QUELLING P2P INFRINGEMENT
PRIVATE AMERICAN HARBOURS OR PUBLIC FRENCH GRADUATIONS?

David J Brennan
Melbourne Law School

Two basic legal models have evolved to tackle the problem of unlawful P2P distribution: safe harbour and graduated response. This article will discuss the two models, with a focus on the American safe harbour regime and the French graduated response regime. Also considered is the open question of what will occur in Australia in the aftermath of the High Court's denial of ISP liability in Roadshow Films v iiNet.

INTRODUCTION

In the wake of the High Court decision in *Roadshow Films v iiNet*[1] there is a renewed focus on the Australian formulation of an industry code of conduct to address the unlawful distribution of content on peer-to-peer (P2P) networks. The attempt to arrive at the code is being undertaken through negotiations between peak industry players – most notably copyright owners on the one side and Internet Service Providers (ISPs) on the other – with the discussions being brokered by the Commonwealth Attorney-General's Department. However it is being played out in trying circumstances, and at the time of writing it is difficult to imagine the exact form of any such code that will satisfy all interested circles.

The code in question is an optional aspect of the regime comprising the *Copyright Act 1968* (Cth) Part V, Division 2AA – Limitation on Remedies Available Against Carriage Service Providers; the Australian safe harbour.[2] That regime has its provenance in US law, and the prescriptive nature of the 2004 US-Australia Free Trade Agreement, which obliged Australia to essentially adopt the US safe harbour.[3] While the US safe harbour was enacted in 1998, and unlawful P2P distribution has been a thorn in the side of copyright owners since 1999, it was not until 2011 that a Memorandum of Understanding was arrived at in the US, which has seemingly normalised relations between copyright owners and ISPs in a joint response to unlawful P2P distribution. In the meanwhile, an alternative has arisen in the form of graduated response laws, of which the French HADOPI regime of 2009 is both the prototype and remains today the standard bearer. Since the French initiative, other countries – including South Korea, the UK and New Zealand – have adopted similar types of laws. Loosely speaking, such laws are more strongly orientated as 'public law' regulation, in contrast to the industry self-regulation invited by the safe harbour laws.

Thus, two basic legal models have evolved which can tackle the problem of unlawful P2P distribution; safe harbour copyright remedial limitations and graduated response regimes in public law. At a time when Australia is grappling with what to do about that problem, it is timely to consider in some detail the provenance and the contours of the two 'original' models – the US safe harbour and the French graduated response regime. That consideration enables deeper thought about the open questions at hand in Australia: what might occur in Australia in the aftermath of the High Court's denial of ISP copyright liability in *Roadshow Films v iiNet*?

This essay attempts that exercise, with a focus upon some of the key drivers that helped to shape the US safe harbour and the French HADOPI laws and explains the application of both regimes to the problem of unlawful P2P distribution. In so doing some concluding observations can be made about the ramifications of the High Court's decision upon efforts to resolve the problem in Australia, and the type of posture that may be required from the Australian government for progress to be made here.

THE AMERICAN SAFE HARBOUR

THE ORIGIN OF THE US SAFE HARBOR REGIME

A July 1994 preliminary draft report was published by a Clinton Administration appointed intellectual property working group on the (so-called) National Information Infrastructure (NII). It observed, based on the then US case law, that copyright owners may allege indirect copyright liability against online service providers (Information Infrastructure Taskforce 1994, [6c]). This observation grew into a lengthy discussion in the group's September 1995 final report. The discussion reported that 'there is a view that on-line service providers ... should be exempt from liability' – presumably in a reaction to the observation in the July 1994 draft report – because 'that exposure to liability for infringement will drive service providers out of business' (Infrastructure Taskforce 1995, 116). However any special treatment for on-line service providers was emphatically rejected in the final report as premature, as it might choke the 'development of marketplace tools that could be used to lessen their risk of liability and the risk to copyright owners' (Infrastructure Taskforce 1995, 123). Pointedly, the 1995 NII report noted that:

> *Service providers expect compensation for the use of their facilities – and the works thereon – and have the ability to disconnect subscribers who take their services without payment. They have the same ability with respect to subscribers who break the law* (Infrastructure Taskforce 1995, 122-123).

Positions adopted in the 1995 NII final report informed the US position at the 1996 WIPO *Diplomatic Conference on Certain Copyright and Neighboring Rights Questions*. The US stance was substantially pressed to colour the two WIPO treaties there concluded. However, service providers formed part of an orchestrated opposition to the pro-copyright policies of the Clinton Administration that were reflected in the 1995 NII final report and Congressional Bills introduced in its wake. The issue of special copyright treatment for online service providers was revisited, and an inter-industry deal was reached. Writing in 2001, an academic involved in the policy contest described the essence of the deal thus:

> *Content owners agreed that Internet service providers should not be liable for their subscribers' infringing transmissions so long as the provider had no reason to suspect infringement was taking place, on the condition that the service provider agreed to shut down copyright violators and remove infringing material as soon as a content owner notified it of a violation* (Litman 2001, 135).

The deal became known as the 'safe harbour' of the 1998 Digital Millennium Copyright Act and has, since 1998, been exported by the US through a series of bilateral free trade agreements – including the US-Australia Free Trade Agreement of 2004. In essence, the 'safe harbour' comprises four categories of activity or thing occurring at the behest of an online service provider's subscribers, for which the service provider will have, upon fulfilment of statutory conditions, immunity from monetary copyright liability. The four categories are:

A – facilitating transitory digital network communications;

B – the provision of system caching;

C – storing material on systems or networks at the direction of users;

D – the provision of online location tools.

