# ISP liability for copyright authorisation: the trial decision in *Roadshow Films v iiNet* Part Two

**This is the second and concluding part (the first part was published in the April 2010 edition of the Bulletin) of an exploration of the contours of copyright authorisation liability as that liability relates to a case involving the Australian internet service provider iiNet and thirty-four film and television companies. In this part the findings in Roadshow Films v iiNet will be described, together with a critique of certain aspects of the trial judgment.**

## The primary infringing activities

In *Roadshow Films v iiNet* the particular technology used for the primary infringing acts was peer-to-peer software coded to BitTorrent protocol.[1] Internet users armed with such software form a virtual network, and are able to copy file content from others in the network and, as a feature of the protocol, make the copied file content available to others in the network. That is to say the Internet users in the network who commence copying to their computer a file (which might encoded for a particular film) are contemporaneously obliged under the protocol to make available copied content to others in the network who desire that content. This forms an online gathering known as a 'swarm' of Internet users who are intent on securing (say) a copy of the same film title through a flurry of communal copying and communication. The applicants were concerned that such distribution of their content was occurring without their permission by persons using iiNet internet connections. Their action was brought against iiNet, the internet service provider (**ISP**), for authorising that distribution.

## The position of iiNet

The respondent iiNet sold internet access to its subscribers in volumes measured by gigabytes ('gigs'). The terms of that service provision conferred upon iiNet power to cancel a service for illegal or unusual use.[2] The applicants – while no doubt benefiting if illegal copyright infringement was curtailed by such contracts – were not privy to those contracts, and iiNet was perceived by the applicants to be uncooperative in working with them to curtail the activities of persons engaging in unauthorised BitTorrent distribution of the applicants' repertoire using iiNet subscriber accounts. The applicants were coordinated and organised by a peak body; the Australian Federation Against Copyright Theft (**AFACT**). Concern about those using iiNet subscriber accounts (**iiNet users**) arose from (i) AFACT being able to identify internet users in BitTorrent swarms by reference to unique internet protocol (**IP**) addresses allocated to iiNet subscribers, and (ii) the absence of any discernable policy or action by iiNet to deal with subscribers whose accounts were identified by AFACT as being used by infringers.

Evidence on iiNet's posture and attitude about the unauthorised distribution of the applicants' repertoire by those using iiNet services was obtained by two employees of AFACT who in mid-2008, as trap-evidence gatherers subscribed to iiNet, joined in BitTorrent swarms by connecting only with iiNet subscribers' accounts (identifiable by an iiNet-specific IP address prefix) and thereafter copied from those communicating in the swarm and communicated to those copying in the swarm the applicants' repertoire. Technical support was sought from iiNet by the AFACT employees and by this means further trap evidence was obtained of the type of advice iiNet provided to those who identified themselves as BitTorrent file-sharers. For example in mid-2008 one of the AFACT employees alerted iiNet that the movie *Kung Fu Panda* was slow to download and asked whether his uploading of other films was to blame. The answer provided by iiNet technical support was that uploads would only affect downloads minimally.[3]

## *The case resolved to three staggered legal issues*

AFACT also engaged a copyright piracy forensics firm operating out of Denmark, DtecNet Software APS, to collate data attributable (by IP addresses and a unique computer identifier) and pseudonymously identified iiNet subscribers' accounts being used to engage in unauthorised BitTorrent distribution of the applicants' repertoire. This was achieved by using deep packet inspection of the unique attributes of the data being transmitted, and being able to make a unique identification of iiNet users' computers transmitting on the relevant BitTorrent network. The DtecNet data, collected from June 2008 until August 2009, was forwarded weekly over 59 weeks to iiNet. The data gave notice of the date and time the alleged infringements of copyright took place; the IP address of iiNet subscribers used by the alleged infringers at the time of the infringements; the motion pictures and television shows in which copyright had been identified as being infringed; and the particular applicant controlling the rights

1 *Roadshow Films Pty Ltd v iiNet Limited (No. 3)* [2010] FCA 24, [56]-[77] (***Roadshow Films***). A good description of the protocol is found in David Lindsay, 'Liability of ISPS for End-User Copyright Infringements' (2010) 60 *Telecommunications Journal of Australia* 29.1, 29.2-29.3.

