Attorney-General's Department and Department of Communications Submission in response to *Online Copyright Infringement Discussion Paper*

1 September 2014

Isabella Alexander
Associate Professor, Faculty of Law, University of Technology, Sydney

Robert Burrell
Professor, School of Law, University of Sheffield
Winthrop Professor of Law, University of Western Australia

Michael Handler
Associate Professor, Faculty of Law, University of New South Wales

Emily Hudson
Fellow, St Peter's College, University of Oxford
Senior Lecturer, TC Beirne School of Law, University of Queensland

Kimberlee Weatherall
Associate Professor, Sydney Law School, University of Sydney[*]

Executive Summary

This submission addresses specific legal issues relating to the three options proposed in the *Online Copyright Infringement Discussion Paper* ('Discussion Paper'): 'extended authorisation liability'; 'extended injunctive relief to block infringing overseas sites'; and the 'extended safe harbour scheme'. It does not seek to engage with the policies embodied in the Discussion Paper. We do not state a view on whether internet access providers 'ought' to 'do more' to address online copyright infringement. Rather, our focus is on the specifics of the three proposed options. However, in order to provide answers to Questions 1-7 in the Discussion Paper, our submission also addresses some broad concerns we have with the options presented that go to the prior questions of how and why the Australian government should adjust the existing rules in relation to liability and enforcement. Our submission has five substantive parts.

Part 2 Extended Authorisation *(page 4 and following)*

In this part we demonstrate that the attempt to 'extend' authorisation liability to address the problems identified in the Discussion Paper will not achieve the government's aims, and is likely to cause further confusion and unpredictable outcomes. The proposed amendments to the *Copyright Act* on page 4 of the Discussion Paper will not clarify the law. Rather, the amendments will only add a further layer of complexity to an already complicated area.

In large part this is because the scope of authorisation liability is determined not only by the current set of statutory factors but also by the law as developed by courts through individual cases. The highly fact-specific nature of the doctrine makes it difficult, if not impossible, to set clear, *ex ante* rules that specify the precise circumstances in which a party will be liable for authorisation. It is therefore not clear how changing the statutory factors would impact on the principles that the courts have developed through case law, or whether such a change would even lead to different outcomes from those reached in earlier cases. Recent legislative interventions in this area that have sought to 'clarify' the scope of authorisation liability have introduced only uncertainty and redundancy into the law. It is therefore not at all clear that the

[*] Our thanks go to Professor Tanya Aplin, Dickson Poon School of Law, King's College London, for her assistance, particularly with Part 4.

amendments would have the effect of ensuring that internet access providers are required to do more 'to discourage or reduce online copyright infringement'.

The proposed expansion could also have significant but unpredictable impacts on other third parties and intermediaries – online and off – that might be said to be in a position to take 'reasonable steps' to reduce copyright infringement.

Finally, insufficient thought has been given to the interaction of extended authorisation with the safe harbours, which could undermine the government's apparent goals.

Part 3 International Obligations *(page 16 and following)*

The Discussion Paper relies on misconceptions about the current state of Australia's international obligations relating to online copyright infringement. It cannot plausibly be maintained that the Australia-US Free Trade Agreement (AUSFTA), the Singapore-Australia or Korea-Australia Free Trade Agreements (SAFTA and KAFTA respectively) or the Japan-Australia Economic Partnership Agreement (JAEPA) require Australia to expand authorisation liability.

Part 4 Extended Injunctive Relief *(page 18 and following)*

In this part we suggest that in drafting any such provision careful attention needs to be paid not only to the wording of equivalent provisions in the UK and Europe but also to the broader context of these provisions and the case law which has developed under them. For instance, the European provisions operate in a particular legal context – one in which the provisions must be interpreted in a manner consistent with the *Enforcement Directive* (which requires that remedies shall be 'fair and equitable' and not, *inter alia*, 'unnecessarily complicated or costly'), the *European Convention on Human Rights*, and the *Charter of Fundamental Rights of the European Union* (which recognises rights to privacy and freedom of expression). Attention would need to be paid to whether Australian courts have the legal tools to balance appropriately the interests implicated by extended injunctive relief, and, if not, what this means for the drafting of any new provision. We discuss both principles which should limit the circumstances in which an injunction to block a website is available and the scope of any order, and a number of process issues that should be considered in drafting a legislative provision.

