Review of Economic Research on Copyright Issues, 2004, vol. 1(1), pp. 119-149

WHEN SHOULD THE BELL TOLL? THE ECONOMICS OF NEW ZEALAND'S DEBATE ON INDIRECT LIABILITY FOR INTERNET COPYRIGHT INFRINGEMENT

ALAN E. WOODFIELD

ABSTRACT. This article evaluates proposed changes to New Zealand's copyright legislation in respect of potential secondary liability for copyright infringement by Internet service providers. Minor changes were envisaged in order to align the legislation with new international standards, with limitation of ISP liability along the lines of the UK Electronic Commerce Regulations 2002 recommended. Both zero liability and strict liability for web-hosting ISPs are correctly rejected, but the proposed uniform regulatory approach provides limited incentives for ISP monitoring effort and while proposed knowledge-based standards should largely prevent excessive permanent removal of legitimate material, the constructive knowledge test may be insufficient to encourage the removal of many infringing items. The counter-notification procedure may not prevent liability-conscious ISPs from removing excessive legitimate material on a temporary basis, and more radical solutions involving ISP purchase of their subscribers' posted material or compulsory ISP purchase of copyrights did not feature. The design of optimal copyright law is fraught with difficulties, however, and the Ministry's consultative processes and careful deliberations have done much to maintain a reasonable balance between the conflicting interests concerned.

1. INTRODUCTION

New Zealand's Copyright Act 1994 ("the Act") was enacted prior to rapid advances in information technology, the Internet in particular. Recognizing that digital technology permits copyright works to be copied, modified, and disseminated at very low cost, the Ministry of Economic Development ("the Ministry") inaugurated a Digital Copyright Review and has consulted widely since 2001 on how to balance the competing interests of copyright owners who claim to be threatened by serious levels of copyright piracy, and users of copyright material particularly those for whom in a small, physically isolated but computer-literate society view computer network devices such as the Internet as pennies from heaven.[1]

I would like to thank the Ministry of Economic Development for making available the public submissions relating to their Digital Copyright Review, Kim Connolly-Stone and Victoria Pearson of the Ministry for points of clarification, Nick McNabb for research assistance in preparing this article, and the Editor for helpful suggestions. Any errors are mine.

[1]For example, between 1986-2002, the number of households equipped with at least one computer increased from less than one in ten to more than 50 percent. Personal Internet use access increased from 42 percent of people in 1992 to 75 percent in 2002, while the percentage of people using the Internet in the previous four weeks increased from 18 percent in the first quarter of 1998 to 58 percent in the third quarter of 2002. In July 2001, New Zealand ranked seventh of eleven OECD countries in terms of per capita webhosting rates, and had the third highest use per capita

Of major concern has been whether the Act, which contains no specific reference to digital technology, is capable of offering appropriate protection to either copyright owners or users, or is simply insufficiently clear as to what is protected. As a consequence, the Ministry first introduced a Discussion Paper ("DP", 2001) identifying key issues and possible approaches to copyright law reform, and called for public submissions on the issues raised therein. In response to the submissions, the Ministry produced a Position Paper ("PP", 2002) stating its preferred position, and called for further submissions.[2] After consideration, the Associate Minister of Commerce made a number of policy recommendations in June 2003 to the Cabinet Economic Development Committee involving proposed amendments to the Act, with a view to their introduction during 2004.[3]

Although an important part of the government's innovation framework, the Digital Copyright Review found that the Act required no substantial changes. Rather, only some clarification and exceptions were required in the digital environment to align the Act with new international standards. No substantial strengthening of the rights of copyright owners is envisaged, the Review properly recognizing that some (if not all) elements of unauthorized copying need not harm their interests, and may improve their welfare.[4]

Included in the list of proposed amendments to the Act was an intention to limit liability for Internet service providers ("ISPs") for both primary and secondary infringement in "appropriate" circumstances. The purpose of this article is to evaluate the debate surrounding ISP liability for secondary copyright infringement, where ISPs are alleged to facilitate copyright piracy by their subscribers. The article is organized as follows. Section 2 identifies sources of potential ISP liability and summarizes the proposed New Zealand policy changes. Section 3 evaluates the general reasoning adopted in the DP submissions in the light of extant literature on third party liability for copyright infringement, while section 4 examines the proposed policy changes in light of alternative legal strategies suggested in this literature. Section 5 provides a brief conclusion.

2. Sources of Potential Liability for Internet Service Providers

There are two sources of potential liability of ISPs for copyright infringement. Primary liability refers to direct ISP infringement, where, for example, ISPs might reproduce on their computer or server a webpage containing copyright-protected material without permission of the copyright owner. Such an activity would currently constitute infringement under sections 29-34 of the Act, and absence of knowledge that the activity would be infringing is no defense. ISP authorization of

of secured servers by international standards (as an index of e-commerce activity) as of January 2002. See Ministry of Economic Development (June, 2003) for further details.

[2]Many of the Ministry's relevant papers may be downloaded from the Publications section of their website: http://www.med.govt.nz.

[3]Cf., Office of the Associate Minister of Commerce (2003).

[4]As Liebowitz (2002) argues, apocalyptic claims by copyright owners have commonly been made in the advent of new copying technologies, yet without industry annihilation subsequently occurring. Nevertheless, it is also argued that aspects of digital technology, particularly recent forms of online file-sharing, make organized, large-scale unauthorized copying a potentially serious threat to owners. This is in spite of various market mechanisms available to contain piracy, including the indirect appropriability of returns in prices of original delivery goods that would be considerably lower in the absence of piracy. For a related view that pours empirical cold water on supporters of the general irrelevance of copyright law in this context, see Klein et al. (2002).

additional copying by users in these circumstances also raises potential liability, as does transient copying where temporary or incidental copies are made on an ISP's servers so as to permit the construction of websites and transmission of material therefrom.

After considering the DP submissions, the Ministry's PP noted that while there appeared to be general agreement that ISPs should be liable for infringement resulting from their own direct action as currently provided, where services are provided to third parties, exemption from liability was arguably warranted in respect of transient copying automatically undertaken as part of a technical process, and caching (transient or otherwise), the latter in order to provide more rapid services. The Ministry also preferred ISPs not to be liable merely because they possessed facilities that technically permitted infringements, and neither would such possession imply authorization of infringement.

Secondary infringement on the other hand essentially involves ISPs providing the means for infringing activities by their customers, and the Act currently requires either actual or constructive knowledge of the nature of users' infringing activities. Under current legislation, ISPs would not appear to be engaged in such infringement by the mere provision of their services.[5] The Ministry appeared impressed with the large number of submissions emphasizing the burdensome, possibly prohibitive, cost of ISPs monitoring material either stored or passing through their systems, and recommended limitation of ISP liability along the lines of regulation 19 of the UK Electronic Commerce (EC Directive) Regulations 2002, exempting ISP liability where infringing information is stored on behalf of a third party subscriber and where the ISP does not authorize the infringement, or where the ISP is unaware either of the infringement or facts making infringement obvious, or, given knowledge of infringement, acts "expeditiously" to remove or disable access to the material.

3. The Discussion Paper Submissions

The 74 DP submissions (along with the 56 PP submissions which the Ministry claimed to largely support its policy proposals) were potentially important inputs into the formation of policy regarding amendment of the Act as it applies to digital technology.[6] Not surprisingly, owners and users typically argued that the advent of digital technology had swung the balance in favour of the other. As a consequence, submissions differed sharply as to what policy objectives should be specified in the digital environment, and what appropriate amendments would entail.

[5]Section 36, however, applies to the possession or dealing with an infringing copy of a work. A person infringes copyright where an infringing copy is either possessed or offered for hire or sale in the course of business, and where that person knows or has reason to believe that the copy infringes copyright. This section may apply to an ISP where a temporary copy is possessed; in such a case the act of making the copy would likely be a primary infringement. There is, however, an argument that there would be an implied licence to make the temporary copy. Liability would arguably arise where an infringing copy is made available on the Internet and the ISP subsequently makes a temporary copy; here, the ISP would possess an infringing copy in the course of business, and an implied licence would not arise.

[6]Some 33 DP submissions were received from copyright owner/creator groups, including four submissions from Crown entities operating in the film, broadcasting and publishing sectors. Thirty-four submissions were received from individual users of copyright works or user groups, including academics and researchers with a substantial input from libraries and educational institutions. The remaining submissions came from legal and IT professionals, along with one foreign government agency, and which could not easily be assigned.

3.1. **Third Party Liability for Internet Service Providers?** The DP posed the questions of whether, and in what circumstances, ISPs and related providers should face liability for Internet-related secondary copyright infringement.[7] Three approaches were identified; viz, zero liability, strict liability, or some form of limited liability for a subset of possibly infringing activities of ISPs' subscribers.[8]

Some 38 DP respondents addressed the specific issue of ISP secondary liability, 18 percent of whom essentially argued in favour of zero liability, while the remainder argued for exemptions in particular circumstances. Those favouring zero liability commonly argued that users rather than ISPs are infringers, that enforcement of liability would be impracticable, and that customer liability is accepted in contracts with ISPs. Even for those in favour of limited ISP liability, zero liability for secondary infringement was frequently recommended where an ISP acted as a 'mere conduit', took reasonable precautionary measures against infringement by subscribers, had no knowledge of the infringement, provided Internet access without also hosting websites, or had no control over website content. Liability was commonly recommended, however, where an ISP either encouraged or authorized infringement activity, knew of an infringement but failed to take action that would prevent infringement from persisting, or refused to obey either a request or an order to remove infringing material.

3.1.1. *Should Either Zero or Strict Secondary Liability for ISPs be Rejected?* A major supporter of zero liability was New Zealand's market-leading ISP; viz, Telecom New Zealand Limited ("Telecom"), which argued as follows. First, the definition of an ISP is important, since a pure access provider has no visibility of content, similar to a telecommunications operator. Access providers make no direct financial gain resulting from copyright work being transmitted, and have no control over such transmissions. Zero liability should apply and the exclusion should extend to an action (or refusal to act) regarding disconnection or taking down material allegedly infringing copyright. Otherwise, liability is effectively a tax on the postie for delivering mail containing copyright-infringed material. ISPs, however, differ from specialized access providers since they typically provide website building, maintenance, and hosting, links to third party websites, and visitor rooms such as bulletin boards and chat rooms. In Telecom's view, ISPs do not typically provide content of websites and lack the ability to control content. Where content is monitored, the ability to identify copyright-protected material and any subsequent infringement is limited. In Telecom's view, the copyright owner, not the ISP, is best placed for identifying infringement. Thus, ISPs should not face liability for content posted by third parties, even if notified that copyright material is posted. Copyright owners have legal remedies against infringers, and ISPs do not generally have the capability to detect infringement.[9]

[7]There were 48 ISPs listed in the New Zealand Internet Service Provider Directory as of March 2004, and it is unclear as to how many "related providers" are also planned to be captured under the proposed amendments to the Act.

[8]Persons using ISP services for infringing activities were always seen to be separately liable; cf., DP, p. 45, clause 151. They may, however, be judgment-proof, in which case the sole use of primary liability fails to prevent infringement, a major plank in the platform of those favouring indirect liability for ISPs.