2 *Roadshow Films*, [99].

3 Affidavit of Aaron Guy Herps, filed in the proceedings on 15 December 2008, [28]. A contentious post-script to this trap-evidence gathering exercise was that once the identity of one of the trap-evidence gatherers became apparent to iiNet, iiNet reported that person to the Western Australian police for violation of the criminal provisions of the Copyright Act. The specific reporting of the trap-evidence gatherer was regarded by the trial judge as 'not intended to be taken seriously': *Roadshow Films* at [170]. This conclusion was surprising in view of the contents of the correspondence forwarded to the police (and not reproduced in the judgment) which included an analysis of the criminal liability of the trap-evidence gatherer written by the iiNet Chief Executive.

in the relevant motion pictures and television shows.[4] The information was capable of permitting attribution by iiNet of the particular subscriber accounts allocated to those implicated IP addresses at the nominated time. However, aside from on-forwarding the notices to the Western Australian police (discussed below) iiNet's conduct was consistent with what was found to be its unwritten policy on such matters; iiNet did not take any action in respect of those identified subscriber accounts.

## The reasons for decision at trial

As explained in Part One, in 2001 and 2004 two rounds of legislative reform to the *Copyright Act 1968* (Cth) (**Copyright Act**) produced: (i) a control-based codification of authorisation (sections 36(1A) and 101(1A)), (ii) an exception to authorisation liability for the providers of communications facilities arising from the facilities' mere use by others (sections 39B and 112E), and (iii) conditional limitations upon copyright remedies that can be awarded against carriage service providers (the Part V, Division 2AA safe-harbour regime). The proceedings initiated by the applicants claimed that iiNet had authorised the infringements of the AFACT employees, those iiNet subscribers in the BitTorrent swarms that the AFACT employees joined, and the iiNet subscribers identified in the notices by DtecNet. In defending itself iiNet argued that it had not authorised any exploitation of the applicants' copyright, but that if it was found to have so authorised, it could rely on the 'mere use of facilities' exception, or failing that, it could seek the protection of the limitation on remedies provided by the safe-harbour regime. The case thus resolved to three staggered legal issues.

### Authorisation liability

There were two important preliminaries to the authorisation analysis by the court. The first was whether any actual primary infringements had been proven to have occurred. The second was the nature of any such infringements in terms of the exclusive right structure of copyright.

#### *Trap evidence*

On the first issue, a contested matter was whether exploitations of copyright entailed in the trap-evidence gathering had been licensed by those represented by AFACT, and was thereby non-infringing. The trial judge found that it was, distinguishing the facts before the court from those in *Moorhouse* where a person 'at the behest' of a copyright owners' interest group gathered trap evidence by infringing the copyright of the plaintiff, Moorhouse.[5] In *Moorhouse* the High Court found that the plaintiff Moorhouse was oblivious to the infringing act at the relevant time.[6] In *Roadshow Films* the trial judge distinguished *Moorhouse* on the basis that the trap evidence gathering was done by individuals employed by AFACT (whereas the gatherer in *Moorhouse* was seemingly a volunteer) and that the plaintiffs in *Roadshow Films* had a higher degree of awareness of the gathering than the plaintiff in *Moorhouse*.[7] That finding, however, was not regarded by the court as being of 'real consequence' because the licensed trap evidence gathering provided evidence from which the court could infer other non-licensed actions.[8] More significantly, the trial judge considered that the DtecNet evidence supplied direct evidence of transmissions of the applicants' repertoire being made by users of iiNet internet access who were manifestly not licensed by the applicants.[9]

#### *Single or repeated exploitation of copyright?*

The second issue was the nature of those transmissions as an exploitation of copyright. The DtecNet data identified the iiNet users transmitting file data to a swarm, as distinct from iiNet users receiving file data as one of the swarm. How should that transmission be regarded as copyright exploitation? The trial judge applied the concept of communication to BitTorrent distribution as a singular making available and electronic transmission to the (collective) swarm, being members of the public.[10] This aspect of the court's characterisation of the rights exercise seems correct in itself.