Part 5 Extended Safe Harbours *(page 23 and following)*

We support Proposal 3. The suggested reforms are both desirable and required in order to bring Australian law into compliance with its obligations under art 17.11.29 of AUSFTA.

Part 6 Answers to the Government's Questions *(page 24 and following)*

In light of the above points our answers to Questions 1–7 in the Discussion Paper are, in summary, as follows:

Question 3: Should the legislation provide further guidance on what would constitute 'reasonable steps'?

> Adding further detail into the list of statutory factors is unlikely to create additional certainty and may produce unforeseen consequences. There is therefore no need for further guidance in this regard.

Question 1: What could constitute 'reasonable steps' for ISPs to prevent or avoid copyright infringement?

> In light of our answer to Question 3 we would respond by saying that this question can only be answered by a court following a fact intensive inquiry. If greater *ex ante*

guidance is thought necessary this would point strongly towards the need for a more tailored scheme aimed specifically at ISPs.

Question 2: How should the costs of any 'reasonable steps' be shared between industry participants?

The expectation must be that costs fall on the party that needs to avoid a finding of legal liability, such that the costs of any 'reasonable steps' should logically be borne exclusively by the ISP. Admittedly there might be cases where a court might take account of an offer of financial assistance from a copyright owner when determining what steps were reasonable in the first place. This must, however, be the exception. If it is thought that copyright owners should be required to share a significant proportion of the costs in every case then this would also point towards the need for a more bespoke regulatory regime.

Question 4: Should different ISPs be able to adopt different 'reasonable steps' and, if so, what would be required within a legislative framework to accommodate this?

The fact intensive enquiry that characterises authorisation cases would inevitably produce this result. The very fact that this question has been posed may again suggest that the government's aims would be better achieved through a bespoke regulatory regime.

Question 5: What rights should consumers have in response to any scheme or 'reasonable steps' taken by ISPs or rights holders? Does the legislative framework need to provide for these rights?

Existing case law suggests that the impact on non-infringing uses is one factor that may influence whether liability for authorising infringement is made out. However, once such a finding has been made it is difficult to see what rights consumers could possibly have: it is difficult to see how individual consumers or representative organisations could be given standing to intervene so as to *enable authorisation of copyright infringement to continue*. Again, the mere fact that this question has been posed suggests that there is deep-seated confusion about the government's aims: the desire appears to be to create a regulatory regime that will weigh the interests of copyright owners, carriage service providers, other online service providers and consumers. Authorisation is a very poor vehicle for such a regime.

Question 6: What matters should the Court consider when determining whether to grant an injunction to block access to a particular website?

Given the potentially far-reaching effects of injunctions that block entire websites, we propose that the circumstances in which they are granted be limited to situations where: (1) the infringement is of a serious nature; and (2) legal action against those directly responsible for the infringement (the primary infringers) has been, or is likely to be, ineffective in halting that infringement because: (a) it is not reasonably practicable to institute legal proceedings against the primary infringers; or (b) it would be impossible to enforce any such judgment against them. We also suggest a number of due process issues that should be considered in drafting a legislative provision.

Question 7: Would the proposed definition adequately and appropriately expand the safe harbour scheme?

We are satisfied that the proposed definition is adequate.

Part 2: Why 'extended authorisation' will not achieve the government's aims, and is likely to cause only further uncertainty

Our first concern relates to the proposal to 'extend' authorisation liability through amending the factors a court must take into account in determining whether infringement by authorisation has occurred. We are concerned that:

(a) the problem the proposed legislative reform is intended to overcome is not clearly articulated in the Discussion Paper, nor is there a precise explanation of how the reform will seek to overcome that problem;

(b) the proposal seems to misunderstand the law of authorisation by failing to take sufficient account of the fact that the scope of authorisation liability is only partially determined by legislation. As such, it is not at all clear that the reforms will have their desired effect; instead, the reforms will only create further uncertainty;

(c) by attempting to reframe the test of authorisation so that it focuses almost entirely on 'reasonable steps', authorisation liability could be expanded in unpredictable and undesirable ways;

(d) the history of attempting to shape the law of authorisation through legislative reform has been problematic;

(e) the proposal gives insufficient attention to the way in which 'extended authorisation' would intersect with other provisions in the *Copyright Act*, in particular the safe harbour provisions, and that giving the safe harbours a greater role to play in the case of ISP liability might serve to undermine the government's intentions; and

(f) the proposal is ultimately premised on misconceptions as to how far authorisation liability can reach and how much of a role it can play in trying to incentivise more 'reasonable' conduct by particular industry participants.