Each category has its own array of conditions that the service provider needs to satisfy to be eligible for the immunity. However, one condition that applies for all categories is that the service provider 'has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers'.[4]

While the safe harbour regime was arrived at through a compromise between the US copyright and communications industries in the mid 1990s, it has an economic justification. Once it is accepted that online service providers are appropriate to be considered for indirect liability arising from the infringements which their services enable – because they are in a good position to deter that infringing conduct – a cost-benefit question arises in deciding whether indirect liability should arise, and if so on what basis. Appropriately weighing costs against benefits requires taking into account several factors, including:

(i) whether it is plausible that direct liability alone against actual infringers would be effective;

(ii) would the creation of indirect liability deter the infringing conduct at a lower cost than direct liability alone;

(iii) would the creation of indirect liability assist the party incurring the liability in making an efficient decision to avoid that liability; and

(iv) would the creation of indirect liability interfere unreasonably with legitimate activity (Arrow et al 2005).

Considering P2P infringement, the safe harbour regime can be seen to be justified by all of these factors. Fundamentally, it is implausible to enforce copyright directly in an efficient manner against infringers. On the other hand, the regime not only shields service providers from liability arising from their customers' infringing acts, but it does so by seeking to minimise the prevalence of those infringing acts in a way that imposes least litigation cost on all concerned. The immunity and the conditions for eligibility (such as the requirement for a repeat-infringer account termination policy) provide (in theory) incentives for non-litigious, cooperation between service providers and copyright owners to achieve multiple objectives: facilitate the provision of legitimate communications services; minimise copyright infringement; and avoid litigation expense.

However when applied to the problem of P2P infringement, the safe harbour scheme has revealed itself to be challenged in both the US, and now Australia, for the same basic reason. P2P activities most obviously fall within category A of the four activity categories, although (as will be explained below) in two important US cases it was argued that an aspect of P2P distribution could also fall within category C. The regime ultimately rests upon a presumption (that can be traced back to the 1994 and 1995 NII reports) that the A-D activities were included in the safe harbour immunities because they potentially gave rise to copyright liability. For ISP liability in relation to their subscribers' P2P activities that presumption has been revealed to be questionable.

ISP LIABILITY FOR SUBSCRIBER-RELATED P2P ACTIVITIES UNDER US COPYRIGHT LAW

Under US law what liability**,** considered in terms of the A-D safe harbour activities, could arise in an ISP as a result of P2P infringements undertaken through the use of some of its customers' internet connections? The short answer, in this 'ISP-P2P setting', is that the ISP has no clear liability. In the past decade there have been two ways to consider the potential US copyright liability of ISPs in the ISP-P2P setting:

(i) secondary liability from category A activities – facilitating transitory digital network communications; or

(ii) direct liability from category C activities – storing material on systems or networks at the direction of users.

In view of the US jurisprudence the former is seemingly difficult to establish in the ISP-P2P setting, while the latter has been specifically rejected by two intermediate appeal courts.

Liability for P2P transmissions: category A activities

Since the 2005 Supreme Court decision in *MGM v Grokster*[5] secondary liability in the US requires a finding that the relevant ISP falls within one of three categories. In the ISP-P2P setting, an ISP will be secondarily liable if it:

- Contributed to the P2P infringement;
- Is responsible vicariously for the P2P infringement; or
- Induced the P2P infringement.[6]

To have *contributed* to P2P infringement the ISP must be shown to have materially contributed to the infringement by supplying the facilities and, because for a general service those facilities may have both infringing and non-infringing uses, the ISP must also be shown to have 'specific' knowledge of the P2P infringement at the time of the material contribution. Can such knowledge be established outside real-time ISP monitoring of customers?

On this point, the DMCA safe harbour notably makes a privacy protection explicit; it imposes neither an obligation upon service providers to monitor their services nor any requirement to seek-out facts which would indicate infringing activity. As such, the knowledge requirement looms as a significant (albeit perhaps not insurmountable) hurdle in US law to overcome in order to establish contributory ISP liability in the ISP-P2P setting.

In the *Grokster* litigation itself, the intermediate appeal court concluded that the publishers and distributors of P2P software (which has both infringing and non-infringing uses) did not fall into this liability category because they lacked at any relevant time 'actual knowledge of specific instances of infringement' (545 US 913, 927-8 (2005)).[7] Ultimately the Supreme Court decided the case on a newly-established basis of inducement liability in copyright and did not disturb this holding.

For an ISP to be *vicariously responsible* in the ISP-P2P setting, it must be shown to have received a financial benefit directly attributable to P2P infringements, and to have also held a (non-exercised) right and ability to stop or limit that infringement. As one commentator observes, 'whether ISPs have the right and ability to control the behaviour of peer-to-peer users may not be a trivial question' (Elkin-Koren 2006, 50). This is especially so given the above-mentioned privacy protections embedded into the safe harbour scheme. Moreover, one US authority has suggested that a general purpose ISP did not receive a sufficiently direct financial benefit from providing infringers access to another form of online distribution: USENET.[8] Returning to the *Grokster* case, the P2P software publishers were found (in the intermediate appeal court) to have had neither the right nor the ability to stop infringements occurring over the network their software facilitated (545 US 913, 928 (2005)).