***This characterisation as one (on-going) act of infringement as opposed to several acts of infringement (determined by a user's connection-disconnection-reconnection practices) is contestable***

More controversially such communication was regarded by the court as being made just once by an iiNet user, no matter on how many separate occasions particular subject matter was made available by a user during different internet sessions.[11] The court's approach rejected the applicants' argument that each time such a user disconnected and reconnected, and again distributed the same subject-matter to a differently constitute swarm, that the user separately communicated that subject matter to the public. This characterisation as one (on-going) act of infringement as opposed to several acts of infringement (determined by a user's connection-disconnection-reconnection practices) is contestable. In part the judge relied upon a provision in the Part VB educational copyright licensing scheme to support the analysis.[12] That provision deems there to be another act of communication to the public by an educational institution where subject matter is 'remains available online' for longer than 12 months. However it is reasonably clear that this provision would not have any application under the statutory licences if the educational institution chose for the material to not remain available online for a period of less than 12 months. The provision is directed to material left available on an educational institution's server continuously, year-in-year-out, for new student cohorts. To the extent that the provision had any analogous relevance to the facts here, it might be if an iiNet user's computer was left on and an iiNet internet connection open for a period of more than 12 months during which time an applicant's film copyright was continuously being made available via BitTorrent. In any event the judge's analysis minimizes the number of identified iiNet users who could be regarded as repeat infringers in respect of the one film title.[13]

---

4 *Roadshow Films*, [100]-[104].

5 *Moorhouse v University of New South Wales* (1974) 3 ALR 1, 14.

6 *University of New South Wales v Moorhouse* (1975) 133 CLR 1, 7-8.

7 *Roadshow Films*, [342]-[343].

8 *Roadshow Films*, [344]. Compare Merkel J's approach in *Ward Group v Brodie & Stone* (2005) 64 IPR 1, [51]: 'The reason, however, why trap purchases are not generally considered a consent to infringing use is that the infringing conduct is usually already occurring when the goods bearing the infringing mark are advertised or offered for sale to the public in the jurisdiction. In that situation the trap purchase is made to establish that fact, and cannot be seen to be a consent to the infringements that are occurring.'

9 *Roadshow Films*, [344].

10 *Roadshow Films*, [310].

11 *Roadshow Films*, [285]-[288].

12 Section 135ZWA(2A) in Part VB of the *Copyright Act*. (See also to like effect section 135JA(4).)

13 Relevant to section 116AH(1), item 1, condition 1 of the safe-harbour regime.

*The requirement for an authoriser to supply 'the actual means of infringement'*

Leaving aside those two preliminary points, twenty iiNet accounts (identified from the IP addresses listed in the AFACT notices) were considered in depth as a result of a preliminary order permitting detailed discovery in respect of a finite number of accounts. These were regarded by the court as providing the "most specific evidence of copyright infringement by iiNet users in these proceedings".[14] Had iiNet authorised those infringements which occurred using accounts after iiNet had received AFACT notices which enabled iiNet to identifying those accounts? In *Roadshow Films* the court's answer was: no. This answer was arrived at without recourse to the three codified factors which were explained in Part One. Instead, the following passage from Gibbs J judgment in *Moorhouse* was particularly relied upon by the trial judge:

> *It seems to me to follow from these statements of principle that a person who has under his control the means by which an infringement may be committed – such as a photocopying machine – and who makes it available to other persons knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorize any infringement which resulted from its use.*[15]

Working back from that application of principle to the facts in *Moorhouse*, in *Roadshow Films* the trial judge reasoned that there could be no act of authorisation unless iiNet actually provided the 'means' of infringement.[16] The broadband internet access supplied by iiNet was merely a 'precondition to infringement', and not the 'means'.[17] The 'means' was found to be the BitTorrent protocol itself.[18]

## *there were two relevant powers in iiNet that were said by the applicants to exist to prevent or avoid infringement: the first was to pass-on to subscribers warning notices, the second was to terminate the iiNet subscriber accounts*