A. What is 'extended authorisation liability' seeking to achieve?

Proposal 1 is intended to 'clarify the application of authorisation liability' by changing the factors in ss 36(1A) and 101(1A) of the *Copyright Act*. These provisions set out matters that must be taken into account by a court in determining whether a person has authorised copyright infringement. The proposed reforms appear to involve:

(1) removing 'the extent (if any) of the person's power to prevent' from its current position in the list of matters for each provision by repealing ss 36(1A)(a) and 101(1A)(a); and

(2) retaining the other two matters (the 'nature of the relationship' in ss 36(1A)(b) and 101(1A)(b), and 'whether the person took any reasonable steps to prevent or avoid' the infringement in ss 36(1A)(c) and 101(1A)(c)), but adding a new series of factors to which a court must have regard in making an assessment of reasonable steps, namely:

   (a) the extent (if any) of the person's power to prevent the doing of the act concerned;

   (b) whether the person or entity was complying with any relevant industry schemes or commercial arrangements entered into by relevant parties;

   (c) whether the person or entity complied with any prescribed measures in the *Copyright Regulations 1969;* and

(d) any other relevant factors.

According to the Discussion Paper, these reforms would 'clarify that the absence of a direct power to prevent a particular infringement would not, of itself, preclude a person from taking reasonable steps to prevent or avoid an infringing act' (Proposal 1, p 4).

Before explaining our concerns with Proposal 1 in detail, our preliminary worry is that the Discussion Paper provides very little detail on the exact purpose sought to be achieved, why the amendments will achieve that purpose, and why 'extended authorisation' rather than a different model of reform was chosen. We appreciate that authorisation is a highly controversial area of the law, particularly in its application to internet access providers whose subscribers might be engaging in infringement. We recognise that there have been long-standing and substantial disagreements between internet access providers, rights-owners and other stakeholders as to what can and should be done to minimise online copyright infringement.

But the specific 'problems' that supposedly need to be addressed are not self-evident; our concern is that these problems have not been articulated in the Discussion Paper with anything near the precision or detail needed to ensure full and robust debate on the merits of adopting particular reform proposals – particularly when those reform proposals are of general application (rather than, for example, applying specifically to internet access providers).

What follows, therefore, is our understanding of the government's concerns about the current state of the law and the outcomes it anticipates from its proposed reforms. In the Introduction to the Discussion Paper, the Attorney-General and the Minister for Communications, after stating that 'Internet Service Providers can take reasonable steps to ensure that their systems are not used to infringe copyright', say that the government wishes to 'provide a legal framework that facilitates industry co-operation' to deal with online copyright infringement. On p 1 of the Discussion Paper, it is stated that this proposed legal framework is one in 'which rights holders, ISPs and consumer representatives can develop flexible, fair and workable approaches to reducing online copyright infringement' and that it 'aims to provide certainty as to legal liability'. On p 3, in the context of authorisation liability specifically, the views are expressed that:

- the current factors in ss 36(1A) and 101(1A) 'are intended to create a legal incentive for service providers such as ISPs to take reasonable steps to prevent or avoid an infringement where they are in a position to do so';
- the High Court's decision in *Roadshow Films Pty Ltd v iiNet Ltd*[1] 'determined that iiNet was not liable for authorising the copyright infringements of its subscribers using systems that iiNet did not operate or control, and that there were no reasonable steps that could have been taken by iiNet to reduce its subscribers' infringements';
- the effect of the High Court's decision 'is to severely limit the circumstances in which an ISP can be found liable for authorising an act by a subscriber that infringes copyright'; and
- 'that even where an ISP does not have a direct power to prevent a person from doing a particular infringing act, there still may be reasonable steps that can be taken by the ISP to discourage or reduce online copyright infringement'.