Inducement liability requires, in the ISP-P2P setting, that the ISP both supplies the facility that may be used to commit direct infringement and does so with the intention of promoting that infringement. Such an intention could be evidenced by assessing the totality of the conduct (including omissions to act), statements and any financial benefit accruing to the alleged inducer. In *Grokster*, the defendants had specifically targeted users of another P2P network (Napster) that had been effectively shut down by prior rights holder legal action, failed to attempt to develop filtering tools and sold space for advertising that would be directed at their P2P users.[9] Notably, the creation of copyright inducement liability was a response to the Supreme Court's acceptance of the inapplicability of either contributory or vicarious liability to the P2P software publishers. Would such liability be apt for in the ISP-P2P setting? It seems highly unlikely, as it is improbable that any mainstream ISP would ever engage in conduct that is tantamount to actively promoting P2P infringement.

The consequence of this analysis is that an ISP in the US, when it acts as a category A conduit in relation to P2P infringements occurring over its customers' connections, has no obvious secondary liability for those infringements. Importantly, this conclusion stands even if rights holders acted (as did the rights holders in the *Roadshow Films v iiNet* litigation) to furnish the ISP with weekly information about those P2P infringements. To the extent liability is conceivable in that setting under the current state of US law, contributory (rather than vicarious or inducement) liability seems the most plausible form of liability. Such a notice stratagem would likely give rise to complex questions in the US about the scope of contributory liability in such a setting. As Elkin-Koren (2006, 37) observes, since ISPs supply services capable of significant non-infringing uses contributory liability would require establishing 'reasonable knowledge of specific infringing files' at the time during which the ISP defendant materially contributed to the infringement.

Because right holders' notices to an ISP are always a report on past P2P infringements, on this view of US law contributory liability is speculative at best. In other words, notice of past infringing conduct to an ISP may fail to establish that the ISP had requisite knowledge of infringement at the time at which it was supplying Internet access. Notice of past infringing conduct (and ISP inactivity) may be insufficient to establish that the ISP is 'acting in concert with the infringer' (Nimmer 1978-, §12.04[A][3][a]). The ISP-P2P setting might create no US copyright liability in an ISP for related category A activities.

Liability for 'making available' via P2P: category C activities

Could it be said however – at least to the extent that an ISP's customer infringes by making available content to members of the public in the P2P network – that the ISP was engaging in a category C activity, which created in it direct liability by storing material on systems or networks at the direction of users? The Record Industry Association of America had, in the past, assumed that such an ISP was engaged in a category C activity.

For a remedial limitation attaching to category C activities – 'storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider' – a safe harbour obligation requires that a service provider must, upon specified notification from a rights holder of alleged infringement, respond 'expeditiously to remove, or disable access to, the material'.[10] A further aspect of the safe harbour enables a rights holder who has prepared that specified notification to have granted from the clerk of any US District Court a subpoena directing the service provider to reveal the identity of the suspected infringer.[11]

At some stage ten or so years ago the Record Industry Association of America (RIAA) commenced seeking these subpoenas in order to obtain the identities of ISPs' subscribers whose connections were identified (through their pseudonymous IP addresses) as making available RIAA-members' sound recordings on P2P networks. Two ISPs – Verizon and Charter Communications – challenged the issued subpoenas on the basis that they could never be validly grounded within the ISP-P2P setting. Both the District of Columbia Circuit in 2003 and the Eighth Circuit in 2005 agreed with Verizon and Charter Communications respectively. In *RIAA v Verizon* Ginsburg CJ, writing for the court, explained that it was clear that the subpoena provisions applied 'to an ISP storing infringing material on its servers ... and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber' (351 F 3d 1229, 1237 (2003)). The Chief Judge then went on to observe more generally on the ISP-P2P setting:

> *The legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works. That is not surprising; P2P software was not even a 'glimmer in anyone's eye when the DMCA was enacted'* (351 F 3d 1229, 1238 (2003)).

In *Re Charter Communications* the Eighth Circuit by majority agreed, observing that 'as a court we are bound to interpret the terms of the statute and not to contort the statute so as to cover the situation presented by this case' (393 F 3d 771, 777 (2005)). As a consequence of these cases, rights holders have reverted in P2P cases to the long-established litigation procedure of seeking, in actions against John Doe, the issue of subpoenas requiring John

Doe's ISP to divulge the defendant's actual identity (Brenner 2012). And significantly, an implication of the decisions is that a subscriber's making available of files on a P2P network does not involve the relevant ISP in any Category C activity that could give rise to liability in the ISP.

Moreover, leaving aside these specific authorities, there remains one other major obstacle in the way of direct liability in any service provider engaging in category C activities at the behest of subscribers; absence of volition. While the decision has been cogently critiqued (Ginsburg 2008), the Second Circuit holding in *Cartoon Network v CSC Holdings* (536 F 3d 121, 2008) can be seen as standing for the proposition that any centralised storage service which involves itself in copyright exploitations merely by being reactive to the commands of subscribers, lacks the necessary element of volition for direct liability to be established in the service provider. Under this approach it is only the subscribers to the service who are directly exercising any copyright through their use of the service. Thus, whether by the *Verizon/Charter Communications* finding or the *Cartoon Network* principle, issues of service provider liability in the ISP-P2P setting seem to most obviously rest in US copyright law with arguments based on the potential applicability of one of the theories of secondary liability.

THE 6 JULY 2011 MEMORANDUM OF UNDERSTANDING

The fragility of any successful argument that an ISP has liability in the ISP-P2P setting leads to the following conclusion. If the ISP has low risk or no risk of liability arising from the setting, the incentives to comply with the eligibility conditions to enter the safe harbour are reduced.