The important aspect of the reasoning was that the trial judge's conclusion that iiNet did not authorise the infringement of the iiNet users' 'regardless' of the codified factors, and was solely on the basis of iiNet not supplying those users with the 'actual means' of infringement.[19] The mandatory nature of those factors is explained by the legislature as follows: "In determining ... whether or not a person has authorised the doing in Australia of any act comprised in the copyright ... *the matters that must be taken into account include the following*" [listing the three codified factors].[20] The court devised a threshold criterion by which 'to authorise' is defined to mean (and seemingly to only mean) to actually provide the 'means' of infringement. If it withstands appellate review, new judge-made law will be created which will be difficult to reconcile with the modern statutory language and modern authorities, and perhaps will substitute in place of that modern law a principle which loosely resembles pre-1911 law in which secondary liability arose only if one actually caused the infringement.[21] Lindsay summarises his similar view thus:

> *The great problem with the reasoning of the judge on this important point is that it reflects neither precedent nor the relevant provisions of the Copyright Act.*[22]

*Codified factors one and three: power to prevent and reasonable steps*

In line with a finding of no authorisation for failure by iiNet to supply 'the actual means of infringement', the consideration of the three mandatory factors was consigned in the trial judge's reasoning to obiter.[23] The first was the power in iiNet to prevent the infringing acts. In relation to the identified sample of twenty accounts identified from the AFACT notices, there were two relevant powers in iiNet that were said by the applicants to exist to prevent or avoid infringement, and seemingly if they were exercised by iiNet as a staggered response, that exercise would have averted the litigation. The first was to pass-on to subscribers warning notices once AFACT had provided iiNet with the DtecNet notices. The second was to terminate the iiNet subscriber accounts repeatedly being used for infringement notwithstanding the provision of warning notices. In relation to termination, the applicants pointed to the broad cancellation discretion that iiNet had conferred upon itself in its supply terms. In short, the policy that the applicants wanted iiNet to implement was to pass on warnings to an account holder identified by allocated IP address, and that if repeated infringement occurred by use of the account after the warnings, to terminate the account for a period of time. This is known commonly as 'graduated response'.

For those twenty accounts, the court found that iiNet had no power to prevent the doing of the infringing acts undertaken by those using the internet access supplied to those accounts. Introducing his 'power to prevent' analysis the trial judge referred to his earlier finding that:

> *There is a distinction between a precondition to infringement and the 'means' of infringement. Any number of persons may have control over whether a precondition exists, and therefore have the power to prevent the infringement by refusing to provide the precondition, but the Court does not believe that all such persons have the power to prevent the infringement relevant to a finding of authorisation.*[24]

Moreover when dealing with the 'power to prevent' statutory factor, the trial judge conflated the first and third mandatory factors to find that the only judicially recognisable power to prevent was a power that was reasonable to exercise in all the circumstances. As Lindsay points out, it is problematic to interpret a statutory provision which explicitly separates power to prevent from reasonable steps as if Parliament intended that the two be read together.[25] But having joined

---

14 *Roadshow Films*, [124].

15 *University of New South Wales v Moorhouse* (1975) 133 CLR 1, 13.

16 *Roadshow Films*, [382].

17 *Roadshow Films*, [400]-[401].

18 *Roadshow Films*, [402].

19 *Roadshow Films*, [415].

20 *Copyright Act 1968* (Cth), sections 36(1A) and 101(1A).

21 The pre-1911 law is discussed in Part One.

22 Lindsay, above note 1 at 29.9.

23 *Roadshow Films*, [416]: 'Nevertheless, as s 101(1A) is phrased as considerations that 'must' be considered, the Court is compelled to go into further consideration of the issue of authorisation pursuant to the considerations in s 101(1A)(a)-(c) of the Copyright Act.'

24 *Roadshow Films*, [417].

25 Lindsay, above note 1 at 29.11.

those two factors by placing a reasonableness gloss on the legislative text, the trial judge then separated the two aspects of the graduated response which the applicants submitted comprised a power to prevent; passing-on of warning notices leading to termination. By means of this separation, the trial judge considered each aspect of suggested conduct discretely rather than as an integrated whole, against an integrated legal standard (a reasonable to exercise power to prevent) that the trial judge had devised notwithstanding the statutory logic.