[9]Opponents of ISP indirect liability might also have suggested that were such liability to be imposed, it would be preferable to pick on a different "gatekeeper" such as manufacturers of modems or even personal computers. As Hamdami (2003) argues, however, while infringing

Many of these arguments also received support in other submissions, including those which support liability for ISPs that continue to host websites containing known infringing material. Against these arguments, however, it is evident that ISPs could choose to view the contents of their servers and determine the extent of copyright infringement (or the likelihood thereof), but will have no incentive to do so under a zero liability rule.[10] Further, given that an ISP may have no incentive to view the webpage contents of its subscribers, it will not invest in technologies permitting least-cost monitoring.

In a recent comprehensive evaluation of ISP liability rules (which will be followed closely here), Hamdami (2002) suggests that a consensus has emerged; viz, that in appropriate circumstances, ISPs *should* be held legally liable for their users' wrongdoings. The major attraction of web-hosting ISPs for secondary infringement liability arises because the main form of Internet access is via ISP gatekeepers, who, unlike their subscribers, are readily identifiable, relatively easily exposed to sanction, and relatively low-risk in terms of being judgment-proof. In the DP submission by Thomborson, it was argued that illicit distributions will be advertised extensively through the Internet via search engines and as such will be easily discoverable by the copyright owner if the distribution websites persist for significant periods of time. If they do not, the damage is likely to be small.[11] It is detection *beyond* the ISP, however, that is the problem for supporters of zero liability and which raises the *prima facie* appeal of strict ISP liability. In the New Zealand case, however, *no* DP respondent favoured strict liability for ISPs, which, for example, was viewed as "very unfair" and would "make them liable for contravening acts that they are unable to control,"[12] or would increase Internet access prices (either via the internalization of expected liability payments or monitoring costs incurred to avoid such payments) and thereby undesirably affect access to information.[13]

In Hamdami's view, strict liability is often preferred as an efficiency-enhancing rule because it supposedly aligns an ISP's private interest with the social interest, in which case the ISP will supposedly undertake the optimal level of its activity but

activity can easily be contained by refusing, say, to sell computers to wrongdoers, the identification of wrongdoers at the time of purchase appears prohibitively costly and the ability to monitor their subsequent use is negligible. Thus, the technical ability to prevent infringement by the exercise of a veto power is not a sufficient condition for imposition of liability; instead, Hamdami argues that the cost of information acquisition about subscriber conduct must also be relatively low.

[10]On the contrary; if it is unprofitable for copyright owners to pursue infringers, the value of ISP webhosting will be greater in the short run, although in the long run, the supply of copyright material will be adversely affected by piracy.

[11]Cf., Clark Thomborson, DP Submission, p. 3. Thus, anyone trading copyright-protected material is "publicizing their infringement to the world", yet detection does not involve a "rocket-science net-sniffer" to detect infringement, and "only minimal competence in network technology is required to locate the infringing distribution at least to the level of the ISP if not the end-user" (pp. 4-5).

[12]Cf., Sky Network Television Limited.

[13]Cf., Newspaper Publishers Association, New Zealand Law Society. In this context, Landes and Lichtman (2003) argue that it may be efficient to impose indirect liability on ISPs even when they find it prohibitively costly to distinguish legal from illegal copyright activity *because* the ISP would increase its price to cover expected damages. Although liability would act like a tax that would reduce welfare by discouraging legal (as well as illegal) uses, in some cases a welfare *gain* might occur; viz, where illegal activity dominates illegal activity, or where harms and benefits are similar but illegal activity is relatively price-sensitive, or where the improved copyright incentives exceed the harms arising from the reduction in legitimate use. These results, however, are predicated on infringers largely switching to legal activity in response to higher access prices.

not undertake excessive liability avoidance costs since this would involve under-compensating savings in expected liability payments (Landes and Posner, 1987, Shavell, 1980).[14] With optimal effort directed at reducing harms resulting from copyright infingement, the cost of this effort will be internalized in socially optimal competitive prices for ISP services. The attraction of strict liability in making ISPs liable for the harm that they 'cause' is that the relative anonymity of Internet users makes detection of copyright law violation very costly, particularly if ISPs are not cooperative in enforcement. The expansion of liability to third parties is then seen as necessary to cope with under-deterrence, in which case the arguments in favour of zero ISP secondary liability fail at this point. Efficiency, however, requires that liability imposition should be directed at the least-cost preventer of misconduct, and Hamdami argues that there seems to be fairly general acceptance that ISPs satisfy this criterion.

Further, under strict liability, ISPs would be in the best informational position to compute optimal prevention levels, and other parties need not acquire this information. Courts would only be required to verify harms resulting from user misconduct. Strict liability also offers a simple and clear legal rule, favoured by a number of DP respondents.[15]

Nevertheless, Hamdami suggests that many commentators reject strict liability for ISPs, since user demand for Internet services is for both legitimate and illegitimate uses. ISPs may be unable to distinguish these alternative uses without very costly monitoring information disseminated through their networks, and may also inadvertently remove legitimate material or block access thereto, denying their subscribers some of their potential profits and end-users some of their potential surplus.[16] In this context, four DP respondents specifically raised the issue of ISP monitoring costs in recommending an exemption from liability when ISPs take reasonable steps to prevent infringement, e.g., by taking cost-justifiable steps to control subscriber webpage content.[17]

In any event, Hamdami argues that there are stronger arguments against strict liability, illustrating the case where 'users' are web-hosters that are charged on the

[14]Negligence is dispreferred on the standard grounds that excessive activity levels will be generated; thus, by taking due care, an ISP will never be found negligent, yet social costs will typically be increasing in activity levels as well as decreasing in terms of care levels. Generally, it is argued that courts cannot condition negligence rules on optimal activity levels because of information held privately by wrongdoers, but strict liability is not subject to this problem and wrongdoers can use their private information to optimize their activity levels at the socially optimal levels. More generally, strict liability imposes light informational burdens on courts since only cause and the level of harm suffered by owners needs to be determined.

[15]These included, for example, Microsoft New Zealand Limited, Information Technology New Zealand, and Consumers Institute.

[16]Against this, however, it is well-known that strict liability provides uninformed defendants with optimal incentives to acquire information (Shavell, 1992). Defendants will either acquire optimal quantities of information or, if these acquisition costs are prohibitive, will accept liability and shift the expected liability costs to users. Unfortunately, users are likely to be heterogeneous and the scope of their illegitimate activities will differ, but they may be pooled in facing the same service cost unless self-selection contracts can be devised. Even when the latter exist, such contracts typically ration the extent of access for relatively low-risk types in order to marginally deter high-risk types from choosing a low-access price contract among those on offer, reducing welfare below that attainable in a world where both ISPs and users possess identical information as to user types.

[17]See the DP submissions of the New Zealand Rugby Football Union Inc., Lincoln University, Sky Network Television Limited, and New Zealand Law Society.

basis of physical space provided and the volume of traffic generated. While ISPs are technically capable of preventing infringement by removing infringing items at negligible cost, the cost of detecting an infringing item among the vast quantity of total items stored on the host's servers is much greater. ISPs will then adopt excessively strict monitoring policies and remove an excessive quantity of legal material. They do not capture the full value of the conduct they are policing, and would assign disproportionate weight to liability risk while ignoring losses to subscribers and end-users. The assumption that wrongdoers capture the full value of the benefits of their actions is inappropriate in the presence of third party liability, and private and social incentives are no longer aligned. As a consequence, Hamdami rejects strict secondary ISP liability as the means of regulating web-host based copyright infringement on the Internet.

3.1.2. *The Role of Regulation.* As an alternative to either strict or zero liability, the regulatory approach places categorical limitations on the level of third-party liability. In essence, this is the general approach supported by the significant majority of DP respondents and adopted by the Ministry. Hamdami, however, argues that it adopts a uniform view of overdeterrence under which all instances of third-party liability receive identical treatment. Taking a principal-agent approach to the issue, removal of the divergence of incentives between principals and agents requires the alignment of residual rewards with residual control.

In this context, a number of DP respondents either objected to, or at least raised doubts about, the application of liability where ISPs act as 'mere conduits', transmitting material without selecting or modifying content, or engage in caching or hosting.[18] ISPs, however, possess ultimate control in a veto sense, by refusing to negotiate proposed contracts, canceling existing contracts without penalty if a contract is for an illegitimate purpose, blocking access to websites, or removing website material in whole or in part. Since ISPs possess residual control of the contents of their servers, residual rewards should be vested with them, with the implication that users need invest nothing in determining what is an ISP's optimal choice of monitoring technology since the ISP will have the correct incentives to choose socially cost-minimizing technologies. ISPs would effectively buy the rights to post whatever is owned by their website owners, and a merging of website owners and ISPs would also correctly align incentives. Buying site contents, however, may lead to many unfulfilled transactions because of uncertainty as to the existence or magnitudes of gains from trade between the parties. Consequently, Hamdami considers that the risk of liability is unlikely to be sufficiently powerful to induce the parties to adopt this solution.

An alternative approach recognizes that ISP liability duplicates transactions cost. The ISP will devote resources to checking content in order to reduce, if not eradicate, its exposure to liability. For the ISP to face residual liability, however, the copyright holder must also spend resources checking content in order to provide evidence to bring suit in cases of infringement. Indirect liability then leads to the duplication of monitoring costs, and it would arguably be more efficient if the ISP were required to invest in the copyright itself and so to have the incentive to monitor optimally and also to correctly bring suit against infringers.

[18]Thus, in the view of the Recording Industry Association of New Zealand Inc., in these cases "the ISP does not select or modify the content and has no control, or possibility of control, over such information or over the sender and receiver of the information." DP submission, p. 13.

At a less "radical" level, however, some form of profit-sharing between ISPs and their subscribers is suggested by Hamdami. Since website owners would attempt to gain opportunistically by concealing the number and value of transactions, contracts must be conditioned on observable and verifiable information regarding transactions; e.g., space and number of hits.

If excessive censoring occurs, subscribers may switch to a firm offering much less aggressive monitoring. In the latter case, the ISP access price will increase to reflect the extent of the higher expected liability, but this is more than compensated by the additional net revenues obtained by the subscriber when a greater quantity of legal material is transmitted via the website. A low-monitoring ISP must provide a credible commitment to monitor less aggressively than its rivals, and it may be unable to do so if subscribers find it very costly to verify monitoring activity. Perhaps the ISP could post a bond, redeemable in the event that it was found in breach of its contractual monitoring duties. Courts, however, may refuse to enforce penal provisions of this nature. The ISP might also be able to establish a reputation for lax monitoring in a market with repeated contracting, but this may be difficult to establish and places the ISP at a greater risk of legal liability. Further, users may self-select low-monitoring ISPs so that those with high infringement rates allocate themselves to such firms, raising expected liability above that for users on average. Hamdami, however, does not discuss the effect on access prices, and the price would presumably reflect the adversely selected 'lemon'.