However, while the incentives are affected, the requirement for a repeat-infringer account termination policy exists for all activities protected by the safe harbour regardless of whether any protected activity creates copyright liability in the ISP. That is to say, the absence of any ISP liability within the ISP-P2P setting, would not excuse the ISP from a failure to adopt an account termination policy for repeat P2P infringing subscribers. Moreover, such a failure would seemingly deny the ISP eligibility for all of the safe harbour liability limitations – e.g. absence of a qualifying policy for P2P infringing subscribers would disentitle the ISP from the limitation from liability for an unrelated activity such as system caching.[12] It is unclear what – if any – role this consideration has had in explaining the 6 July 2011 Memorandum of Understanding arrived at in the US between major rights holders and about 60% of the US ISPs (the '2011 MoU').[13] Other commercial considerations – such as the desire of ISPs to partner with content producers to differentiate their services – have been identified as incentives for ISPs to arrive at agreement (Brenner 2012). Also, and as will be explained, whatever else the 2011 MoU might represent it is not in itself a safe harbour repeat infringer account termination policy.

The 2011 MoU needs to also be viewed with a backdrop of emerging graduated response laws. As is discussed below, starting with France in 2009, other countries had begun to enact more public law orientated graduated response regimes. These regimes, unlike the safe harbour approach, are not predicated on supplying incentives to ISPs to cooperate with rights holders so as to minimise their liability risk. Rather, they place a direct public law obligation on ISPs to comply with a legislated regime, administered by a public body, and designed to facilitate a diminution in infringing P2P activity. The French scheme – very much the gold standard for graduated response public law – is discussed in the next section. The Obama Administration played a material behind-the-scenes role in negotiations (Kravets 2011) and welcomed the final result (Espinel 2011). The French solution, and the possibility of US Congressional action *in lieu* of agreement, was presumably in everyone's mind.

Under the terms of the 2011 MoU, a private body named the Centre for Copyright Information (CCI) is established in which both rights holders and ISPs hold an equal stake. The CCI has primarily a public education role, but under the 2011 MoU also oversees the formulation of methodologies relating to the making by rights holders of allegations of P2P infringement, and the matching by ISPs of those allegations to subscribers' accounts. Alerts – as described below – are sent to the matched subscribers and an obligation exists in ISPs to

produce monthly reports for rights holders of subscribers (uniquely identified in an anonymised form) who have received copyright alerts.

The 2011 MoU sets out a four-step 'Copyright Alert' process that any participating ISP is obliged to adhere to. Assuming that continuing allegations are matched to a subscriber's account, in summary the steps that must be taken by the ISP are as follows:

(i) Initial Education – up to two alerts sent to a subscriber which informs the subscriber that copyright infringement is illegal and that repeated alerts may lead to mitigation measures;

(ii) Acknowledgement – up to two alerts requiring the subscriber to agree to cease infringing or to confirm that the subscriber has instructed other users of the subscriber's account to cease infringing;

(iii) Mitigation Measures – a further alert giving the subscriber notice that there will be restrictions (such as throttling) placed on the subscriber's account, with both a mechanism for a subscriber to seek review and a discretionary ISP waiver being available to hold off such restrictions;

(iv) Post Mitigation Measures – these may involve the imposition of further mitigation measures but significantly, the ISP must both:

  (a) Inform the subscriber that continued infringement may, in appropriate circumstances, result in account-termination under a policy required to be applied in order to be eligible for the safe harbour limitations; and

  (b) Continue monthly reporting to rights holders of the number of ISP allegations the ISP receives for that subscriber's account, so that information is available if a copyright infringement action is initiated against the subscriber – likely commencing with a John Doe action to ascertain the subscriber's identity.

Thus it is only after five (or perhaps six) alerts to a subscriber that measures such as throttling can be applied and, under the logic of the 2011 MoU, the more drastic measure of account termination would only follow under a separate policy if infringement continued to occur after the imposition of mitigation measures. Also, the logic of the agreement is that while ISPs must retain aggregated data about allegations of infringement associated with each subscriber's account, identification of a subscriber could only occur with court oversight.

The 2011 MoU is therefore neither a collective safe harbour account termination policy nor the contractual creation of an alternative to the safe harbour subpoena regime. Rather it is an industry-agreed precursor to the activation of any account termination, and it effectively creates industry-agreed databases amenable to being mined by rights holders by the issue of a subpoena addressed to the ISP. Thus it can be understood as coexisting around both the safe harbour account-termination policy requirements and the existing *Verizon/Charter Communications* jurisprudence.[14]

THE FRENCH GRADUATED RESPONSE

THE ORIGIN OF THE HADOPI REGIME

In 2007 President Sarkozy commissioned a report by a group of experts and industry leaders, headed by Denis Olivennes, on the '*Development and Protection of Culture on New Networks'*. The resulting Olivennes Report had such an impact that the French President, prior to its publication, personally oversaw what has become known as the Olivennes Agreement.[15] The Olivennes Agreement, arrived at on 23 November 2007 between the French government, ISPs and rights holder groups, was underpinned by the key recommendations of the Olivennes Report. Many of those recommendations were directed at accelerating the availability of content through lawful online avenues and the removal of technological protection measures upon music catalogues. However the final recommendation was that a warning and sanction mechanism should be established – with sanctions including the

suspension of a subscriber's ISP account – in which the mechanism would apply to all providers of internet access and might require the establishment of an independent authority (Olivennes Report 2007, 25).