Under the court's approach, merely passing on warning notices, without more, was found not to prevent infringement because:

> *It may be readily assumed that merely passing on notices could hardly be a power to prevent infringement or a reasonable step without more, given that a person intent on infringing would quickly become aware that such warnings were ineffectual if termination of accounts did not follow ... That is, an ineffectual step is not a power to prevent infringement nor is it a reasonable step. ... That can hardly be a power to prevent infringement.*[26]

It is by no means clear that the trial judge's assumption is correct. It could be equally assumed that the receipt of such a notice in an iiNet subscriber household might have an immediate and permanent chilling effect upon propensity of iiNet users in the household to infringe the applicants' copyright by use of the BitTorrent protocol. However leaving to one side the correctness of this judicial assumption, the court then considered that account termination was not reasonable because:

- The broad contractual power in iiNet to cancel subscriber accounts was largely irrelevant because the applicants were not privy to the contract;
- Notwithstanding the DtecNet information, matters of copyright infringement were too difficult for iiNet to determine;
- The express conditioning of the safe-harbour regime upon iiNet adopting and reasonably implementing 'a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers' was not relevant;
- While iiNet could have cancelled an identified subscriber account and thereby stopped infringements continuing by iiNet users, it was not reasonable for iiNet to decide to do that without a court first determining that infringement had occurred;
- Termination would deny an iiNet user internet access for non-infringing purposes, and the evidence revealed that the identified accounts were not predominately used for infringing the applicants' repertoire.[27]

By considering graduated response in this segregated way but against an integrated legal standard, iiNet was found to have no reasonable power to prevent infringement. The trial judge's post script to the analysis was an echo from 1909.[28] Fault lay with the applicants for choosing the wrong respondent. The trial judge's observation was that iiNet:

> *does not stand in the way of the applicants pursuing those who have directly infringed their copyright nor in the way of the applicants pursuing any of the constituent parts of the BitTorrent system for authorisation.*[29]

*Codified factor two: nature of the relationship*

The nature of the relationship between iiNet and the primary infringers was also considered by way of obiter. The trial judge found that there was a direct contractual relationship between iiNet subscribers who infringed, and a more distant relationship between iiNet and non-subscribers who used iiNet internet access services to infringe – for example a member of the household of an iiNet subscriber. The nature of the relationship between a supplier and consumer of internet access in gigabytes (the file-sharing of audio-visual material is notoriously bandwidth intensive) did not lead to a finding that it was in iiNet's financial interest that its customers infringed copyright in the applicants' repertoire.[30] To support that analysis, the court observed that in respect of the 20 identified accounts from the AFACT notices 'only half of the subscribers moved up to a higher plan in the period examined, and one of those ten subsequently downgraded back to their original plan'.[31] However it is far from clear that such evidence supports the court's analysis, unless in that period (July 2008 to August 2009) the average plan-upgrade rate across all Australian household broadband subscribers was at 45-50% or higher. No such evidence was referred to by the trial judge.

## Fault lay with the applicants for choosing the wrong respondent

*Other factors: knowledge in, inducement by or other conduct of iiNet*

The consideration by way of obiter of how the three codified factors applied to iiNet's position led the court to reinforce its conclusion that no act of authorisation had occurred. Other arguments made by the applicants to claim iiNet's authorisation liability relied upon three main types of evidence.

First was evidence of specific knowledge in iiNet of infringement. The trial judge, based upon admissions by the iiNet Chief Executive under cross-examination, found that iiNet had (at least during the course of the litigation) been provided with sufficient information to have understandable notice of infringements arising by use of specific iiNet subscribers' accounts.[32] The court found however that such knowledge of infringement, even if coupled with the power to prevent such infringement, "is not, ipso facto, authorisation" in view of its earlier analysis.[33] It is this holding that will be a central issue of contention in any appeal. The applicants' case on authorisation is that any ISP has an obvious power to prevent infringing use undertaken using one of its subscriber's account, and that power is converted to authorisation of that use at least when the ISP has been given specific notice of ongoing infringing use, chooses to sit on its hands.

---

26 *Roadshow Films*, [433].