Based on this, the conclusion is reached that '[e]xtending authorisation liability is essential to ensuring the existence of an effective legal framework that encourages industry cooperation and functions as originally intended'.

[1] (2012) 248 CLR 42 ('*Roadshow v iiNet*').

The Discussion Paper implicitly suggests that the key problem being addressed relates to one particular set of industry participants – internet access providers – and that these entities do not have sufficient legal incentives to take steps when confronted with allegations that their subscribers have engaged in copyright infringement, even though taking such steps might be classified as 'reasonable' (separately from how that term is used in the current law of authorisation). The Discussion Paper ties this problem to the presence in the *Copyright Act* of the requirement that courts consider the alleged authoriser's 'power to prevent' the direct infringements, and the High Court's finding in *Roadshow v iiNet* that iiNet lacked such a power because it did not control the system being used by its subscribers to infringe, and that there were no reasonable steps it could have taken to reduce its subscribers' infringements.

Although not made explicit in the Discussion Paper, it seems that the government's view is that in determining who should be responsible for enforcing rights online, the law has somehow shifted so as to favour ISPs unduly: there are references to *Roadshow v iiNet* having 'severely limit[ed]' the circumstances in which ISPs will be held liable for authorisation (implying that the circumstances were, or at least were thought to be, much broader before the High Court's decision), and to extended authorisation being needed to ensure a legal framework that 'functions as originally intended' (p 3).

To this end, it appears that the aim is to 'reverse' the outcome of *Roadshow v iiNet*, in the sense that if a case with identical facts were to be determined after the reforms became law, the ISP would be found liable for authorisation. This would be because the ISP's failure to pass on allegations of infringement by its subscribers (in circumstances where no relevant industry codes of practice are in place) would amount to a failure to take reasonable steps to prevent or avoid such infringements, notwithstanding the ISP's absence of a direct power to prevent such conduct. Put another way, it appears that the intention is to expand the reach of the law to 'clarify' that if an ISP acts as iiNet did immediately before it was sued in 2008, it will expose itself to liability.

This, in turn, appears intended to give ISPs a new incentive to take 'reasonable steps' when confronted with allegations of infringement, e.g. by entering into 'relevant industry schemes or commercial arrangements' with rights owners (with some detail provided on p 4 as to what these schemes should and should not involve). The addition of a further statutory factor that would go to 'reasonable steps', namely whether there was compliance with 'prescribed measures in the *Copyright Regulations 1969*', is explained by the suggestion that 'if effective industry schemes or commercial arrangements are not developed' (p 5) the government might seek to intervene, although no detail is provided in the Discussion Paper as to what 'prescribed measures' are contemplated. It is in this way that the proposed new legal framework seems to be designed to facilitate co-operation between industry stakeholders leading to 'flexible, fair and workable approaches to reducing online copyright infringement' (p 1).

Our analysis of 'expanded authorisation' is informed by our understanding of the government's goals in reforming the law. However, it is problematic that we should have to try to glean the government's intentions in the way we have – by piecing together various statements in the Discussion Paper. It is extremely difficult to assess the claim that the proposed reforms are 'essential' (p 3) when scant detail has been provided as to how and why the law is deficient and why 'extended authorisation' is the solution. Similarly, the government has stated repeatedly that its reforms will 'clarify' the law (p 4), but without any explanation of how and why such clarity will result.

B. The proposal appears to be based on a misunderstanding of the law of authorisation

Turning to the detail of Proposal 1, our main problem is that it appears to be based on a misunderstanding of the law of authorisation and, in particular, the role of the statutory factors and the reasoning in *Roadshow v iiNet*. In short, it appears that the government wants to use a threat of extended authorisation liability (of general application) to steer a particular group of parties – namely, ISPs – towards greater co-operation with rights holders in developing strategies to combat online copyright infringement. The problem is that there is no guarantee that changing the factors a court would be required to consider under ss 36(1A) and 101(1A) would in fact change the law of authorisation, and certainly not in such a way as to provide ISPs with any meaningful incentive to act differently and to seek to enter into co-operative arrangements with other industry stakeholders.