Subscribers may also be unrepresentative mixtures of liability risks for ISPs that cannot determine their risk class *ex ante*. Hamdami (2003) examines this issue in the general context of "gatekeeper" liability with respect to market participation decisions, finding familiar parameter-dependent 'lemons' market results whereby markets may not form in equilibrium, or where wrongdoers drive lawful types from the market, or where participation is unaffected by illegal activity and wrongdoers are cross-subsidized by law-abiding citizens. Further, welfare effects depend on the benefits of wrongdoing as well as harms generated, and general results are not evident. The analysis, however, assumes that wrongdoers and law-abiders will be pooled in equilibrium, which will not generally be the case if, in addition to participation decisions, the level of user activity is endogenous. Thus, adverse selection theory suggests that an ISP faced with different types of customers whose risk classes (in terms of expected liability faced by ISPs) cannot be identified *ex ante* would offer a menu of contracts such that access prices would be lower for relatively low risk types but their server space would be more-heavily rationed in comparison to relatively high risk types who would pay more per unit of server space but suffer less quantity rationing. The high risk types would impose negative externalities on the low risk types since contracts accepted by low risk types must not also attract high risk types.[19] These contracts, however, may be very difficult to implement since even if subscribers could be distinguished as to risk type, the demand for server space is very unlikely to be identical across subscribers yet is required to be known by ISPs in order to design separating quantity-rationed contracts.[20]

[19]Pooling (Nash) equilibria tend not to exist in models of this genre; see Rothschild and Stiglitz (1976) for an insurance market example. Further, as is well-known, separating (Nash) equilibria may not always exist, although either pooling or separating equilibria exist under alternative non-myopic equilibrium concepts such as anticipatory or reactive equilibria.

[20]For similar reasons, Hamdami (2003) rules out implementable costly signaling by law-abiding types that would permit their identification and result in access at lower prices than wrongdoers.

Competition may also be inadequate to generate optimal monitoring on other grounds, according to Hamdami. ISPs compete on a range of bundled characteristics that might prevent separation of say, quality, bandwidth, and monitoring. Internet access is also provided incidentally to other services (e.g., in Universities) and service quality (monitoring included) is likely to play a small role in the choice of institution by either faculty or students. The presence of switching costs may be sufficient to keep subscribers with their current high-monitoring ISPs, particularly if early entrant market-leading ISPs have engaged in strategic policies involving switching costs.

3.1.3. *The Role of Private Contracting.* While the Ministry's Discussion Paper did not specifically raise the question of the appropriate role of contracts in attenuating digital copyright piracy, respondents were free to raise the issue. In the event, neither the DP nor submissions thereto had much to say about the role of private negotiations in attenuating problems associated with strict liability.[21]

Are competitive market forces likely to be sufficiently strong so as to align the incentives of the parties involved? ISPs compete to attract subscribers by offering them more profitable opportunities. Subscribers would not accept a less profitable contract offering fixed fees for space provided compared to an alternative that was no less profitable for either party, and which would induce the ISP to adopt an efficient technology for monitoring with a different fee structure. If an ISP can commit to optimal monitoring, the joint surplus of the parties will be maximized. To induce an ISP not to set a fixed fee that ignores a website-owner's lost benefits from exclusion of valuable legal material, the owner will write a contract such that the ISP will be compensated for the increase in expected ISP liability resulting from the choice of socially optimal technology along with a side payment reflecting the negotiated share of additional subscriber benefits obtained by the adoption of this technology.

Hamdami, however, rejects the generality of this argument on the grounds that transactions costs of different types might prevent the parties from negotiating efficient outcomes and thereby eliminating the risk of overzealous censorship. A number of examples are provided. First, the terms for the removal of specific infringing items could be negotiated. But if an ISP blocks access to a suspicious site, all end-users who rely on the ISP to provide them access are denied the ability to view the material. The collective gains to these users might outweigh ISP liability but the transaction costs for any user (or organized group of users) might exceed the individual benefits obtained. Among respondents, the submission of IBM NZ Ltd. addressed this issue, but argued instead that ISPs should not be liable for removal or restriction of access to potentially infringing material on request. Recognizing that in the absence of liability to compensate subscribers harmed thereby, ISPs will typically respond positively to such requests and hence copyright owners who deliberately misrepresent the facts should be liable for damages to users. This

[21]Two DP respondents favoured zero liability for ISPs on the grounds that contracts between ISPs and subscribers frequently shift liability for copyright infringement from ISPs on to subscribers; cf., D.J. Harvey (emphasizing liability assignment as a contractual matter), and National Library (emphasizing that ISPs would inform users of their statutory obligations regarding copyright infringement). The New Zealand Computer Society Inc. argued that ISPs should not be prevented from setting contractual terms and conditions providing them with rights to control content, but these rights should not extend to blocking transmissions. Courts, however, were seen as requiring the power to order ISPs to remove stored illegal material.

argument, however, does not address the issue of which agent is the least-cost identifier of infringing material. Many copyright owners may find it prohibitively costly to identify the multitude of sources of infringement and hence request few, if any, ISPs to block access or remove material. In these circumstances, under-deterrence is likely to occur.

Secondly, a web-hosting contract might specify the technology to be adopted by the ISP for monitoring purposes, along with the conditions under which an item can be removed. But this involves bait and switch, and the ISP has a strong incentive to renege on its contractual promises if users cannot verify to a third party that the ISP is failing to perform its obligations. Observing and verifying monitoring policy is costly for subscribers, and end-users cannot easily make reliable inferences from their available information. The removal of a particular infringing item is not a reliable signal that all infringing items have been removed. Hence, end-users may be unaware of the extent of blocking by an ISP.

Finally, Hamdami claims that the legal system itself might impose obstacles to private contracting. A commitment to limit monitoring would undermine an ISP's decision in future litigation over any failure to remove offending material. If the standard is an 'all possible' (or even 'all practicable') steps to prevent misconduct rule, it would be hard to argue in court in the face of contracts where ISPs explicitly agree not to monitor with excessive ferocity. Further, the legal system may impose constraints on the ability of subscribers to sue ISPs for damages associated with removing their materials from the Internet.

4. The Design of Copyright Law Reform

The above considerations lead Hamdami to suggest that no single rule should cover all cases of third-party liability, and he offers three distinct strategies for implementing the "incentive-divergence thesis". Liability rules are tailored to specific situations, similar to the standard arguments in favour of tailoring rules in (primary) tort liability.[22] This contrasts markedly both with the general nature of both the DP and PP Paper submissions and also the liability rules subsequently adopted by the Ministry. It is argued that efficient law will take different severities of overdeterrence into account. The strategies suggested involve (i) strict liability with suitable adjustments in penalty levels, (ii) having the state determine appropriate ISP monitoring levels either via a monitoring-regulation regime or via a negligence-based regime, and (iii) regulating the contractual arrangement to overcome divergence of incentives.[23] These are considered in turn.

4.1. **Adjusting Penalties.** Although DP respondents were free to raise the issue of appropriate penalty levels under the current Act or proposed amendments thereto, few chose to do so. Absent overdeterrence, however, optimal expected penalties should equal social harm, and when apprehension probabilities are less than one, punitive damages should adjust so as to maintain the equality between expected damages and losses to copyright owners. It was argued in the DP submission of Microsoft New Zealand Limited ("Microsoft") that penalties in New Zealand are insufficient to deter digital copyright piracy and that effective enforcement was

[22]See, for example Shavell (1987).

[23]The emphasis is on third-party liability when full technical control is available. An issue is whether there are incentives to develop ISP formats where such control is absent or only partial, and where users may circumvent control, perhaps under contracts with ISPs.

a critical aspect of copyright law reform. Not surprisingly, this submission focused on computer software piracy in its various forms.[24] Overdeterrence is not discussed in the Microsoft submission, but seems likely to be of significance for software only for the case of Internet piracy. Given that underdeterrence was the major focus, Microsoft recommended a substantial increase in the level of criminal enforcement since in their experience, civil action is insufficient. The high cost of bringing actions was seen to be a disincentive for many copyright owners to bring suit, while procedures were argued to be inadequate either to apprehend offenders or to secure effective remedies. Court orders were flouted, companies liquidated to become judgment-proof, and damages were arguably undercompensatory.

To date, *no* civil suits under s 36 of the Act have been brought in New Zealand,[25] and the rare cases of criminal actions, which focus on technical procedural matters concerning evidence acquisition, tend to be based on s266A or 266B of the Crimes Act 1961 rather than s 131 of the Copyright Act.[26] Criminal actions can be brought by police or private prosecution, with higher penalties than for their civil counterparts (including imprisonment up to 10 years), but require proof of intent to defraud, and consequently do not apply to most instances of copyright infringement. The apparent reluctance of the police to prosecute for copyright infringement was possibly a "hangover from initial judicial resistance" that infringement is properly a crime rather than an invasion of a private property right.[27] As a consequence, Microsoft recommended the introduction of sentencing guidelines to ensure imposition of higher penalties for software theft, along with a statutory damages regime similar to that adopted by the US and Canada, an example being s504 of Title 17 of the United States Civil Code, whereby a copyright owner may elect trying to prove damages or ask the court to award statutory damages.[28]

Although heavy costs of litigation and inadequacy of awards of damages may deter copyright owners from pursuing pirates via the courts (and little is known about settlements in this regard), it must also be noted that an inability to establish significant harm is an important deterrent to litigation, as it should be.[29] In the event, the Ministry made no recommendations concerning the levels of penalties

[24] *Number One Software v Dr Floppy Ltd*, unreported, High Court Auckland, 24 April 1989, CP748/89 is a rare New Zealand case brought for counterfeiting software, where injunctive relief was awarded to the plaintiff as exclusive licensee of a major word-processor program.

[25] Although Telecom's DP submission argued (p. 12) that it was "only a matter of time".

[26] See, for example, *R v Mikhail* (1999) District Court Reports (NZ) CR 331, and *Power Beat International Limited v Attorney-General* (2000) 2 New Zealand Law Reports 288. In a rare case brought under s 131 in 1995, an Auckland counterfeit software dealer was convicted and fined NZ $18,000. The illicit software, however, was valued at $1.28 millions. See AJ Park & Son (1998, paragraph H. 27) for discussion.

[27] Cf., Microsoft, DP Submission (p. 17).

[28] Those found guilty of an offence under s131(5) continue to be liable for fines up to $150,000 but the maximum term of imprisonment has recently been raised from 3 months to 5 years. For statutory damages in the US, a range of US $750-30,000 (approximately NZ $1,150-45,000) covering all infringements in respect of a single copyrighted work applies, and for willful infringement, up to US $150,000, applies. Pending legislation to amend s 504(b) of Title 17 provides that for certain digital-based infringing copyright material distributed through networks that is known, or should have been known, to be commercially distributed, the presumed minimum fine per infringement will be at least US $2,500.

[29] Thus, in the celebrated *Napster* case, Liebowitz (2002) argued that evidence of past harms to the compact disk industry was not well-established, but reasoned that future harms may well be considerable. In later work, (Liebowitz, 2003) found that significant, if non-fatal, injuries had indeed occurred.

in New Zealand, and did not propose the introduction of statutory awards. If expected penalties *were* set appropriately in the absence of overdeterrence, however, it is arguable that penalties should be reduced *below* the levels of harms suffered in the presence of overdeterrence (Polinsky and Shavell, 1979). The notion is to maintain the informational advantages of strict liability while eliminating the risk of overdeterrence. Hamdami, however, considers that this approach would only generate optimal deterrence in highly limited circumstances, involving profit-sharing contracts between web-hosting ISPs and their subscribers.