In arriving at this final recommendation, the Olivennes Report observed:

- The maximum criminal penalties for online copyright infringement were a €300,000 fine and three years imprisonment. However these were maximum penalties that French courts resisted applying for non-commercial P2P infringement, as they were disproportionate given the commonality of such infringement. Further, it noted that a legislative attempt to create in 2006 a small-fine regime for online infringers – €38 for downloads and €150 for uploads – had been ruled unconstitutional on the basis that online infringers should not be treated more leniently than other infringers. (Olivennes Report 2007, 7)
- Technical filtering of unauthorised material on P2P networks by cooperation between ISPs and rights holders was not yet a technically feasible approach. (Olivennes Report 2007, 27-31)
- The then operation in the US of safe harbour mandated repeat infringer account termination policies instituted by ISPs under their contractual terms of service with subscribers. The Report noted that both punitive account terminations, and the necessity of correlating reported IP addresses to subscriber identities, were considered virtually impossible for an ISP to justify doing under French law solely on the basis of a contractual power. That was because, under French human rights protections, penal measures and matters affecting online privacy required the intervention of a judge or public authority. (Olivennes Report 2007, 17)

Thus, by a process of elimination, the Olivennes Report squarely moved onto a solution which effectively mimicked the types of outcomes envisaged by a safe harbour repeat infringer account termination policy, but by public law (rather than private bargain), with the State taking a lead role in administering the solution. This approach can also be seen as overcoming the threshold problem of establishing ISP liability in the ISP-P2P setting. It does so by making the ISP's compliance with an order suspending a subscriber's internet access more a matter of regulatory compliance than, as is the case with the US safe harbour regime, an aspect of minimising copyright liability.

The proposed solution also seemed to achieve something equivalent to the 2006 small-fine regime, while seeking to avoid the constitutional road-block that the 2006 measures had encountered in France. This was by the suggested creation of a wholly new legal obligation unique to Internet subscribers; the duty to supervise one's Internet connection so as to ensure it was not being used to commit infringement. It would be repeated breaches of the duty to supervise – breaches regarded as petty offences – that would give rise to the possibility under an administrative process of both lesser fines and the suspension of Internet access. Incidentally, the creation of the duty to supervise also resolved the difficult question of the legal setting, where the subscriber and an infringer using the subscriber's access are different actors, by creating an obligation on the subscriber to supervise the online activities of the user.

At the time of proposing the adoption of this solution, the preamble to the Olivennes Agreement explained the French public policy orientation in this way:

> *Our country possesses one of the strongest content industries in the world, and this agreement provides an opportunity for the preservation and development of the cultural identity and influence of France and Europe. Our country also benefits from having one of the most developed broadband Internet access industries in the world, which is a considerable competitive advantage in the virtual economy. These strengths should not cancel each other out, but rather should complement each other in the best interests of the consumer who will therefore have both powerful distribution networks and richly diversified content.*

Notably, the sentiment expressed here is consistent with a philosophy expressed at the conferences revising the Berne Convention – a good example being comment made almost 100 years earlier at the Berlin revision conference when a free exception to copyright for the mechanical reproduction of musical works was abolished. At that time it was stated:

> *The right of the author and the right of the inventor of instruments must not be weighed against each other; the latter may have achieved wonders, shown true genius, but his right stops at that of others; he cannot appropriate a raw material which does not belong to him and, in this case, the raw material is precisely the musical expression. It matters little what method is used and how difficult it may or may not be to read the disk or the cylinder, the musical expression is nonetheless incorporated in that disk or cylinder*. (WIPO 1986, 155)

The Olivennes Agreement imposed responsibilities upon government, rights holders and ISPs (in that order) to address the issue of uncontrolled and unauthorised content distribution over the internet. The responsibilities upon government – consistent with the Olivennes Report's final recommendation – included introducing 'legislation to the Parliament and adopt regulatory measures, which will allow the setting up of a warning and sanction mechanism aimed at deterring infringement of copyright an digital networks' (Olivennes Agreement, Principle 1 – Government's Undertakings). This became the HADOPI regime.

THE FEATURES OF THE HADOPI REGIME

The public body established to administer the warning and sanction mechanism envisaged by the Olivennes Agreement was named the *High Authority for the Distribution of Works and Protection of Rights on the Internet*, from which the acronym HADOPI is derived from the original French name.[16] In many ways the centrepiece of the regime is its creation of the duty of an Internet subscriber to ensure that its Internet access is not used for the purpose of infringement of copyright (known as the 'duty to supervise').[17] Under the terms of the new law, 'negligence' in meeting this duty makes the person guilty of a misdemeanour which is punishable by a fine of up to €1,500 and suspension of internet access for up to one month. Such negligence is effectively established by the HADOPI sending three warnings to an Internet subscriber in the period of one year. Those warnings, while sent by the HADOPI, are on the basis of information supplied by accredited rights management organisations – usually IP addresses observed being involved in unauthorised file sharing over P2P networks – and through the obligatory assistance from the relevant ISP which matches the IP addresses to subscriber details.

Suspension orders for negligence in failing to meet the duty to supervise are not made by the HADOPI, but by a judge in a streamlined procedure attached to the HADOPI processes. Notably, and consistent with the public law nature of the regime, the suspension order prohibits the subscriber from entering into any internet access subscription agreement, not just with the subscriber's current ISP, and provides that the subscriber is guilty of a further and more serious offence if another internet subscription is entered into during the suspension period.[18] Finally, the regime also involves the possibility of up to a one-year suspension being ordered against those successfully prosecuted for infringement of copyright by means of the Internet (Mariez 2011, 9-12).