27 *Roadshow Films*, [425]-[436]. Also iiNet submitted that it was unlawful under the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) to terminate a subscribers account on the basis of the DtectNet information. This was said by iiNet to arise in so far as to terminate an account in reliance upon that DtectNet information would be to make use of information relating to the contents of communications carried by iiNet for a reason not authorised by the Telecommunications Act. This argument failed because of a defence in the Telecommunication Act that the trial judge considered would have applied had termination been effected in those circumstances. That defence excused employee conduct done in performance of duties as an employee. The trial judge considered that if an iiNet employee used the DtectNet information to terminate an account, this defence would have applied because of the contractual discretion in iiNet to terminate for illegal use: *Roadshow Films*, [508]-[532].

28 Part One, text associated with note 6.

29 *Roadshow Films*, [445].

30 *Roadshow Films*, [452].

31 *Roadshow Films*, [551] and [235].

32 *Roadshow Films*, [471].

33 *Roadshow Films*, [472].

Second, the applicants pointed to evidence of iiNet overtly inducing infringement. In particular an iiNet radio advertisement explained what a 'gig' was in these terms: "A gig is about 500 hi-res photos or about 300 songs or about 5 episodes of *The Golden Girls*".[34] *The Golden Girls* was a television program series that was not available for online distribution in any authorised form and comprised a title in the applicants' repertoire.[35]

When cross-examined on the selection of *The Golden Girls* example for the advertisement, the iiNet Chief Executive stated it "was a very unfortunate choice". It is difficult to avoid the conclusion that at the time of the advertisement iiNet was at least careless about whether or not its subscribers downloaded infringing material. Far from considering this an admission of indifference, the trial judge made these findings about the use of the advertisement:

> *The reference to Golden Girls was clearly intended to be humorous given its somewhat less than contemporary relevance. Indeed, the joke is that it is highly unlikely that someone would download an episode of the Golden Girls. It is not an invitation to download the Golden Girls. Rather, it is a tongue-in-cheek reference to a section of popular culture. The Court does not understand why [the iiNet Chief Executive] found it necessary to be so apologetic about the advertisement in his cross-examination.*[36]

It is perhaps surprising that the trial judge was able to objectively identify this intended humour. It seems clear enough that no humour was intended in the references to the 500 hi-res photos or 300 songs. Given this was a radio advertisement directed to 'non-technically minded people', objectively considered the advertisement might have been directed to a demographic that was expected by iiNet to have a positive preference for consuming *The Golden Girls*.

Third, there was the conduct of iiNet in forwarding the applicants' infringement notices to the Western Australian police. At the time of the initiation of the proceedings iiNet publicised in a November 2008 press release that the AFACT notices had been forwarded by iiNet to the police, and that AFACT had been advised by iiNet that "their complaints had been forwarded to law enforcement agencies and that they should follow the matter up with them".[37] The evidence of iiNet's general position – that copyright infringement undertaken by use of iiNet subscriber accounts was a police matter and not a matter to trouble iiNet with – was not dealt with substantively by the court.[38] For example, the above statement in the iiNet press release, and similar statements in iiNet correspondence to AFACT, was not included in the judgment. This is very surprising. A careful reader of the judgment would not discover that this on-forwarding of the notices to the police was central to iiNet's response to the notices.[39] The self-promoted conduct of iiNet in on-forwarding the notices seems on its face to go to issues such as: iiNet's belief in the credibility of the notices; iiNet's knowledge about the likelihood of infringement; whether the steps that iiNet took in on-forwarding the notices to the police and publicly promoting that conduct were reasonable steps to prevent or avoid infringement; and the relevance of the conduct to any existence of a repeat-infringer policy for safe-harbour purposes. Presumably any appellate court will be asked to reconsider this evidence.[40]

## *The submission of iiNet was that its unwritten posture – indifference unless subjected to court order – could amount to a qualifying policy for the regime is contrary to the object and purpose safe-harbour regime*

**Mere use of facilities provided authorisation exception**

Having established that there was no authorisation, the discussion of the 'mere use of facilities' exception was obiter. As explained in Part One, under a statutory authorisation exception the mere use of communications facilities provided by a defendant could not, without more, amount to authorisation.[41] However, and inconsistent with the trial judge's 'actual supply of means' theory of authorisation, the exception presupposes the existence of authorisation liability arises simply from the strong power that the provider of such facilities has to prevent resultant communications occurring over the network.[42] This inconsistency was explained away by the trial judge with the observation "it would appear that [the exception] provides protection when it is not needed".[43] That observation might be true if the trial judge's approach to authorisation liability were vindicated on final appeal. However, a more cogent explanation of the operation of the provision is found in the relevant Second Reading speech.[44] That explanation suggests that the trial judge's approach to authorisation liability at least is inconsistent with statutory purpose. Prior authority (more consistent with statutory purpose) of *KaZaa* and *Cooper* had established that actual knowledge or encouragement of the primary infringement took a defendant outside the protection of the provision.[45] That was because knowledge or encouragement

---

34 *Roadshow Films*, [480].