The argument is that if ISPs charge fixed fees and so derive zero marginal benefit from an increase in the number of items posted by a subscriber, overdeterrence will continue as long as penalties imposed on the ISP are positive. Removing items is costless whereas expected liability costs are positive. Unless they drive subscribers into the arms of rival ISPs, nothing is lost from removing items if liability falls as a consequence. Each additional posted item suspected of being infringing increases exposure to liability. As Hamdami argues, however, scaling down penalties will not do the trick unless removal costs are positive. If the ISP acquires a share of the benefit generated by a hosted website, then, for any given share, penalties can be scaled-down appropriately to induce optimal monitoring. The incidence of benefit-sharing appears to be rare, including in New Zealand, presumably because subscriber benefits generated by most hosted websites are not verifiable and contracts cannot be conditioned on this information.[30] For this reason, and because courts would be faced with the difficult task of verifying the socially optimal level of monitoring in order to calculate the required reductions in the penalty rates, it is unsurprising that the Ministry has not pursued this option for legal reform.

4.2. **State-determined ISP Monitoring Levels.** A different approach suggested by Hamdami would grant the state power to specify the required level of ISP monitoring in one of two ways. First, lawmakers rather than ISPs might be assigned the task of setting the optimal level of monitoring, and liability for ISP misconduct would occur only when the ISP fails to meet the regulatory standard. Overdeterrence is eliminated by making the divergence of incentives between ISPs and their subscribers irrelevant for ISPs' decisions to monitor. ISPs would compare the cost of compliance with the expected liability of failing to comply, and there would be no incentive to monitor beyond the minimum level specified in the regulations. This approach is information-intensive for lawmakers since it not only requires estimation of the social harm of user misconduct but also the actual cost of monitoring, its effectiveness as a deterrent to misconduct, and its effect on legitimate conduct.

Alternatively, a negligence-based standard could be adopted, whereby the optimal level of monitoring would be determined by the courts, so that ISPs would only be liable if they fail to meet this standard. If courts succeed in determining the optimal level of monitoring, ISPs will not monitor excessively since there is no payoff at the margin for so doing. There may also be good reasons to combine an *ex post* negligence rule with *ex ante* regulatory standards in the likely event that poorly-informed courts make errors in their estimate of the socially optimal level of monitoring.[31] *Ex ante* liability would hold ISPs liable for deficient monitoring

[30] A counterexample provided by Hamdami is auction sites, where fees tend to vary according to the sale prices of items sold through the site. Notably, auction outcomes can be monitored almost costlessly by ISPs, unlike transactions arising more generally from hosting websites.

[31] Cf., Kolstad et al. (1990). This analysis has been applied in the New Zealand context to explaining the role of safety standards in complementing a version of the negligence rule in the

effort even where it is not established that any harm has been suffered as a result of copyright infringement. The standards send a signal to ISPs of the courts' 'bottom-line' permitted level of monitoring, and hence reduce any dilution of incentives to take care due to uncertainty associated with *ex post* liability rules. If uncertainty is considerable, ISPs will find that increasing monitoring effort will have little impact on savings in expected liability payments, and will tend to monitor at too low a level. The function of the standard is to induce ISPs that engage in too little monitoring to revise upwards their perceptions of the strictest legal standard of care. The defect of this approach, however, is that if overdeterrence occurs under the *ex post* negligence rule, the overdeterrence problem will be exacerbated.

In the New Zealand context, the DP did not explicitly seek submissions on the issue of monitoring duties. Several respondents, however, raised concerns about any such requirements.[32] In some cases, this was due to a belief that monitoring was impossible. For others, it was "impractical", partly because of the scope of the problem in terms of data volumes, and because of privacy issues. However, concern was also expressed about the imposition of additional costs on ISPs and users. Imposing monitoring duties that necessarily removed all infringing items without inadvertently removing any non-infringing material, however, is certainly likely to be non-optimal.[33] Lesser duties, however, could clearly be imposed, and two DP respondents recommended that ISPs make positive efforts to regulate content as a necessary condition for exemption from liability.[34]

In Hamdami's view, supporters of voluntary ISP monitoring implicitly accept the view that copyright holders are in the best position to detect online infringement, in which case it might be desirable to place the burden of detection on them. The imposition of strict liability on ISPs would leave copyright owners with no incentives to assist in acquiring infringement information. A number of DP submissions, however, instead expressed concern with zero ISP liability on the grounds that it also fails to facilitate cooperation between copyright owners and ISPs, but here the problem is that ISPs have no incentive to monitor for subscriber infringement.[35]

Of course, concerns about the adverse incentive effects of either zero or strict liability regarding negotiations between copyright owners and ISPs in respect of infringement detection fly in the face of the Coase Theorem. Presuming rights are well-defined in favour of copyright owners, the liability rule should be immaterial

---

context of New Zealand's Health and Safety in Employment Act 1992; see Gordon and Woodfield (2001).

[32]See, for example, A.H. Higgins, Electronic Frontier Foundation, Ken Moon & AJ Park, and New Zealand Law Society.

[33]Microsoft also argued against costly monitoring being imposed on ISPs, considering that if a notice is received that infringing material resides on an ISP's network, out it must go, and fast. The issue of removal of legitimate material, however, was not raised.

[34]The New Zealand Rugby Football Union recommended imposing liability if an ISP did not make "reasonable effort" to regulate content, while Sky Network Television Limited supported liability where an ISP makes "no effort" to regulate content. Taken literally, the latter would have ISPs avoiding liability with minimum feasible effort. The respondent provided examples of effort in terms of either a statement of policy regarding copyright infringement, or scanning material for potential infringement, the latter appearing to be a much more costly exercise. If the "reasonable effort" requirement is interpreted as equalization of the marginal benefits (in terms of expected liability payments) and marginal cost of monitoring, strict liability will generate overdeterrence, and the requirement will need to account for this when it is implemented if an efficient outcome is to be achieved.

[35]Cf., IBM NZ Ltd, Association of Consulting Engineers, and Microsoft.

according to this view. Under strict liability, ISPs will wish to minimize the costs of adopting monitoring technology and will purchase copyright-owner support if owners are least-cost detectors. Under zero liability, if owners are least-cost detectors, owners will purchase ISP support in tracking down Internet pirates. Contractual arrangements of this form, however, are likely to stumble for a number of reasons (De Meza 1998), including conflict of interest situations for ISPs who possess service supply contracts with their subscribers, many of whom may be Internet copyright pirates. Nevertheless, ISP contracts with subscribers can specify terms and conditions for service provision that are contingent upon subscribers posting legitimate information, and can make known to subscribers side agreements with copyright owners regarding infringement detection procedures. Where bargaining fails, however, the choice of liability rule is crucial, and a single rule is unlikely to be optimal in all circumstances.

In the event, no monitoring provisions were included in the Ministry's proposed amendments to the Act. It appears that the majority view may have swayed the day on this issue, and, if so, raises the important matter of appropriate incentives for R&D in the monitoring technology industry itself. It is inappropriate to take the cost structure of existing monitoring technologies as immutable, since investment in new monitoring technologies will not be independent of the extent of copyright protection or the nature of the secondary liability rule. If, as is widely argued, copyright protection under existing legislation has been seriously eroded by the advent of digital technology, ISPs will have felt relatively immune from liability and so have little reason to invest in monitoring technology. Knowing this, the best response for manufacturers of such technologies is not to invest in cost-reducing technologies which would only be profitable if it were cost-minimizing for ISPs to adopt them under the liability rules ultimately adopted across most jurisdictions. As a small country without a developed industry producing monitoring technologies, however, the secondary liability rule adopted by New Zealand will have negligible effect on these investment decisions. In this case, it may be optimal to follow an international standard even if the latter has limited merit.

If a general rule of ISP monitoring is sought, however, it could be specified in a general form, much as is the reasonable care standard of the negligence rule in tort. And while verification costs may be high in respect of determining whether an ISP is in compliance with socially optimal monitoring, enforcement costs could be reduced by engaging in random monitoring with penalties increasing sharply in terms of the deviation from the regulator's estimate of the socially optimal monitoring level.

4.3. **Knowledge-Contingent Standards and Contractual Arrangements.** Of the DP submissions that included a discussion of ISP secondary liability, three-quarters favoured liability where a knowledge-contingent standard had not been met. Knowledge-contingent standards have been advanced as responses to over-deterrence in ISP monitoring (Yen, 2000), where liability is imposed on ISPs only if they fail to remove or block access to material known to them to be illegal. Notably, three-quarters of those respondents supporting ISP liability required that ISPs be notified of infringement by copyright owners. Others may have assumed that ISP knowledge would be acquired only in this manner, but some respondents clearly distinguished knowledge attained by notification from other means. Further, 64 percent of respondents supporting liability favoured harmonization of liability rules with new international standards.

It was less clear as to which existing standard ought to be adopted, although the greatest support was for the Digital Millenium Copyright Act 1998 ("DMCA") adopted by the US. Also supported were standards adopted in the European Union ("EU"), Australia, Canada, and Japan.[36] In the event, the Ministry proposed adoption of regulation 19 of the UK Electronic Commerce (EC Directive) Regulations 2002 for secondary liability.

By way of comparison, s 512 of the DMCA provides various limitations on liability related to online material, and creates affirmative defenses in the form of 'safe harbors' for providers that might have been found liable under traditional principles of copyright law, New Zealand's Copyright Act included. Whether a harbor is safe or not depends on the service provided; in what follows, the focus is on ISP information storage by way of web-hosting. The DMCA also contains detailed prescriptive notice and take down provisions but the EU (including the UK regulations) has not followed suit. Nevertheless, ISPs in the EU are required to act promptly to remove infringing material once known. Both the DMCA and UK regulations preclude liability if ISPs have no actual knowledge of subscriber infringement.[37] Overdeterrence no longer occurs because ISPs will not face liability unless they possess knowledge of infringement. Clearly, they have no incentive to invest in such knowledge since they can only be penalized for its acquisition. At best, ISPs will act to remove infringing material when it is brought to their attention, which raises the problem of whether to remove material merely claimed to be infringing since a rival could falsely claim that an item is infringing hoping that the ISP will remove it.

Although ISPs have incentives to maintain their ignorance of unlawful postings, Hamdami suggests that adopting an actual knowledge framework in conjunction with monitoring-regulation standards *could* create an optimal regime of ISP liability. The idea is that if an ISP meets the monitoring standard *and* removes any infringing material known to be infringing, optimal deterrence is assured. It is evident that New Zealand does not plan to follow this particular path, perhaps reflecting a general (if weakening) move towards light-handed regulation, motivated by a recognition of the informational constraints facing regulators in setting optimal standards along with an unwillingness to explore the prospects for the adoption of incentive-compatible revelation mechanisms.

4.3.1. *Contracting Costs and Monitoring Policies.* The DMCA adopts several measures affecting contracting costs over monitoring policies between service providers and subscribers. First, this legislation provides immunity from liability for web-hosting ISPs choosing to remove material from the Internet. Hamdami notes that this encourages ISPs to inefficiently disregard the costs associated with screening policies and their removal decisions, and potentially impedes attempts to negotiate over monitoring policies. The current New Zealand Act makes no provision for exemptions from liability on these grounds, and the Ministry's proposed amendments

[36] A number of submissions supported more than one standard, suggesting that either they were ignorant of the differences among the standards, or considered the differences immaterial.

