assessment

There seems to be no shortage of innovative business models emerging which might enable the music industry to thrive, nor does it seem the public are unwilling to embrace them. Among a multiplicity of surveys over the years, the trend emerges that users will, or at least say they will, pay if the price is right, and there is access to the right content, in the right way, across multiple platforms. The success of Spotify in Europe seems to bear

[262] See http://audiblemagic.com/clients-partners/contentsvcs.asp.
[263] See http://gigaom.com/video/youtube-silences-then-restores-lessig-presentation/.
[264] http://www.ugcprinciples.com/ especially at 3(f).

credence to these figures, as does the general shift from unlawful downloading to lawful streaming, whether supported by adverts or not[265]. For example one UK study found that 80% of users in 2008 were interested in voluntarily paying for legal P2P[266], while a study of Swedish users in 2009 similarly found that 86% of users would pay[267].

However, the key problems around the launch and expansion of such services remain the reluctance of the music industries to license properties to such services, and the terms of such licensing. It took competition from illicit P2P initially to spur the record labels into licensing their products as digital downloads to iTunes and later, other online music stores, and progress in multi-site or blanket licensing remains slow[268]. Sean Parker, who notoriously launched the first Napster P2P site in 2001, recently acquired a share in Spotify, and is seeking to relaunch it in the USA. Spotify's US launch has already been postponed several times, however, because of delays in securing deals with the major labels. Talks with EMI, Sony, Universal, and Warner are ongoing. According to the *Independent*, in October 2010: *"Mr. Parker has said that he hopes it could get the go-ahead by the end of the year, but some industry analysts remain doubtful"*. In April 2011 however another delay was announced.[269]. Licensing for monetizing "legal P2P" - which would involve unlimited downloads without DRM, as well as streaming, across an inclusive cross-label repertoire of artists - seems particularly difficult to achieve, with attempts by Virgin Media to launch such in the UK unsuccessful due allegedly to record label pressure since January 2009[270].

Against this background, the EU Commission appears to be becoming impatient about the failure of the industry to advance the state of new business models, rather than concentrating on punitive measures against filesharers. Viviane Reding, the EU Commissioner, gave a speech in June 2009 putting equal blame for the problem of unlawful content on the record labels for dragging their heels in giving customers what they want:

"It is necessary to penalize those who are breaking the law, but are there really enough attractive and consumer-friendly legal offers on the market? Does our present legal system for Intellectual Property Rights really live up to the expectations of the Internet

---

[265] See e.g. http://evolver.fm/2010/11/10/streaming-music-more-popular-than-downloading-music-france/ (French stream more music than download for first time, November 2010); Nielsen Report, January 2011 found that three times more people surveyed (of 20,000) had recently streamed music as opposed to (legally)downloaded it (http://www.musicweek.com/story.asp?storycode=1043858); interestingly in the latter survey a multiplicity of platforms were used for streaming: 21% of respondents streamed music on their mobile and 23% watched videos on their handsets , 36% streamed music to the PC, 35% accessed music via a social networking site, 30% listened to music files on their phones and 27% used portable music devices such as MP3 players. Finally in a Tunecore poll of musicians only, in April 2011, 82% predicted more streaming than downloading in the future: http://www.online-mixing.com/2011/04/tunecore-poll-82-say-more-will-stream-than-download-music/.

[266] See http://www.theregister.co.uk/2008/06/16/bmr_music_survey/.

[267] See http://www.theregister.co.uk/2009/04/23/sweden_p2p/.

[268] Some artists who control their own rights have also historically refused to be sold as digital downloads: see the jubilation at the Beatles finally being sold on iTunes in November 2010, e.g. http://www.guardian.co.uk/music/blog/2010/nov/16/itunes-beatles-expectation.

[269] See http://www.independent.co.uk/news/world/americas/music-pirate-launches-new-assault-on-us-2120496.html , 30 October 2010. No US launch had been announced as of 1 April 2011 inspiring the following amusing April Fool : http://eu.techcrunch.com/2011/04/01/spotify-announces-us-launch-closing-european-service-to-fund-it/.

[270] See http://www.theregister.co.uk/2009/01/23/virgin_puts_legal_p2p_on_ice/.

generation? Have we considered all alternative options to repression? Have we really looked at the issue through the eyes of a 16 year old? Or only from the perspective of law professors who grew up in the Gutenberg Age? In my view, growing Internet piracy is a vote of no-confidence in existing business models and legal solutions. It should be a wake-up call for policy-makers[271]".

It is clear that cross-label, cross-platform, multi-jurisdictional licensing, and especially licensing for true legal P2P, is a topic needing detailed investigation, as to competition and contract as well as copyright, and with account taken of interlocking issues like orphan works, deleted back catalogue, open licensing and private use exceptions. The existing framework of copyright law and copyright licensing, where rights are divided up by jurisdiction, and in music, widely distributed between composers, lyricists, musicians, publishers and recording companies makes such licensing deals laboriously hard to achieve for start ups trying to offer innovative music services. ISPs or other providers which might offer such services also vary enormously in size, bargaining power and vertical integration with content providers. Rightsholders often now have existing agreements for online licensing e.g. with iTunes, and perhaps relatively little incentive to seek other licensing partners. Some countries e.g. recent EU Accession countries, though with developed potential music markets, often lack access to any legal online music services at all.