The Discussion Paper contains almost no engagement with the current law of authorisation, other than a brief mention of the factors in ss 36(1A)/101(1A) to which a court must have regard, and a passing (and unfortunately inaccurate) reference to the High Court's decision in *Roadshow v iiNet*. What is missing is a clear recognition of first principles. The overarching issue is that a party will be liable under ss 36(1) and 101(1) only if that party 'authorises' another's infringement. Determining whether a person has authorised infringement is a complex and highly fact-sensitive inquiry.[2] As can be seen in the judgments in *Roadshow v iiNet*, 'authorisation' is a concept that has been fleshed out since the early twentieth century by British Commonwealth courts, with judges articulating a range of factors that are relevant in determining whether a party's conduct amounts to authorisation of infringement by others.

It is well known that the statutory factors in ss 36(1A)/101(1A) were intended to be a partial codification of some of the factors that had been articulated in case law. In particular, factors (a) and (c) are closely based on statements made by Gibbs J in *University of New South Wales v Moorhouse*.[3] They were introduced at a time when, in light of decisions such as *Telstra Corporation Ltd v Australasian Performing Right Association Ltd*,[4] there was some uncertainty about the extent to which carriage service providers might be liable in relation to infringements carried out over facilities provided by them, and it was thought desirable to put some of those common law factors on a statutory footing.[5]

However, those statutory factors are not the end point of the inquiry in assessing whether authorisation has occurred. They must be taken into account, but the court is neither obliged to give any particular weight to any one factor, nor – crucially – is the court confined to these factors, the list in ss 36(1A)/101(1A) being inclusive. In answering the question of whether there is liability under ss 36(1) or 101(1), the court may therefore consider other factors. As the High Court noted in *Roadshow v iiNet*, 'the ultimate question of whether [the defendant] authorised the infringements will be an inference to be drawn from those facts'.[6]

Proposal 1 moves words around in the statute. However, the fact remains that a court would be required to address exactly the same question under the new regime as under the current law: did the defendant authorise infringement? The amendment does not *say* anything explicit to change the law, in that it does not say that a direct power to prevent infringement is *not* to be taken as precluding authorisation liability. Courts could therefore continue to take this matter

---

2 *Roadshow v iiNet* (2012) 248 CLR 42, 48 [5], 67 [63] (French CJ, Crennan and Kiefel JJ); see also *University of New South Wales v Moorhouse* (1975) 133 CLR 1, 12 (Gibbs J); *Performing Right Society Ltd v Ciryl Theatrical Syndicate Ltd* [1924] 1 KB 1, 9 (Bankes LJ); *Adelaide Corporation v Australasian Performing Right Association Ltd* (1928) 40 CLR 481, 504 (Gavan Duffy and Starke JJ).

3 (1975) 133 CLR 1, noted in *Roadshow v iiNet* (2012) 248 CLR 42, 54 [22] (French CJ, Crennan and Kiefel JJ).

4 (1997) 191 CLR 140.

5 See Explanatory Memorandum to the Digital Agenda Bill 1999 (Cth) part 1.1.

6 (2012) 248 CLR 42, 67 [63].

into account, along with any other matters identified in the case law, such as whether/what the defendant knew, and whether they actively encouraged or induced infringement.[7]

Proposal 1 is also premised on a second, fundamental misunderstanding of the law of authorisation: the idea that the absence of a direct power to prevent infringement precludes liability following *Roadshow v iiNet*. This is simply incorrect. The limited and indirect nature of iiNet's power to prevent infringement was certainly *one* relevant factor taken into account by the court.[8] But so was the failure of the copyright owners to provide detailed information backing up the allegations of infringement and the steps that the owners demanded that iiNet take. Both judgments emphasised that the notices served on iiNet did 'not provide iiNet with a reasonable basis for sending warning notices to individual customers containing threats to suspend or terminate those customers' accounts.'[9] The judges assumed (in the absence of any evidence to the contrary) that any warnings sent to subscribers would need to be backed up by enforcement (ie, termination) to be effective.[10] The judges were also concerned that given the lack of detail in the notices, termination of service would have required iiNet to undertake significant investigations of its own.[11] Finally, the judges noted that customers could take their business elsewhere, suggesting that ultimately the effectiveness of the proposed process was unclear.[12] In short, it was all of these facts, together, which led to a finding that iiNet was not liable for authorising infringement.