[37] Some overdeterrence might persist if courts err in inferring knowledge, or if ISPs are excessively cautious in removing materials because they cannot determine their legality with certainty (or at least not at reasonable cost). For example, the New Zealand Law Society believed that most take down notices will simply be followed automatically. Residual overdeterrence, however, is argued by Hamdami to be less than under strict liability.

contain no plans for immunity from liability for the erroneous removal of legitimate material.

Absent such immunity, however, several DP respondents expressed concern at this aspect of the US take-down provisions. For example, one respondent suggested that ISPs should not necessarily be subject to such provisions, recognizing that suspicious material need not be illegal since permission to distribute copyright material may have been given to a subscriber but which is unknown by the ISP, copyright protection on some items may have expired, or a permitted use under Part III of the Act may be involved.[38]

Concern was also expressed at the prospect of liability for removing legitimate material in response to false (perhaps deliberately false) allegations of infringement.[39] The DMCA deals with this perverse incentive in two ways. First, liability is imposed on copyright owners making false allegations, and, in New Zealand, s130 of the Act currently contains similar provisions. If effective, these provisions should deter false allegations of infringement, and, in this knowledge, an ISP notified of infringing material would be most unlikely to escape liability if a take down notice were ignored. Against this, however, the DP submission of David McNabb emphasized that copyright complainants typically escape liability by declaring the truth of their complaint "to the best of their knowledge". The waters are likely to remain muddy from this perspective.

Secondly, a necessary condition for immunity under the DMCA is that the ISP must immediately notify the subscriber and offer the opportunity to respond and perhaps dispute the decision. The UK regulations, however, contain no similar provision. The general DMCA approach is consistent with another legal strategy suggested by Hamdami; viz, to check overdeterrence via direct regulation of the contractual relationship between ISPs and their subscribers. The idea is that the imposition of uniform measures will reduce transaction costs over monitoring policy and facilitate negotiation, and so avoiding a great deal of duplication in determining whether end-users have continuous access to their desired sites. Not all potential sites are valuable to end-users, and the ISP is the least-cost discloser of their available sites. Hamdami also argues that ISPs might also adopt less aggressive policies if it were immediately known that material was being removed, while immediate notification would facilitate *ex post* negotiation between the parties over the fate of particular items. Once notified, a subscriber believing an item to be legal could make representations to an ISP on the matter. Notification of an intention to remove material unless the ISP was satisfied that the material was legal or that compensation for liability would occur would also facilitate ISP-subscriber bargaining.

In this context, the PP noted that several respondents suggested that the ISP should be required to inform a subscriber that a copyright owner has served a notice requesting removal or blocking of allegedly infringing information, and that the ISP

[38]Cf., Richard Mansfield.

[39]See, for example, IBM NZ Ltd., Richard Mansfield; also David McNabb who recommended absence of ISP liability unless a number of stringent conditions were satisfied, including ISP/subscriber knowledge of infringement and the requirement that the ISP is capable of monitoring and blocking infringing traffic without also disrupting legitimate traffic. This, however, raises the issue of endogenity of choice of monitoring technologies. In order to avoid liability, ISPs may choose technologies that are incapable of generating negative externalities, particularly if they are less costly.

intends to comply. The Ministry supported this position in its proposals. If the ISP is immune from liability by complying, however, any effort to determine whether the complaint is valid has little payoff, and there is likely to be excessive taking-down. Subscribers then have to raise their objections with copyright owners, but this may be reasonable in many circumstances, and it is surely more difficult to falsely argue that a person believed they had ownership rights compared to a subscriber's false claimed belief that they were posting legitimate material. Pre-notification of subscribers, however, is only in response to a notice served on the ISP, and hence is not applicable to situations where the ISP intends to remove or block material as a consequence of monitoring activity that is potentially subject to error. Not only are specific ISP monitoring duties absent from the Ministry's proposals, neither are any incentives for ISP monitoring directly created. Nevertheless, copyright owners need not be the least-cost detectors of infringement in all circumstances. Hamdami, for instance, points to the desirability of affirmative monitoring duties for ISPs concerning unlawful conduct such as online child pornography, for which ISPs are likely to be in the best position to detect wrongdoing.

In the DP submission of the Electronic Frontier Foundation, it was argued that it is unclear whether an ISP is required to implement DMCA-type counter-notice procedures or whether it can avoid liability via a contractual waiver of liability. The view was expressed that most ISPs in the US include provisions in contracts that render counter-notices provisions of the DMCA safe harbors optional, at best. Further, if counter-notification procedures increased ISP costs, waivers rather than counter-notices may be preferred by ISPs, and the provisions would then constitute empty promises. The Foundation concluded by suggesting that ISP attempts to waive liability should be thwarted.

This view does not seem to appreciate that contract terms will internalize waivers, and that liability waiver may be efficient in many cases. Subscribers may find it more profitable to negotiate contracts offering them lower-priced server space even if they lose some custom resulting from take down notices that are followed but not advised to subscribers. For example, suppose that a given subscriber and its ISP both know that the ISP can detect at low cost whether an infringement allegation is true for this particular subscriber. If the ISP charges a uniform price for server space, the subscriber will be inefficiently pooled with others for whom the cost of detection is much greater. By choosing a different mixture of price and information access, the subscriber can be efficiently separated. While the Foundation does not go as far as to suggest that contracts are unconscionable, an argument that would be difficult to sustain in the highly competitive ISP market, their arguments are not consistent with encouraging contractual solutions.[40]

As an alternative, the Foundation recommended a counter-notification process for subscribers wishing to contest allegations, whereby forwarding a copy to the complainant would absolve the ISP from liability. A complainant could then bring suit against the subscriber directly, with costs awarded to a successful defendant if the original notice was determined to have been sent in bad faith.[41] If persons claiming copyright ownership can regularly avoid liability on the basis that they

[40]The Electronic Freedom Foundation also noted that take-down is effective upon notice and remains such for 10 days even if a counter-notice is filed. It was argued that infringement allegations then effectively become gag orders, failing to protect free speech, and encouraging subscribers to inefficiently switch among ISPs in order to avoid these problems.

[41]Costs would presumably be awarded to a successful plaintiff, however.

possessed honestly held beliefs (that may be nothing of the sort), however, notification of claims to ISPs could reasonably be interpreted as cheap talk, especially if the claimants had developed a reputation for false claims over time. To deter such behaviour, copyright owners might be required to post a large bond to a disinterested party that would be forfeited should costly verification by either subscribers or their ISP establish that the claim was invalid, or that inadequate care was taken by the owner in ensuring the validity of the claim. In these circumstances, ISPs could be confident that only valid notifications would be received, and would be advised to remove material to avoid liability.

The Ministry's proposals absolve an ISP from liability by its pre-notification to subscribers of a receipt of notice and intention to comply. If the ISP received notice of allegedly infringing material but without verification, it would likely be found to have 'turned a blind eye' if it did not seek further information from the claimed owner who presumably is the least-cost verifier of ownership. If the ISP requests further information, and is satisfied that it would be prima facie liable if it did not comply, it will presumably then advise its subscriber of its intentions to take down or block the material and hence be free from liability. If the complaint is invalid, however, it is socially wasteful both for investment in evidence supporting false claims and also for access to be denied on the basis of such evidence, and significant user losses could occur during the period where the dispute between the claimed copyright owner and the subscriber is resolved. Excessive taking down is likely to occur, compared to the situation where ISP liability is zero during the period of the dispute and where the material remains available to users.

In both the DMCA and the proposed New Zealand legislation, preconditions for immunity do not apply for the provision of Internet access in its own right. Specialist access providers are not required to follow notification rules. Yet subscribers of access are less likely than website operators to learn about blocking decisions concerning a particular site. Even when they know, the costs of collective action are unlikely to make it worthwhile disputing the decision. Hamdami concludes that "subscribers of access services should enjoy greater protection than should subscribers of hosting services" (p. 952). This is possible if end-users can sue access providers in the event of their being blocked legitimate access, or by imposing mandatory disclosure requirements on access providers who seek to block access. Notably, the Ministry's proposals for New Zealand do not make reference to the protection of Internet end-users against erroneous removal of legitimate material.

4.3.2. *Disclosure Duties of ISPs.* Under the DMCA, to be exempt from liability, ISPs must notify users of policies to terminate accounts of repeat infringers, a provision that is not found either in New Zealand's Copyright Act or proposed amendments thereto. This notification rule serves to reducing transaction costs somewhat. Hamdami, however, notes that the DMCA does not require ISPs to notify subscribers of other aspects of compliance policies, such as the technology used to screen for copyright infringement, and which would also reduce transaction costs between ISPs and their subscribers. No information disclosures of this nature are currently required in the New Zealand Act, and none are contained in the Ministry's proposed amendments, presumably reflecting an implicit assumption that ISPs will not initiate monitoring under the proposed amendments to the Act.

4.3.3. *Comparing the Knowledge Tests.* As far as the current secondary infringement provisions in sections 35-39 of the New Zealand Copyright Act are concerned,

the knowledge test imports a version of constructive knowledge in that an alleged infringer either "knew or had reason to believe" than the act in question constituted an infringement.[42] This contrasts with the knowledge test in both the DMCA and the UK regulations. Here, the tests involve "actual knowledge" of unlawful activity or information establishing the existence of infringement, although the Ministry points out that case law would suggest that "actual knowledge" is somewhat more than what is stated literally, and "would encompass those who deliberately refrain from enquiry or who shut their eyes to that which is obvious".[43]

Constructive knowledge, however, is seen as involving knowledge of facts or circumstances from which a reasonable person would arrive at the relevant belief, mere suspicion of infringement being insufficient.[44] The Ministry's position was to maintain the New Zealand constructive knowledge standard for ISP secondary liability, the major reason being a desire to prevent excessively extensive immunity for ISPs from emerging, and to better allow content owners to protect their exclusive rights. Thus, suppose that an ISP suspects that a particular hosted site contains infringing copyright material. Such a suspicion apparently would not be held to amount to constructive knowledge. If a copyright owner notified the ISP that the site contained infringing material, but without verification of the claim, suspicions might be further aroused, yet the ISP might still not possess constructive knowledge of *actual* infringement. Notification, after all, may only be an allegation of infringement. If the copyright owner provides unequivocal verification of infringement, presumably the ISP then possesses actual knowledge of infringement, and is liable if the infringing material is not promptly removed.

Wherein lies a role for 'constructive knowledge' here? Perhaps if the owner provides equivocal information concerning infringement, so that suspicion becomes even stronger, but is not conclusive? For example, the copyright owner may claim that there exists no royalty contract with the website owner, but this involves a costly verification process for the ISP. More generally, if an ISP seeks verification of ownership, what is its legal status if it remains uncertain about whether the material is infringing? Willful blindness, is one thing, but making zero effort to directly determine infringement is another. Yet, the Ministry does not appear to propose either explicit or implicit infringement monitoring duties on ISPs. Notably, the New Zealand test differs from that in Australia, where regard may be paid to the knowledge, capacity and circumstances of a particular defendant in determining

[42]Once an infringement of copyright is made out, it may be actionable under s 120 of the Act. It should be noted that under s 121 damages are not available where the knowledge test is failed; however, an account for profits will however be available. Where the infringement is of the secondary kind, the infringer would have satisfied the knowledge requirement, so damages would be available.

[43]Cf., Ministry of Economic Development, Position Paper, p. 18; citing in support, inter alia, the New Zealand case *Crystal Glass Industries Ltd v Alwinco Products Ltd* (unreported, High Court, Hamilton, A236/78, 15 April 1983).