The EU launched a reflection document in October 2009 which canvassed options for creating a European single market in creative content[272] in which they suggested a greater role for extended collective licensing, and a possible pan-European or multi-territory licensing process, as well as a need perhaps for more fundamental harmonization of EU copyright laws. WIPO has also taken a lead in this area with its conference on copyright licensing and access to culture in Geneva in October 2010[273] and publication of these results will be valuable.

Interestingly, the Society for Computers and Law in the UK (a group representing lawyers primarily acting for large commercial businesses rather than a digital freedom group) questioned in June 2010 in their paper on *Digital Music and Online Intermediaries*[274] if a practical licensing system to promote innovation could be left to develop via commercial negotiation, especially given the possibility of the content industries sticking to their existing business models predicated on copyright control over selling physical or online copies of music and video works, and bolstered by legal frameworks such as volume litigation against users and graduated response.

"*There is real uncertainty*", they said, "*whether sufficient incentive exists for concerned parties to negotiate such a licensing system while content owners retain the option to sue individuals and intermediaries.*"

Accordingly they concluded that:

---

[271] Quoted by *Ars Technica*, November 4 2009 at http://arstechnica.com/tech-policy/news/2009/11/record-labels-keep-blaming-p2p-but-its-a-hard-sell.ars.

[272] *Creative Content in a European Digital Single Market:* Reflection Document of DG INFSO and DG MARKT, 22 October 2009 at http://ec.europa.eu/avpolicy/docs/other_actions/col_2009/reflection_paper.pdf.

[273] See http://www.wipo.int/pressroom/en/articles/2010/article_0045.html.

[274] See http://www.scl.org/site.aspx?i=ed16493.

"*..the only identifiable solution at present is a compulsory licensing system, similar to the statutory schemes which were established to allow recordings to be made during the early development of the phonograph. The advantage of a statutory scheme is that the law can establish both pillars (free private use and license fees) simultaneously. Although neither the music industry nor ISPs are presently in favor of such a scheme, it may turn out to be the only way in which a legitimate framework for online music consumption can be established"*.

Are we back to the concept of compulsory licensing dismissed at the start of this section?[275]

XI. CONCLUSION: THE FALL AND RISE OF ONLINE INTERMEDIARY LIABILITY FOR COPYRIGHT?

In November 2010, Neelie Kroes, EU Commissioner and Vice President for the Digital Agenda made a significant speech, declaring that:

"Just [as] cinema did not kill theatre, nor did television kill radio, the internet won't kill any other media either... Take copyright. For 200 years, it has proved a powerful way to remunerate our artists and to build our creative industries. But copyright is not an end in itself. Copyright exists to ensure that artists will continue to create. Yet we see more and more often that it is not respected. In some sectors, the levels of piracy demand that we ask ourselves what are we doing wrong. We must ensure that copyright serves as a building block, not a stumbling block. Today our fragmented copyright system is ill-adapted to the real essence of art, which has no frontiers. Instead that system has ended up giving a more prominent role to intermediaries than to artists. It irritates the public, who often cannot access what artists want to offer and leaves a vacuum which is served by illegal content, depriving artists of their well-deserved remuneration. It may suit some vested interests to avoid a debate, or to frame the debate in moralistic terms that merely demonise millions of citizens. But that is not a sustainable approach. Time alone will not solve the problems that have emerged." [276]

How should copyright law respond to the overwhelming pressures detailed above? From the above survey, it seems certain lessons can be learned, and some avenues for further work proposed.

– The issue of the liability of online intermediaries for copyright infringing content cannot be divorced from the general issues around immunities or safe harbors for intermediaries in respect of other types of content, such as obscene or hate speech, child pornography and libel. However it may need to be considered if "one size fits all" horizontal regimes, such as the EC E-Commerce Directive (ECD) are still in principle workable or desirable.

– There has been reasonable global consensus that notice and take down (NTD) paradigms represent a fair and practicable balance between the interests of online intermediaries, the public and those damaged by unlawful content or activities online. Problems remain with NTD paradigms in relation to potential chilling of free speech, due

[275] See also "Behind the music : Why can't labels agree on a music streaming service?" *Guardian*, 22 November 2010 at http://www.guardian.co.uk/music/musicblog/2010/oct/18/record-labels-unified-streaming-service.

[276] See http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/619.

to lack of public oversight of demands for take down of content; and due to uncertainty as to the extent of immunities for new linking intermediaries such as search engines.

– Responsibilities beyond NTD, such as content identification and filtering, may be appropriate and feasible for some intermediaries but not for others, depending on practice and resources. Any attempt to extend intermediary duties beyond NTD should be carefully examined for impact on other interests and on human rights.