THE POLITICS AND EFFICACY OF HADOPI

This regime was initially enacted in May 2009 in a somewhat different form; after the third notice within a year HADOPI could itself order up to a one-year suspension of Internet access for breach of the duty to supervise. A June 2009 constitutional ruling, however, found that aspects of the regime were invalid; effectively only a judge (not the HADOPI) could order suspension of Internet access and that, in any event, a 12-month suspension for breach of the duty to supervise was a disproportionate penalty (Jančić 2010, 452-454). More fundamentally the same ruling gave two important validations of the approach underpinning the HADOPI

regime. First, it found that the duty to supervise was a validly enacted obligation. Second, it found that the regime struck a correct balance with privacy interests. The necessary revisions – reducing the suspension term to one month and vesting power in a judge – were made by the French Parliament in September 2009. Further constitutional review in October 2009 left the revised laws largely undisturbed, and these remain current.

As Davor Jančić vividly explains, during the revision of the HADOPI regime following the decision of the French Constitutional Court, a parallel consideration was occurring at a European level in relation to a raft of amendments to European Directives and Regulations on telecommunications (Jančić 2010, 454-459). In an attempt to reform a Directive on a common regulatory framework for electronic communications networks and services (the 'Framework Directive'), an amendment was tabled by a group of members of the European Parliament headed by the French Socialist Guy Bono. It proposed that 'no restriction be imposed on the fundamental rights and freedoms of end-users without a prior ruling of the judicial authorities' (the 'Bono proposal'). While the principle underlying this proposal ultimately informed the final form of the HADOPI regime – specifically as a consequence of the French Constitutional Court's intervention – the ultimate amendment to the Framework Directive did not require a prior judicial ruling for internet end-user restrictions. Rather, the revised article requires that restrictions upon end-users' Internet access require a 'prior, fair and impartial procedure … including the right to be heard of the person or persons concerned' and the 'right to effective and timely judicial review'.[19] In other words, natural justice needs to be instituted prior to restricting Internet access and judicial review needs to be available promptly thereafter. These are, however, softer requirements than that of a 'prior judicial ruling'.

The HADOPI regime is opposed by those from both the left and the far right of French politics, and stridently opposed by information-liberationists such as La Quadrature du Net, the latter being a type of French Electronic Frontiers Foundation. With its €11 million annual budget, HADOPI is seen as a weapon to oppress Internet users, gifted to rights holders by the Sarkozy administration. In the inaugural HADOPI Annual Report, HADOPI's President De Marie-Françoise Marais wrote:

> *To date, this work has been carried out under conditions never seen before: rarely has a new institution been facing ... such a refusal from certain parties to work together, whether these parties be political, public officers, researchers or even members of civil society. And, the numerous comments made have illustrated that people have a total lack of knowledge about the institution and its actions.* (HADOPI 2010, 3).

In February 2012 the operation of the HADOPI regime was reported under the following heading: 'France Claims Victory Over Piracy – but as first cases come before the courts, opposition to approach grows louder'. [20] As at the time of writing, those cases have not yet been decided and the French Socialist party has won power on a platform that included abolition of the HADOPI regime. The consequences that arise from the pending court decisions, and whether the French Socialists adhere to their platform, create uncertainty about the future of the HADOPI regime.

However a paper by US researchers on the effects of the HADOPI regime on the sale of authorised downloads within France offers some comfort to those in the creative industries whose interests are intended to be served by the HADOPI regime (Danaher et al 2012). On the analysis of the data undertaken by the research team, it summarised its findings as 'increased consumer awareness of HADOPI caused iTunes song and album sales to increase by 22.5% and 25% respectively', a causal connection substantiated by the 'observed sales increase is much larger in genres that, prior to HADOPI, experienced high piracy levels (e.g., Rap and Hip Hop) than for less pirated genres (e.g., Christian music, classical, and jazz)' (ibid). The researchers went on to observe that:

> *The most interesting, and potentially surprising, part of this conclusion is that the study occurs before anyone received a third notice (i.e. before any cases have been referred to the criminal court), and that the increase in sales is observed even before the law's final passage. While this may seem irrational, it is*

> *consistent with the idea that increasing the salience of the law, the illegality of piracy, and the potential penalties is sufficient to change user behaviour.* (Danaher et al 2012, 19)

The results of the research are also important to the global debate. They suggest that the introduction of the type of laws that the HADOPI regime represents can be shown to alter the behaviour of internet users. Evidence of this nature responds to the assertion put in certain quarters that 'there is little evidence that a graduated response mechanism is likely to reduce the rates of infringement' (Suzor and Fitzgerald 2011, 15).

CONCLUSION

Roadshow Films v iiNet rejected authorisation liability for an ISP which sat on its hands while being supplied with weekly notices from rights holders of apparent P2P infringements occurring via its subscribers' connections. The majority reasons offered the following observation on this outcome:

> *This final conclusion shows that the concept and the principles of the statutory tort of authorisation of copyright infringement are not readily suited to enforcing the rights of copyright owners in respect of widespread infringements occasioned by peer-to-peer file sharing, as occurs with the BitTorrent system. The difficulties of enforcement which such infringements pose for copyright owners have been addressed elsewhere, in constitutional settings different from our own, by specially targeted legislative schemes, some of which incorporate cooperative industry protocols, some of which require judicial involvement in the termination of internet accounts, and some of which provide for the sharing of enforcement costs between ISPs and copyright owners.* ((2012) 286 ALR 466, 486)