[44]Cf., Position Paper, p. 18-19; citing *LA Gear Inc v Hi-Tech Sports plc* (1992) Fleet Street Reports 121, 129. The test in this case was applied in New Zealand in *Husqvarna Forest & Garden Ltd v Bridon New Zealand Ltd* (1999) 3 New Zealand Law Reports 215. Here, the plaintiff produced a set of drawings in which copyright was claimed, but was slow in producing information reasonably requested by the defendant, provided limited data, provided some drawings at a late date, and ultimately relied on only two drawings by the time the trial had advanced to its fourth day. While accepting that the defendant may have had earlier suspicions aroused, no "reason to believe" that infringement had occurred was established prior to this stage of the trial. Injunctive relief, however, was provided to the plaintiff.

whether that person rather than some other "ought reasonably to have known" about an actual infringement. Such a requirement could efficiently impose implicit monitoring duties on an ISP if it were determined that it was the least-cost detector of an infringement.

Unlike the UK regulations, the DMCA distinguishes between contributory liability and vicarious liability regarding secondary infringement, and the knowledge tests differ in each case. The actual knowledge test applies for contributory liability, while, for vicarious liability, if certain other conditions are also met, defendants are strictly liable whatever their state of knowledge of infringement. A contentious condition is that the defendant must have had the right and ability to supervise the misappropriation of the copyrighted work. A broad interpretation such as failing to exercise a veto right to remove potentially infringing material in spite of a prohibitive cost of distinguishing infringing from non-infringing material effectively exposes an ISP to strict liability, inducing overdeterrence. Hamdami prefers a narrow interpretation which changes the emphasis from the identification of the party that should internalize the social cost of infringement to the provision of incentives for third parties to police infringement while eliminating risks of overdeterrence. The narrow approach requires a cost-effective ability to distinguish types of material located on an ISP's servers, and finds liability when appropriate actions are not taken.

An optimal regime of third-party liability should target the least-cost avoiders of the misconduct, and Hamdami argues that while contributory liability targets those who have knowledge of infringement, vicarious liability targets third parties with low monitoring costs, thereby providing incentives to detect infringement. Further, vicarious liability typically requires that third parties gain financially from their underlying misconduct, which Hamdami reasons can be rationalized as a deterrent to excessive monitoring since it provides for the internalization of the social cost of their monitoring activities if ISPs lose profits as a result of censoring material held on its network.

Among the DP submissions, only the Auckland District Law Society and Technology Committee addressed the distinction between contributory and vicarious liability for ISPs. After reviewing relevant overseas case law, the Society argued that ISPs should be (i) liable for contributory infringement where the ISP's "contribution" is active, and (ii) vicariously liable, except where reasonable steps to prevent infringement have been taken. The latter condition seems consistent with Hamdami's analysis of the overdeterrence problem, although the Society did not elaborate in its submission. The recommendation did not form part of the Ministry's proposals, again reflecting an apparent acceptance of a rather too general view of the inability of ISPs to detect infringement at reasonable cost.

4.3.4. *Authorization and Australian Legislation.* The Australian approach to regulating digital copyright infringement received a mixed reception in the New Zealand DP submissions. The New Zealand Copyright Act, unlike its Australian counterpart, does not have an explicit provision where an ISP could be liable by reason of authorizing an infringement of copyright. Section 16(1)(i) of the New Zealand Act provides that a copyright owner has an exclusive right to authorize copying of the owner's copyright-protected material. The issue at stake, however, is the authorization by a person of illegal copying by another party. The Act, unlike s 16(2) of the UK Copyright, Designs and Patents Acts 1988 which it follows closely on

these matters, does not directly address this issue. In the UK Act, s 16(2) provides that copyright is infringed by a person doing, or authorizing another to do, any act restricted by the copyright. Consequently, authorizing illegal copying must arise by implication under s 29(1) of the Act, so that authorization is treated as equivalent to primary infringement. The High Court in Fibreglass *Technologies Ltd v Fibreglass Solutions Ltd* (Unreported, High Court Auckland, 30 May 2002, M1727-SW99), however, indicated that authorization of an infringement means more than mere "sanctioning, approving, or countenance" of that infringement by another. In the case, a number of actions of the Managing Director of the defendant companies were essential inputs into the primary infringement.

It is likely that the provision does not operate like the secondary liability authorization provisions of the Australian Copyright Act 1968 as amended in 2000 to incorporate changes in digital technology. Section 36 provides for secondary infringement by way of authorization of a restricted act. An ISP may be liable if deemed to authorize an infringement, s 36 further specifying considerations to be taken into account in determining whether authorization has occurred. These considerations are a codification of the High Court of Australia decision in *Moorhouse*.[45] In this case, the University of New South Wales was held to have authorized infringement of copyright where students used coin-operated photocopiers in the University Library to make infringing copies of a work.

Included in the Copyright Amendment (Digital Agenda) Act 2000 was s 39B, which provides that an ISP does not authorize copyright infringement "merely because another person uses the facilities so provided to do something the right to do which is included in the copyright". It is arguable that little has been clarified regarding ISP liability by this provision. For one thing, it appears to have been interpreted differently in the DP submissions of Telecom and the New Zealand Law Society ("Law Society"). In Telecom's interpretation, ISPs would not be taken as having authorized infringement merely because they had provided facilities that are used for infringing purposes. The Law Society's interpretation seems much more narrow, considering that ISPs were given very limited protection from liability in that the while the mere provision of facilities used by someone to do something that is not itself a breach of copyright, an ISP is *not* protected where its facilities are used by another party to infringe copyright. Both interpretations cannot be correct, and Telecom's sigh of relief may be premature.

Secondly, the new provision has been criticised as being uncertain as it raises the question as to when an ISP does more than provide 'mere facilities'.[46] Where more are provided, liability is determined by the common law of authorization. The Law Society, however, noted that there was little real direction as to what might constitute reasonable steps to prevent infringement from occurring in the context of an ISP's service provision. Microsoft argued in similar fashion, considering the provisions to be too general in nature to be capable of precise application, so that courts would become arbiters and be required to build up bodies of precedent. This process, described as "laborious and undermining", was unfavourably compared with the provisions of the DMCA, which offered clear procedures to absolve complying ISPs from liability. It seems that the march of technology is too impatient for

[45] *University of New South Wales v Moorhouse and Angus Robertson (Publishers) Pty Ltd.*, (1975) 6 Australian Law Review 193.

[46] For further discussion on the new provisions, see Aplin (2001), especially pp. 572-73.

the development of a suitable common law of authorization.[47] Nevertheless, the approach, rejected in the New Zealand proposals, shifts the burden of detection from copyright owners (who would no longer have to scour the University libraries and computer laboratories of the world sniffing out miscreant students) to ISPs, who, in some circumstances at least, may be least-cost detectors of infringement. As is the way of things, trying to find a single liability rule that is optimal in all circumstances is likely to be a chimera. In this context, the Recording Industry Association of NZ argued that ISPs are frequently not only the only means by which infringement can be stopped, but also initially detected, so that blanket immunity would remove any incentives for ISPs to prevent distribution of infringing material and to cooperate with rights holders.

4.3.5. *Peer-to-Peer File Sharing Issues.* As noted above, Hamdami considers that the DMCA provides insufficient protection to those who buy access services, and this failure "is very significant because it is very likely that the emergence of distributed peer-to-peer file exchange services in the aftermath of the Napster injunction would increase the pressure on content providers on access providers to prevent the access of their users to these file-sharing networks" (p. 952). Given that New Zealand appears set to adopt legislation requiring prompt removal of allegedly infringing material by ISPs, similar concerns hold.

The debate concerning copyright piracy in music file-sharing has crystallized many problems of the design of robust secondary liability rules for ISPs. The ability to make near-perfect copies of delivery goods at trivial cost compared to the market prices of those goods at their release dates in circumstances where royalties comprise a small fraction of these prices has seriously begged the question as to whether copyright law as currently designed excessively protects copyright owner's exclusive rights or fails to properly protect those rights. Taking protection as given, however, eradicating piracy arising via music file-sharing technology has been a major issue for recording companies, and for which the Napster injunction was seen as a major victory. Napster was first in its use of peer-to-peer file-sharing websites, transmitting MP3 music files over the Internet rather than through its own servers. Napster did not transfer music so could not be liable for nor commit primary infringement, but were sued for secondary liability.[48] Nevertheless, the steps required to obtain the music file could not be taken without the use of

[47]The Microsoft DP submission raised the following related issue; viz, would rapid technical change affect the relative merits of the Australian and US approaches? Not so, according to Microsoft, since the basic structure of the Internet is well-established and so the basic provisions of the DMCA should be able to be maintained for some time. Alternatively, its provisions could be amended. The New Zealand amendments, however, appear likely to exceed a three year consultation and enactment period, a lengthy period in a world of changing digital technology.

[48]*A & M Records, Inc. v Napster, Inc.,* (N.D. Cal., 2000) 114 F. Supp. 2d 896; *A & M Records, Inc. v Napster, Inc.*, (9th Cir., 2001) 239 F. 3d 1004. Napster was variously sued for vicarious (and contributory) liability. A preliminary injunction enjoined Napster from facilitating music file downloading but the two courts disagreed as to its scope. The District Court ruled that Napster must screen out all infringing files on its server regardless of the ability to find them infringing. The Ninth Circuit remanded and instructed a new injunction that would account for the limited ability to distinguish infringing and non-infringing files with a given architecture of its system. At that time, Napster was able to detect infringement only on the basis of the names given by subscribers to the files offered for downloading. Note that the narrow interpretation of the control requirement by the Ninth Circuit took system architecture as given. Architectures, however, are endogenous, which raises the issue of inefficient incentives to choose architectures than cannot distinguish infringing material at reasonable cost, thus encouraging underdeterrence.

the Napster server, which was an essential input into the infringing activity. The ensuing litigation ultimately left Napster with a shut down order until they could comply with previously imposed revised preliminary injunctions.

A major plank in Napster's defense was that as an ISP, they were a mere passive conduit, entitled to the protections of the safe harbours of the DMCA. The fatal flaw, however, was their evidence that the MP3 files were never transmitted through their servers, the files being transmitted through the Internet from the host user's Napster browser to the requesting user's computer. As a consequence, Napster was held not to be a mere conduit, being well aware of the infringing activities of users, had failed to remove infringing material, and had materially contributed to infringing conduct of users.[49]

Not surprisingly, ingenious investment in litigation-defying technologies quickly emerged.[50] In *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.*, (C.D. Cal., 2003) 243 F. Supp. 2d 1073, a consortium of motion picture studios and record companies brought an action against companies that produced the Grokster and Morpheus file-sharing software.[51] Unlike Napster, these file sharing networks existed without a central server, and once the relevant software program was downloaded, Grokster or Morpheus ceased to have any further involvement in the copying process. Unlike Napster, the defendants provide no infrastructure that directly support infringing activity, and as in *Sony Corporation of America v Universal City Studios, Inc.*, (1984) 464 US 417, the defendants distribute and support software that users can choose to employ for lawful or unlawful ends but which is outside the control of the defendants. Be it peer-to-peer software or a videorecorder, liability does not accrue merely because the technology may be used to infringe the plaintiff's copyright. Here, it was held it had not been established that the defendant companies had made a substantial contribution to the infringement and hence were not subject to secondary liability.