– Despite the fact that traffic flows freely around the globe via the Internet, rules even at the NTD level relating to online intermediary liability are not globally harmonized, with significant dissensus even between the US with the CDA s 230 (c) as well as the DMCA, and the EC regime. There is a role here for international agreements to play in establishing uniform rules, providing certainty for intermediaries and businesses, and safeguarding user rights across the globe. In this regard apart from any possible role for WIPO, it should be noted that the EC is looking currently at reform of the ECD and that the OECD is also engaged in formulating global guidelines on online intermediary liability.

– The advent of P2P filesharing, and to a lesser extent the use of hosting and streaming sites to perpetuate copyright infringement, has damagingly destabilized any global consensus on the role and liability of intermediaries, not only among states but between rightsholders, intermediaries and the public as stakeholders. In particular, the previously successful NTD paradigm fails to have any impact on P2P intermediaries, since they do not host the files they enable to be shared. Hosts of content for download or streaming situated in law havens, or otherwise beyond the effective control of rightsholders, have also reduced the value of NTD to the content industries.

– Attempts over the last decade to control unlawful filesharing have thus turned to lawsuits against those who might be seen as most obviously culpable - P2P intermediaries, and users of P2P. Arguably these have failed, leading the content industries to turn to other means of regulation such as graduated response and filtering, which however justified, may involve considerable overheads in terms of “collateral damage” to user rights, and costs to intermediaries and society.

International expert evidence, and experience in countries where schemes have been implemented is yet incipient. However, preliminary findings show that though graduated response has significant advantages of speed, cheapness and educational value, it may also have substantial downsides in that it may (i) infringe user rights to due process, for example, “presumption of guilt” (ii) lack basic legal, organizational and technical safeguards to ensure that allegations of infringement against users are transparent, error free and independently verified (iii) infringe basic rights of privacy and protection of personal data (iv) infringe basic rights of freedom of expression (v) reduce digital inclusion, increase the cost of Internet access and create problems for lawful intermediaries such as universities and open Wi-Fi providers; and (vi) breach existing legal immunities guaranteed online intermediaries in many states. These results raise the question of whether graduated response, despite the advantages listed above, represents a proportionate response to the problems of online infringement.

– Furthermore, while not the main focus of this report, it should be noted that there is also as yet no clear evidence that the benefits in reduction of unlawful filesharing to industry, will exceed the total costs, economic and non-economic, of implementing graduated response. Furthermore there is no consensus on how the economic costs should be shared between the content industries, online intermediaries and the state.

– Any attempt therefore to introduce graduated response as a mandatory system for users (whether by legislation or by industry agreements with intermediaries, and particularly by virtue of international agreement) should be subject to a prior empirical investigation, independent of both state and industry interests, in which an assessment is made on whether proposed laws are appropriate, legitimate and proportionate. Any such assessment should take account not only of economic interests but also of (a) non-economic damage to fundamental freedoms such as due process, privacy and freedom of expression, both for individuals and for society as a whole (b) the public interest in digital inclusion and in promoting innovation and (c) the state of incentives to create a market for legal alternatives to unlawful filesharing. It would also be useful to assess if any new scheme might work better to prevent the abuses of process that have been identified in current volume litigation practice.

– Other alternatives than full graduated response should also be examined, for example whether "notice and notice" schemes combined with access to new legal alternatives can alone produce an effective and fair return for artists and/or publishers. International guidelines on these threshold tests for when a graduated response scheme can be justified would be welcome.

– If graduated response schemes, as at present, continue to be implemented by individual domestic laws, or by agreement (voluntary or coerced) between rightsholders and intermediaries, there is clearly a role for international guidelines on its scope and procedures as well as on the safeguards which must be put in place at the same time to protect user rights and fundamental freedoms; to fairly allocate the costs of the process so as not to impede digital inclusion; and to continue to incentivize the creation of legal alternatives to replace unlawful filesharing.

– Particular attention must be paid to some kind of independent scrutiny of accusations of alleged copyright infringement *before* any sanctions are imposed, as well as access to review afterwards, as the Internet Freedom clause demands. Users should have access to redress for economic, reputational and privacy harms caused by false or negligent allegations in a way that effectively discourages such.

– Content filtering, including traffic slowing, website blocking and deep packet inspection (DPI) involve crucial issues as to the legality of blanket monitoring, data retention, and restrictions on freedom of expression, etc, on which there is no consensus across Europe, let alone globally. International research and guidelines here would be of great help before any of the current legislative approaches being suggested in , inter alia, the UK, US, Spain and Korea, become established as practice.

– While WIPO remains the natural venue for discussion on the distribution of creative content in the digital environment any possible international guidelines should take into account the general work that is going on relating to the need for an international "bill of Internet rights" [277] within the Internet Governance Forum process, and in other regional venues concerned with Internet user rights and freedoms, such as the Council of Europe.

– The international copyright policy community should consider what steps, legislative or otherwise, might facilitate the new business models emerging for delivery of online music services and other digital copyright products, since these offers the best

[277] See http://internetrightsandprinciples.org/.

opportunity for a fair return to artists and publishers, at the least cost to users and the public interest. The issue of compulsory licensing and /or levies, possibly as an interim solution until new business models mature, should also be considered.

[End of document]