The first sentence of this passage could strain credulity in an informed reader. There was an undoubted judicial choice involved in rejecting authorisation liability; the reason why such liability was 'not readily suited' in the ISP-P2P setting was because the judges chose for it to not apply. Justice Jagot convincingly demonstrated in a lower court that under existing Australian law a finding of authorisation liability was well within the accepted orthodoxy given the notices and the posture that the ISP, iiNet, had then adopted.[21] Had the High Court chosen to share Jagot J's analysis, it would have provided what might be considered a full incentive to all Australian ISPs to cooperate with rights holders under the Australian safe harbour regime to adopt an appropriate policy that provides for account termination of repeat infringing subscribers. (Notably the ISP in the litigation, iiNet, to some extent precipitated the litigation by refusing to cooperate with rights holders by passing on warning notices in relation to the notified activities.) A finding of authorisation liability would have led to Australia being a text book case study on whether the safe harbour regime – with its remedial limitation upon liability arising from category A activities – could work effectively in the ISP-P2P setting in a manner consistent with the principles underpinning the regime.

Having rejected that course, however, the comments in the second sentence of the majority's observation can be reflected upon in view of the above discussion. The 2011 MoU in the US arose in liability circumstances that are not dissimilar to that which the Australian High Court has now created for Australia. Those are that, in the ISP-P2P setting, the ISP most likely has no copyright liability unless it does something more that merely provide a service – such as positive encouragement to infringe. However the fact that a US rights holder and ISP consensus still arose notwithstanding that being the liability position – albeit with an apparent role played by the plausible threat of Congressional action – is of particular relevance to the Australian situation. That is because, and as noted at the outset, the Commonwealth Attorney-General's Department is hosting on-going negotiations between peak players in the content and communications industries with a key objective of those negotiations being to develop a code of conduct to address the issue of unlawful P2P distribution.

At a public seminar in May 2012 on the High Court *Roadshow Films v iiNet* decision and its ramifications, speakers included both Chief Executives of the main negotiating bodies – the

Australian Federation Against Copyright Theft and the Communication Alliance.[22] There, one aspect of the negotiations was exposed for all to see: who pays? The Communications Alliance set out the following as a hypothetical trial of ISPs passing on rights-holder notices to their subscribers: 50,000 notices at a cost of $40 per notice; $250k contribution to education and appeal mechanism; total cost to rights holders of $2.25m. Implicit in this proposal is a view that because an ISP has no liability in the ISP-P2P setting – or to use the phrase adopted by Gummow and Hayne JJ in *Roadshow Films v iiNet*, the ISP owes no 'duty of care' to rights holders – then any cooperation is being done as a matter of favour, and that an ISP's cost of so doing should be fully indemnified by rights holders.

As explained above, it seems that one aspect explaining the 2011 MoU in the US was the role of the Obama Administration. The possibility of Congressional action and indeed a graduated response regime being enacted as US public law appeared to have loomed large in the negotiations. Does such a condition exist in Australia? It seems most unlikely that there would be much appetite for an Australian HADOPI regime. Australian public policy has traditionally favoured bottom-up industry agreement and small government, rather than top-down bureaucratic control and big government. However, if the evidence that emerges continues to reveal pubic law graduated response approaches to be efficacious in converting unlawful down-loaders into lawful consumers, it is not impossible that the Australian government might start to consider such an approach as a substitute for a safe harbour regime. Indeed, perhaps only if the Australian government begins to seriously consider HADOPI-style laws would conditions exist in Australia – in view of the outcome in *Roadshow Films v iiNet* – for a type of industry agreement along the lines of that arrived at in the US under the 2011 MoU.

REFERENCES

Arrow, Kenneth J; Ayres, Ian; Becker, Gary; Landes, William M; Levitt, Steven; Lichtman, Douglas; Murphy, Kevin; Picker, Randal; Rosenfield, Andrew; Shavell, Steven. 2005. Brief of *Amici Curiae* in support of the petitioners in *MGM Studios v Grokster*, 545 US 913 (2005)

Brenner, Daniel. 2012. 'Five strikes and ... you're not out: the new US copyright ISP agreement' (2012) 18 *Computer and Telecommunications Law Review* 67

Danaher, Brett; Smith, Michael D; Telang, Rahul; Chen, Siwen. '2012. The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France', Version as at March 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240 (visited 29 June 2012)

Elkin-Koren, Niva. 2006. 'Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic' (2006) 9 *New York University Journal of Legislation and Public Policy* 15

Espinel, Victoria. 2011. 'Working Together to Stop Internet Piracy' *The White House Blog* 7 July 2011, http://www.whitehouse.gov/blog/2011/07/07/working-together-stop-internet-piracy (visited 29 June 2012)

Ginsburg, Jane. 2008. 'Recent Developments in US Copyright - Part II, Caselaw: Exclusive Rights on the Ebb?' (2008) 218 *Revue Internationale du Droit d'Auteur* 167

HADOPI 2010. Annual Report 2010. http://www.hadopi.fr/actualites/rapport-annuel/2010 (visited 29 June 2012)

Information Infrastructure Task Force. 1994. *Intellectual Property and the National Information Infrastructure - A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights*, July 1994 http://cool.conservation-us.org/bytopic/intprop/ipwg/ (visited 29 June 2012)

Information Infrastructure Task Force. 1995. *Intellectual Property and the National Information Infrastructure - The Report of the Working Group On Intellectual Property Rights*, September 1995

Jančić, Davor. 2010. 'The European Political Order and Internet Piracy: Accidental or Pragmatic Constitution-Shaping?' (2010) 6 *European Constitutional Law Review* 430

Kravets, David. 2011. 'U.S. Copyright Czar Cozied Up to Content Industry, E-Mails Show' *Wired* 14 October 2011, http://www.wired.com/threatlevel/2011/10/copyright-czar-cozies-up/ (visited 29 June 2012)

Lindsay, David. 2012. 'ISP liability for end-user copyright infringements: the High Court decision in Roadshow Films v iiNet'. *Telecommunications Journal of Australia* 62 (4): 53.1-53.24. Available from: http://tja.org.au.