The failure of the action against Grokster and Morpheus means that there is no central body who is a clear defendant in these cases.[52] This could explain why the Recording industry has now focused its attention on the individual user, encouraging peer-to-peer users to develop new encryption devices to hide infringing files as quickly as the industry can break the encryptions.

These cases make an interesting comparison with *Re Aimster Copyright Litigation*, (7th Cir., 2003) 334 F. 3d 643. Aimster operated a peer-to-peer file sharing system similar to that of Napster in that a central server facilitated the searches and requests for files. Communications between users, however, were made through the America Online ("AOL") Instant Messaging Service. An Aimster user needed

[49]Napster also had further problems since their policy regarding termination of accounts of repeat infringers, required under s 512(i) of the DMCA, was not advised in writing to users and was only publicized when action was brought.

[50]Liebowitz (2002) points to the irony of the Napster victory for the recording companies, since the resulting Napster-substitutes pose much more serious litigation-proof forms of unauthorized online copying. Landes and Lichtman (2003) consider these dynamic responses to be both predictable and inevitable, and must be accounted for in deciding the appropriate role for indirect liability.

[51]These programmes were spawned by the Gnutella program and demonstrate that once a program like Gnutella enters the public domain of the Internet, it takes on a life of its own, and continues to exist long after its origin disappears.

[52]For a discussion of the 'phantom defendant' problem for policing Internet piracy, see Riehl (2001).

to be logged on to AOL, and transmissions occurred through the AOL system. Further, all communications were encrypted, so that Aimster remained unaware of what was being traded through their network. Lacking actual knowledge of infringement, Aimster considered themselves free from secondary liability.

As with *Napster*, a preliminary injunction was entered. Justice Posner considered that the central issue was whether Aimster came within the *Sony* exception that there were substantial non-infringing uses for their service. Aimster argued that proof of a possible non-infringing use was all that was required to fall within in *Sony*, whereas the plaintiffs argued that a single known infringing use is sufficient. Posner J rejected both arguments, considering that recognition needs to be given to the respective magnitudes of the actual and potential infringing and non-infringing uses.

In any event, the Aimster service was put solely to infringing use, and Aimster failed to adduce any evidence at all showing that there were non-infringing uses. The online tutorial instructed users how to download copyrighted material, and the only revenue that was made was subscription to a service allowing the user to download any of the top 40 traded music files without needing to search and link up with another user. Posner J considered that Aimster invited the users to trade copyrighted material, an element that was missing in *Sony*, as Sony never promoted infringing uses of their video recorder. Posner J also made reference to the safe harbour provisions in the DMCA, indicating that they will apply where ISPs do what is reasonable to prevent the use of its service by repeat infringers. These conditions did not apply to Aimster as by providing encryption, Aimster deliberately disabled itself from doing anything to prevent infringement.[53] In this light, it should be recognized that actual knowledge of infringement for an ISP may frequently arise because of notification by a copyright owner, but, given the 'blind eye' arm of this knowledge test, ISPs may be held to have actual knowledge in a wide range of other circumstances likely to be relevant in digital distribution context. Since New Zealand plans to maintain its constructive knowledge test, it will be interesting to determine the extent to which ISPs will need to take positive actions to acquire knowledge in order to be immune from secondary liability, rather than simply fail to take negative actions which deliberately deny them knowledge they could attain at negligible cost.

In the absence of legal reform in New Zealand, it was argued that it was "likely that a Napster-like service could currently be operated in New Zealand with impunity".[54] Further, DMCA-type provisions were viewed as having the merit of avoiding problems of regulation via secondary liability provisions currently framed in terms of tangible copies but which would be likely to become less relevant to digital distribution issues such as file-sharing services. For example, Microsoft argued that Napster was guilty of copyright infringement because the US law relating to secondary liability was sufficiently broad to apply to activities that encourage or knowingly facilitate copyright infringement by others. In contrast, the New Zealand provisions were seen as relatively fact-specific, and not technology-neutral. In particular, s 36 of the Act might be inapplicable because Napster-type services neither possessed nor dealt in infringing copies (even if digital music files are characterized

[53]For an attempt to reconcile the different legal treatment involved in the apparently similar cases of *Sony*, *Napster*, and *Aimster*, see Armstrong (2003).

[54]Ken Moon & AJ Park, DP submission, p. 7.

as 'objects').[55] Also inapplicable could be s 37, which provides for infringement where it is known or believed that the 'object' designed or adapted for making copies will be used for illegal copying, unless Napster-type software could be characterized as such an 'object'. Microsoft concluded by arguing that secondary liability provisions should be amended to cover Napster-type activities, perhaps by including a specific provision applying to activities encouraging or knowingly facilitating infringement of copyright by others, a recommendation that has not been taken up by the Ministry.

As a consequence, a suit brought against a Napster-type service would be a nice test of sections 16(1)(i) and 29(1) of the Act, but nothing has yet reached the New Zealand courts. On 28 October 2003, however, it was reported that among the many file-sharing websites in existence in New Zealand, the ISP Orcon had removed a site www.p2p.net.nz, thereby narrowly avoiding legal action from the Recording Industry Association of New Zealand.[56] This site utilized Orcon's servers and was reported to act as a trading point for MP3 music files, digital versions of blockbuster films, and pirated software. Although the content was not hosted centrally, and was instead stored on the computers of users connected to the hubs via software programs such as DC++, the Association's chief executive reportedly argued that downloadable infringing material existed on the hub, and while pleased to see its exit from the market, planned to pursue action against those that sought to take its place. Nevertheless, the action was not seen as sufficient to deter all illegal file-sharing activity, and the Association believed that ISPs needed to take more responsibility in policing file-sharing. Further, in mid-2003, three stores in Dunedin received notices from lawyers of the Association threatening legal action if they did not remove vending machine like compact disk ("CD") copiers from their store. Similar to a drinks vending machine, the copiers were on public display in a retail outlet, and a customer could copy a CD for $NZ 5.00.

In neighbouring Australia, however, music file-sharing litigation has proceeded where relatively weak protection for ISP secondary liability is argued to occur. The ISP ComCen, a subsidiary of E-Talk Communications, has been sued by the Australian Recording Industry Association for profiting from the illegal sharing of music files. The site www.mp3s4free.net, hosted by ComCen, allegedly facilitated 140 million illegal downloads in a twelve month period. Following an investigation by Music Industry Piracy Investigations ("MIPI"), proceedings were brought against the site and ComCen, reportedly the world's first instance of action against an ISP.[57]

The MIPI alleged that up to 20 percent of ISP revenue came from the illegal trade of music files, the increased revenue resulting from greater flows of Internet traffic and greater file downloads. Similar to Napster, mp3s4free did not have any illegal files located on their site; rather, it acted as a search engine or directory allowing users to find the songs that they wanted. As no music files were ever on

[55]Unlike the circumstances in *UMG Inc. v MP3.Com Inc.*, (S.D.N.Y. 2000) 92 F. Supp. 2d 349, where it was held that MP3.Com permitted a user to listen to an illegitimate rather than a literal copy of a CD owned by a user, even though the user was required to established that they owned an original version of the CD. The defense of fair use failed in these circumstances, and would almost certainly fail under the Act since format shifting, although proposed to be made lawful, is currently illegal.

[56]Cf., Peter Griffin, The Herald, (28 November 2003) Plug pulled from file-sharing hub; http://www.nzherald.co.nz/story/display.cfm?storyID=3536469.

[57]Cf., (www.australianit.news.com, 22 October, 2003).

the site, no music files were ever located on ComCen's servers, and the ISP argued that since no hosting of infringing material occurred, it could not be found to have infringed copyright. Unfortunately, the particular legal arguments are at this stage unknown, although it has been alleged that ComCen has profited from the illegal sharing of music files. The site, however, was removed before the court considered the question of whether the absence of infringing material located on their servers ComCen will absolve the ISP from liability. Whether ComCen is sufficiently far removed from the infringement is unknown, but they may be expected to rely on the innocent dissemination defense introduced in 2000.

Institutions that might well be classified as ISPs for copyright litigation under legislative amendments have recently become nervous in Australasia. For example, the University of Canterbury's IT Newsletter (2003) 31(6) pointed to publicity surrounding litigation involving the Recording and Motion Picture Industries against members of the public, including tertiary students, for alleged illegal music and movie file sharing via the Internet. One major tertiary institution had instructed its employees to delete potentially illegal downloaded files from the institution's computers, and the IT Department advised staff and students at the University of Canterbury not to store unauthorized material on their computers, in part because the University may become liable for the consequences even though such actions would be in contravention of University Computer Regulations and subject to discipline.

A likely motivation for this warning is the case *Sony Music Entertainment (Australia) Ltd v University of Tasmania* (2003) FCA 532. Sony, Universal, and EMI identified that users of the networks operated at three Universities had been involved in distributing files containing unauthorized copies of copyrighted music recordings. The music companies brought an action under a preliminary discovery rule that would require the Universities to provide access to the information on the University networks. This request had initially been sent to eleven Universities, of which eight complied, but the Universities of Tasmania, Sydney and Melbourne did not. The Universities did however agree to save a 'snapshot' of what was contained on their network at the time should the court order that access be provided. This snapshot was a backup of all the information held by the University networks at a specific time, including material not relevant to the case. The snapshot was saved on electronic tapes, CD Rom, and hard drives. In the event, the tradeoff between disclosure of infringers and protection of the privacy of innocent parties was resolved by the Court's agreement to Sony appointing a forensic expert to extract relevant information which would be made available to the University, which, after taking legal advice, would provide an affidavit of the inspected documents that would include relevant information enabling identification of copyright infringers and made available to Sony. It should be noted that one of the specific actions that Sony was attempting to support was a possible action against the Universities for authorizing, aiding or abetting a primary act of infringement or distribution of unauthorized copies of sound recordings. The preliminary disclosure rule may also be used to obtain information from a prospective defendant so as to identify whether action can be taken against that defendant.

Further, related Australian litigation has made many Australasian users less blasé about the probability of apprehension for serious copyright infringement. In May 2003, three University students were arrested and charged with offences under the Copyright Act for operating an Internet website offering tracks from over 390

different CDs free of charge over the Internet. All three pleaded guilty and were sentenced in November 2003. The prosecution, backed by the Recording Industry, sought a prison term for the offenders. Two had been charged with multiple counts of distributing, and aiding and abetting the distribution of copyrighted materials that arose from running the site that had reportedly received over 7 million hits and cost the music industry over $A60m. The third student was charged and convicted in relation to four compilation CDs that he had distributed over Internet.

These were the first criminal convictions for Internet music piracy in Australia, although in the UK similar cases had led to prison sentences of between 24-30 months. The Judge sentenced the first two students to 18 months imprisonment, suspended on payment of a $A1000 bond for 3 years. The third student received 200 hours community service, as did the other two for aiding an abetting the third to distribute the compilation album over the Internet. The sentences were suspended because the students were only 20 years old, they had no previous convictions, and they were still studying at University.[58]

Further from home, in July 2003 the Recording Industry Association of America ("RIAA") issued hundreds of federal subpoenas demanding that certain ISPs and some Universities provide the names and addresses of users suspected of illegally sharing music.[59] Two months later, 261 lawsuits were filed against suspected file swappers.[60] The RIAA indicated that those users with more than 1000 music files on their computers that are available for downloading would be pursued. In October 2003, 204 letters were sent to suspected infringers who were advised that unless they contacted the RIAA within ten days to settle, they would be sued. Some 124 users settled for between $US2,500 and $7,500 each, while and the remaining 80 users were sued. At the same time, the RIAA initiated an amnesty scheme for those not already served with notices of suit. The RIAA Anti-Piracy Unit also continued to take action against CD counterfeiters, bringing prosecutions against those who commercially copy CDs then sell them in the Black Market. In the first six months of 2003, some 2.5 million counterfeit CD-Rs were seized.