35 *Roadshow Films*, Transcript of proceedings, 2 November 2009, page 694.

36 *Roadshow Films*, [482].

37 The iiNet Media Release dated 20 November 2008 remains available at: http://www.iinet.net.au/press/releases/201108_iinet_to_defend_court_action.pdf

38 The sole, quixotic, reference in the judgment was "much of the applicants' submissions, particularly in criticism of the respondent's practice of forwarding the AFACT Notices to the police, are predicated on an assumption that the actions of the infringing iiNet users are not criminal actions": *Roadshow Films*, [352].

39 In emails to AFACT dated 25 July 2008, 12 August 2008, and 29 August 2008 (all in evidence) iiNet, (and consistent with its Press Release) stated and then reiterated the on-forwarding, providing the contact details of the relevant Western Australian police officer to whom iiNet had passed on the notices.

40 A ground of appeal is that the trial judge erred in 'failing to refer to and adopt relevant evidence before the Court': *Roadshow Films* Notice of Appeal filed 25 February 2010.

41 *Copyright Act 1968* (Cth), sections 39B and 112E.

42 *Cooper v Universal Music Australia Pty Ltd* [2006] FCAFC 187, [32].

43 *Roadshow Films*, [573].

44 Thus, and as explained in Part One, liability created by *Music on hold case* was dealt with via section 22(6). "Typically, the person responsible for determining the content of copyright material online would be a web site proprietor, not a carrier or Internet service provider. Under the amendments, therefore, carriers and Internet service providers will not be directly liable for communicating material to the public if they are not responsible for determining the content of the material": House of Representatives, Chamber Hansard, Copyright Amendment (Digital Agenda) Bill 1999 Second Reading Speech, Daryl Williams MP, 2 September 1999, 9750. Sections 39B and 112E dealt with the consequences for carriers and internet service providers of the codified authorisation liability under the three mandatory, control-based factors. 'The reforms provide that a carrier or Internet service provider will not be taken to have authorised an infringement of copyright merely through the provision of facilities on which the infringement occurs. Further, the bill provides an inclusive list of factors to assist in determining whether the authorisation of an infringement has occurred': ibid

45 *Roadshow Films*, [568]-[569].

meant that the authorisation arose from more than the mere use of the facilities that had been provided by the defendant. In *Roadshow Films* the trial judge had not found encouragement but had found specific knowledge of infringements in iiNet arising from the applicants' notices. As such the court, considered itself bound by that prior authority to find that the 'mere use of facilities' defence would not have been available to iiNet.[46]

**The safe-harbour limitation on remedies**

The final aspect of the trial judgment – also obiter in view of the earlier finding – was iiNet's eligibility for the limitation on remedies provided by the safe-harbour regime also explained in Part One. If liability had been found in iiNet, and if it qualified for the regime, its liability would have been confined to disabling access to offshore online locations and termination of specified customer accounts.[47] However qualification for the regime required that iiNet adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers.[48] What was iiNet's relevant policy? It had no written policy.[49] Presumably the conduct of on-forwarding the AFACT notices to the Western Australian police did not seem to reflect any relevant policy. Rather, the Chief Executive gave evidence that iiNet's posture was that if it was ordered by a court to terminate the account of an infringer, it would so terminate. But, absent a subscriber's admission of copyright infringement, it would not terminate an account without a court finding of infringement and a court order.[50] In other words, its policy was that it would not act in contempt of such a court order. As explained in Part One, the underlying public policy explanation of the safe-harbour regime is to protect ISPs from liability arising from their customers' infringing acts in a way which minimizes both the prevalence of those infringing acts and that imposes least litigation cost on all concerned. The submission of iiNet was that its unwritten posture – indifference unless subjected to court order – could amount to a qualifying policy for the regime is utterly contrary to the object and purpose safe-harbour regime. However, it was a submission which was wholly accepted by the trial judge, who found that on the basis of that unwritten posture iiNet had adopted and reasonably implemented a policy that terminated the accounts of repeat-infringers. This finding too will be likely to attract appellate court scrutiny.