Litman, Jessica. 2011. *Digital Copyright* (Prometheus Books 2001)

Mariez, Jean-Sébastien. 2011. 'HADOPI ... 3 Small Suspension Points ...' (15 March 2011), http://www.juriscom.net/pro/visu.php?ID=1302 (visited 29 June 2012)

Nimmer, Melville B; Nimmer, David. 1978. *Nimmer on Copyright : a treatise on the law of literary, musical and artistic property, and the protection of ideas* (1978-)

Olivennes, Denis; Bomsel, Olivier; Falque-Pierrotin, Isabelle; Faure, Pascal. 2007. *Development and Protection of Culture on New Networks – Report to the Minister of Culture and Communication*, November 2007, http://www.culture.gouv.fr/culture/actualites/conferen/albanel/rapportolivennes231107.pdf (visited 29 June 2012)

Olivennes Agreement for the Development and Protection of Works and Cultural Programs on New Networks, Friday 23 November 2007, http://www.culture.gouv.fr/culture/actualites/conferen/albanel/accordolivennes.htm (visited 29 June 2012)

Suzor, Nicolas; Fitzgerald, Brian. 2011. 'The Legitimacy of Graduated Response Schemes in Copyright Law' (2011) 34 *UNSW Law Journal* 1

WIPO. 1986. *Berne Convention for the Protection of Literary and Artistic Works from 1886 to 1986* (1986) 155

ACKNOWLEDGEMENTS

I thank and acknowledge the input provided to me by Rebecca Borden and Victor Lei in the drafting of this essay, and the valuable suggestions which arose through the refereeing process. Naturally, all responsibility for the analysis rests with me.

ENDNOTES

1. (2012) 286 ALR 466; [2012] HCA 16. The case and its implications are discussed at length in David Lindsay (2012).

2. The provisions of Part V Division 2AA relating to any such code require (by regulation) that 'it must be developed through an open voluntary process by a broad consensus of copyright owners and carriage service providers', and be registered by the Australian Communications and Media Authority (ACMA) under processes specified in the Telecommunications Act 1997: *Copyright Regulations 1969* (Cth) reg 20B.

3. Australia-United States Free Trade Agreement 2004, article 17.11(29).

4. Copyright Act 1976 (US), §512(i)(1)(A). The US Senate Report on the Digital Millennium Copyright Act of 1998 explained: 'By subscribers, the Committee intends to include account holders who are parties with a business relationship to the service provider that justifies treating them as subscribers, for the purposes of section 512, even if no formal subscription agreement exists. Examples include students who are granted access to a university's system or network for digital online communications; employees who have access to their employer's system or network; or household members with access to a consumer online service by virtue of a subscription agreement between the service provider and another member of that household' (Senate Report 105–190 at page 52, note 24).

5. *MGM Studios v Grokster*, 545 US 913 (2005).

6. Melville B. Nimmer and David Nimmer, *Nimmer on Copyright : a treatise on the law of literary, musical and artistic property, and the protection of ideas* (1978-) § 12.04[A][4][b] suggesting that contributory and inducement theories of liability are discrete. Compare *Roadshow Films v iiNet* (2012) 286 ALR 466, 490 (Gummow and Hayne JJ) where inducement liability is regarded as an aspect of contributory infringement.

7. Compare *Ellison v Robertson*, 357 F3d 1072, 1077 (2004) where it was held that had 'a reasonable trier of fact could find that [the ISP defendant] had reason to know of potentially infringing activity'.

8. *Ellison v Robertson*, 357 F 3d 1072, 1078-9 (2004).

9. *MGM Studios v Grokster*, 545 US 913, 939-940 (2005).

10. Copyright Act 1976 (US), §512(c)(1)(A).

11. Copyright Act 1976 (US), §512(h).

12. Copyright Act 1976 (US), §512(i) 'The limitations on liability established by this section shall apply to a service provider only if the service provider ...'.

13. The text of the memorandum is available at: http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf (visited 29 June 2012).

14. As at the time of writing the regime established by the 2011 MoU has not been implemented – an expected start date is the second half of 2012.

15. The French text of the agreement, fully titled 'Agreement for the development and protection of cultural works and programmes on new networks' is available at: http://www.culture.gouv.fr/culture/actualites/conferen/albanel/accordolivennes.htm (visited 29 June 2012).

16. *Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet*.

17. French Intellectual Property Code L 336-3.

18. French Intellectual Property Code L 335-7-1.

19. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services ('Framework Directive') by inserting into Framework Directive Article 1 new paragraph 3a.

20. Eric Pfanner, 'France Claims Victory Over Piracy – but as first cases come before the courts, opposition to approach grows louder' *International Herald Tribune*, 20 February 2012, 16-17.

21. (2011) 275 ALR 1, 62-120; [2011] FCAFC 23, [275]-[528].

22. See: http://www.ipria.org/events/seminar/2012/VillagevsiiNet/VillagevsiiNet.html (visited 29 June 2012).

Cite this article as: Brennan, David J. 2012. 'Quelling P2P infringement: private American harbours or public French graduations?' *Telecommunications Journal of Australia* 62 (4): 55.1-55.15. Available from: http://tja.org.au.