Such deterrence activity may induce counter-measures. For example, in 2003, a graduate student cracked the protection mechanism developed by SunnComm for BMG. The mechanism downloaded an anti-piracy programme when the personal computer ("PC") automatically loaded the CD, preventing the PC from being able to read an Audio CD. The student, however, found that if the shift key was held down the automatic loading would be bypassed and the anti-piracy programme would not be loaded. This information was posted on the Internet and widely disseminated, causing the share price of SunnComm to fall by one quarter. SunnComm threatened to sue the student under the DMCA, but the action was not pursued.

Music file sharing over the Internet emphasizes the gulf between the retail price of music delivery goods and the cost, expected liability included, of acquiring excellent copies via Internet piracy. Until recently, however, while downloading MP3 files was both quick and easy for users, the same could not be said for downloading pirated

[58]One of the students had claimed that he did not know that his actions were illegal, but it transpired that he had taken a paper in IT law, and had written an essay on the topic of Internet piracy and copyright!

[59]The Los Angeles Times (19 July, 2003) claimed that at least 871 federal subpoenas had been filed seeking users' identities.

[60]Cf., Wingfield and Smith (2003).

movies which required many hours to download files of several hundred megabytes even using broadband connections. During 2003, however, new technology emerged permitting large files to be rapidly downloaded, and which exhibited scale economies which reduced downloading time as a function of the number of 'swarmloaders' simultaneously engaged in the same exercise. This software, of which BitTorrent is an example, operates by permitting users to share bandwidth and make it readily available to other users, unlike networks based on Gnutella and the like, which rapidly reach capacity before search requests for popular music are satisfied. Yet while designed to prevent website bottlenecks, its main use has been for sharing copyright material over the Internet, with rogue sites containing easily downloadable pointers to pirated 'seed' files of copyright films, television shows, programmes and music. The response from the Motion Picture Association of America has been to send approximately 300 infringement notices since November 2003 to the hosts of websites accessible from BitTorrent links.

The curious amalgam of limited successful litigation, legal threats, technological progress, and continued non-accommodated piracy has led to a number of interesting recent market-based developments in the control over illicit trade in the music industry and, more recently, the motion picture industry. For example, early in 2003, British Telecom in association with Warner, BMG, and Universal launched a new Internet music site where a user may download an unlimited number of songs for STG £10 per month. A database of over 150,000 songs emerged, but the files contain a code that allows them to be played on only three designated computers. The downloadable digital music files cannot be copied except onto a blank CD provided that the CD is for personal non-commercial use. Similarly, Apple has developed their iTunes site, allowing the downloading of a particular track for US$0.99 or an entire album for $9.99.[61] The site allows a user to listen to a track before they purchase it, and the ability to sample prior to purchase has been claimed to increase sales as buyers are exposed to music that they would otherwise not buy. Further, Napster, bloodied and presumably somewhat bowed, has returned, although Napster2.0 only permits users to legally purchase music in the same way as does the Apple iTunes site. Thus, technological progress in conjunction with competitive markets may do much to eradicate digital copyright piracy by facilitating the distribution of legal material at a fraction of the current retail price of delivery goods such as CDs.

Regarding New Zealand, the site www.amplifier.co.nz predated Napster, providing a small collection of New Zealand music in digital form at a price of $NZ1.99 per track, much the same as an iTunes price. The site, however, does not sponsor the best-known labels. Only 3000 tracks from as many as 400 independent musicians are available, with more widely-known commercial New Zealand artists unavailable through the site. Because of international licensing issues, tracks featuring New Zealand groups affiliated to international labels are unavailable. As a consequence, the site records only several hundred downloads per month. Although the high profile bands are unavailable from the amplifier website, it would be relatively easy to download an illicit copy over the Internet. The fact that legitimate copies of the available songs are not available in conventional CD delivery good format only

[61] This equates to $NZ17.43, and might be compared with the lowest discounted album retail price of NZ$23.00 that could be found locally, the significant price difference reflecting the inability of New Zealand users to access the iTunes site. Notably, Apple's iTunes Music Store received the accolade of TIME magazine's "coolest invention" of 2003.

serves to increase the demand for illegal copies. In the meantime, international licensing arrangements restrict access of New Zealanders to market-based legitimate online music providers such as iTunes.

5. Conclusions

Following a lengthy process reviewing the Copyright Act 1994, New Zealand's Ministry of Economic Development proposed a number of fairly minor legislative changes to incorporate the rapidly-changing digital environment while remaining essentially technology-neutral. Regarding ISP indirect liability for user copyright infringement, the Ministry appeared to be impressed by submissions emphasizing the cost of ISP monitoring of infringing activity, implying that the burden of enforcing copyright holders' rights is best vested in the holders rather than ISPs. Nevertheless, no blanket immunity for ISPs was proposed; instead, a knowledge-based standard similar to that adopted in the UK Electronic Commerce (EC Directive) Regulations 2002 was put forward, along with a constructive knowledge test and a requirement that in the knowledge of infringement, the ISP would be required to inform the relevant subscribers of their intention either to take down or block end-user access to the material concerned. No monitoring duties were proposed for ISPs, however, even though socially optimal monitoring may require them to make positive efforts in some circumstances.

The Ministry is correct in rejecting zero secondary liability for ISPs since gatekeepers may have an important and cost-effective role in controlling Internet copyright piracy. The rejection of strict ISP liability is also correct since web-hosting ISPs would otherwise remove an excessive amount of material from their servers, including legitimate material of high value. The main problem is that the interests of ISPs and users are not aligned, and an ISP focus on avoiding liability will typically harm the interests of users given the nature of the feasible contracts that can be written by the parties. This issue, however, received little attention in the Ministry's deliberations. Further, the uniform regulatory approach proposed by the Ministry leaves little room for distinguishing different severities of overdeterrence, and while the proposed knowledge-based standards should largely prevent excessive permanent removal of legitimate material, the constructive knowledge standard (which is weaker than adopted in Australia where ISPs receive limited protection) may be insufficient to encourage the removal of many infringing items. The knowledge test also leaves a degree of residual uncertainty as to when ISP liability is likely to arise. The counter-notification procedure may not prevent liability-conscious ISPs from removing excessive legitimate material on a temporary basis, causing significant losses to end-users in the process. More radical solutions that appear to have desirable efficiency properties, whereby ISPs would effectively buy their subscribers' posted material or where ISPs would be required to purchase copyrights and pursue infringers, did not feature in the proposals. Nevertheless, it is widely recognized that the design of optimal copyright law is fraught with difficulties and the Ministry's consultative processes and careful deliberations have done much to maintain a reasonable balance between the conflicting interests concerned.

References

Aplin, Tanya (2001), "Contemplating Australia's Digital Future: The Copyright Amendment (Digital Agenda) Act 2000," *European Intellectual Property Review,* 23(12); 565-75.

Armstrong, Jeffrey R. (2003), "Sony, Napster, and Aimster: An Analysis of Dissimilar Application of the Copyright Law to Similar Technologies," *DePaul-LCA Journal of Art and Entertainment Law,* Spring, 29; 1-10.

De Meza, David (1998), "Coase Theorem," in Peter Newman (ed.), *The New Palgrave Dictionary of Economics and the Law*, New York, Stockton Press; 270-82.

Gordon, Paul and Alan Woodfield (2001), "Negligence 'in the Air' and New Zealand's Health and Safety in Employment Act: a Law and Economics Analysis," University of Canterbury Department of Economics Discussion Paper No. 2001/02.

Hamdami, Assaf (2002), "Who's Liable for Cyberwrongs?," *Cornell Law Review,* May, 87; 901-56.

Hamdami, Assaf (2003), "Gatekeeper Liability," *Southern California Law Review,* 77; 53-121.

Klein, Benjamin, Anders V. Lerner and Kevin Murphy (2002), "Intellectual Property: Do We Need It? The Economics of Copyright 'Fair Use' in a Networked World," *American Economic Review,* 92(2); 206-08.

Kolstad, Charles D., Thomas S. Ulen and Gary V. Johnson (1990), "Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?," *American Economic Review,* 80(4); 880-901.

Landes, William M. and Richard A. Posner (1987), *The Economic Structure of Tort Law*, Cambridge, MA, Harvard University Press.

Landes, William, and Douglas Lichtman (2003), "Indirect Liability for Copyright Infringement: Napster and Beyond," *Journal of Economic Perspectives,* 17(2); 113-24.

Liebowitz, Stanley (2002), "Policing Pirates in the Networked Age," *Policy Analysis,* 438; 1-28.

Liebowitz, Stanley (2003), *Will MP3 Downloads Annihilate the Record Industry? The Evidence so Far,* Working paper, School of Management, University of Texas at Dallas.

Ministry of Economic Development (2001), *Digital Technology and the Copyright Act 1994: A Discussion Paper,* July 2001,Wellington.

Ministry of Economic Development (2002), *Digital Technology and the Copyright Act 1994: Position Paper*, December 2002,Wellington.

Ministry of Economic Development (2003a), *Digital Copyright Review: Policy Recommendations and Report Back on Submissions on Position Paper,* 2 April 2003,Wellington.

Ministry of Economic Development (2003b), *Statistics on Information Technology in New Zealand,* Information Technology Policy Group, Ministry of Economic Development, June 2003, Wellington.

Office of the Associate Minister of Commerce (2003), *Digital Technology and the Copyright Act 1994: Policy Recommendations,* June 2003,Wellington.

Park A.J. & Sons (1998), *Theft of Intellectual Property - Piracy and Counterfeiting,* Consultant's Report for the Ministry of Commerce, Wellington.

Polinsky, A. Mitchell and Steven Shavell (1979), "The Optimal Tradeoff Between the Probability and Magnitude of Fines," *American Economic Review,* 69(5); 880-91.

Riehl, Damien A. (2001), "Peer-to-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna?," *William Mitchell Law Review,* 27(3); 1761-95.

Rothschild, Michael and Joseph E. Stiglitz (1976), "Equilibrium in Competitive Insurance Markets: an Essay on the Economics of Imperfect Information," *Quarterly Journal of Economics,* 90(4); 630-49.

Shavell, Steven (1992), "Liability and the Incentive to Obtain Information About Risk," *Journal of Legal Studies,* 21(2); 259-70.

Shavell, Steven (1980), "Strict Liability versus Negligence," *Journal of Legal Studies,* 9(1); 1-25.

Wingfield, Nick and Ethan Smith (2003), "The High Cost of Sharing," *The Wall Street Journal,* September 9.

Yen, Alfred C. (2000), "Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment," *Georgetown Law Journal,* June, 88; 1833-94.

Alan E. Woodfield, Associate Professor of Economics, Department of Economics, University of Canterbury, New Zealand.