## Concluding comments

The trial judge's decision in *Roadshow Films* has as its core the holding that to authorise the exercise of an exclusive right means to actually supply the 'means' by which the exercise occurs, as opposed to supplying a pre-condition necessary to exercise the right. As applied in the case, the provision of internet access by iiNet was found to merely supply the latter and could therefore never comprise an act of authorisation. Also central to the decision was the interpretation of this statutory language: "the matters that must be taken into account include the following". The court determines the non-existence of authorisation liability 'regardless' of the matters there set down. The control-based nature of the three codified factors, coupled with the existence of the authorisation defence for the mere use of communications facilities and the safe-harbour for transmission and connection services, all suggest a legislative intention that is contrary to the court's approach.

An important aspect of the applicants' case was that authorisation liability at least arose from the provision of notice of infringements. The exact position of the alleged authoriser, including its knowledge or indifference, has long had relevance in the assessment of authorisation liability. This is possibly related to the joint introduction (and often in the early cases the joint construction) of general authorisation liability and specific liability for knowingly permitting a venue to be used for an infringing performance.[51] In *Roadshow Films*, notwithstanding the lengths that the applicants went to provide notices, the finding was that knowledge of infringement, even if coupled with the power to prevent such infringement, "is not, ipso facto, authorisation".[52] This finding appears to be a far cry from modern authorities in which there has been a direct relationship of on-going control between the alleged authoriser and infringer.

***the finding was that knowledge of infringement, even if coupled with the power to prevent such infringement, "is not, ipso facto, authorisation"***

Appeal courts will likely reconsider the position of iiNet. If the core holding of the trial judge is upheld, it will create conditions for legislative intervention along lines that have occurred elsewhere. For example, the French have recently created a regulatory body known as HADOPI (the High Authority for the Dissemination of Works and the Protection of Rights on the Internet), which has taken relations between ISPs and copyright owners out of a cooperative scheme and into a regulatory one.[53] Similar is recent reforms in the UK. These are overseen by another regulatory body Ofcom. The new UK law requires ISPs to notify their subscribers if the IP addresses associated with those subscribers are reported by copyright owners, and to retain records on subscribers so reported in a form available to copyright owners through court order.[54] While industry cooperation is usually considered preferable to bureaucratic intervention, one of the paradoxes of the current court holding is that, if upheld, it will likely accelerate the Australian Parliament in regulating the copyright mores of ISPs.[55]

***David Brennan is an Associate Professor in the Faculty of Law at the University of Melbourne.***

---

46 *Roadshow Films*, [578].

47 As explained in Part One.

48 The public policy reasons for such a regime were explained in Part One.

49 '[The iiNet Chief executive] made clear that the detail of the policy does not exist other than in his mind': *Roadshow Films*, [614].

50 *Roadshow Films*, [614].

51 As explained in Part One.

52 *Roadshow Films*, [472].

53 See generally: Alexandre Entraygues, 'The HADOPI Law - New French Rules For Creation On The Internet' (2009) 20 *Entertainment Law Review* 264.

54 See generally: Ofcom, *Online Infringement of Copyright and the Digital Economy Act 2010 Draft Initial Obligations Code*, 28 May 2010 available at http://www.ofcom.org.uk/consult/condocs/copyright-infringement/condoc.pdf

55 On the choice between the 'private law' solution of inter-industry cooperation (effected through codes of conduct managing ISP authorisation liability) and the 'public law' solution of industry regulation (effected through a body such as the Australian Communication and Media Authority policing ISP handling of copyright notices) see the discussion by Andrew Wiseman and Matt Vitins, '"The means, baby" – ISP responsibility for copyright infringement and the need for an industry code of practice' (2010) 81 *Intellectual Property Forum* 13.