The misunderstanding reflected in the Discussion Paper may stem from a comment in the judgment of French CJ, Crennan and Kiefel JJ that '[a]n alleged authoriser must have a power to prevent the primary infringements'.[13] The judgment, however, does *not* state that any such power must be *direct*, and the rest of the judgment makes clear that an indirect power could be sufficient *in the context of other facts* supporting a finding of authorisation. This is consistent with other cases where courts have held entities liable for authorisation in the presence of only an indirect power to prevent infringement, like *Sharman*[14] or *Evans v E Hulton & Co Ltd*.[15] It is therefore incorrect to assert that *Roadshow v iiNet* has 'severely limited' the scope of ISPs' liability for authorisation, or that the decision has made the doctrine of authorisation function otherwise than 'originally intended'.

A final point which is often not appreciated when people discuss *Roadshow v iiNet* is that the copyright owners' own stance throughout the proceedings was that reasonable steps included

---

7 See, eg, *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 220 ALR 1 ('*Sharman*').

8 *Roadshow v iiNet* (2012) 248 CLR 42, 69 [70]–[71] (French CJ, Crennan and Kiefel JJ). See also Gummow and Hayne JJ at 90 [146], finding not that iiNet lacked any power to control customers' activities, but that it had power to control infringements 'only in an attenuated sense'. Gummow and Hayne JJ immediately go on to note that '[i]t was not unreasonable for iiNet to take the view that it need not act upon the incomplete allegations of primary infringements in the AFACT Notices without further investigation which it should not be required itself to undertake.'

9 *Roadshow v iiNet* (2012) 248 CLR 42, 71 [78] [2012] (French CJ, Crennan and Kiefel JJ).

10 *Roadshow v iiNet* (2012) 248 CLR 42, 69–70 [72] (French CJ, Crennan and Kiefel JJ).

11 *Roadshow v iiNet* (2012) 248 CLR 42, 70 [73]–[75] (French CJ, Crennan and Kiefel JJ).

12 *Roadshow v iiNet* (2012) 248 CLR 42, 88 [138]–[139] (Gummow and Hayne JJ).

13 *Roadshow v iiNet* (2012) 248 CLR 42, 69 [69] (French CJ, Crennan and Kiefel JJ).

14 (2005) 220 ALR 1.

15 [1923-28] MacG Cop Cas 51, 60, cited in *Roadshow v iiNet* (2012) 248 CLR 42, 83 [121] (Gummow and Hayne JJ). In *Evans* Tomlin J held that 'a man having a manuscript the copyright in which does not belong to him and in respect of which he has no authority to deal', but who 'sells to another some right in relation to it with a view to that other producing it', has authorised the ensuing production. See also *Falcon v Famous Players Film Co Ltd* [1926] 2 KB 474 at 491, in which the first three defendants made a film of the plaintiff's play in the US and imported their film into the UK. They agreed with the fourth defendant, a cinema proprietor, that he would show the film and they would share the box office receipts. It was held that the first three defendants authorised the performance by the fourth defendant. See the discussion in *Roadshow v iiNet* at 84–85 [126]–[127] (Gummow and Hayne JJ).

termination.[16] According to Roadshow, 'once iiNet had received credible information of past infringements sufficient to raise a reasonable suspicion that such acts of infringement were continuing, failure to enforce the terms of the CRA (through warnings, *suspension and termination*) amounted' to authorization.[17] In discussions in the High Court, AFACT/Roadshow et al suggested that the appropriate relief in the case would be an injunction which 'from a specified date restrained iiNet from continuing to provide internet services to each of the eleven specified customer accounts without obtaining confirmation from each respective account holder that each of the relevant films has been removed from the BitTorrent system on that account.'[18] Having put the case this way, focused on iiNet's power to prevent infringement through termination of service, and having brought proceedings before demonstrating the credibility of the notices of infringement, the movie and television companies that participated in *Roadshow v iiNet* can hardly complain, *ex post*, that the High Court should have ruled that iiNet was required simply to pass on notices if backed up by credible information known to be acquired through a rigorous process for identifying infringers.[19]

C. The proposed amendment will lead to unpredictable outcomes

We argued above that, given that (i) the underlying legal test is whether the defendant 'authorised' infringement and (ii) there is no proposal to change this test, a court would be entitled to reach identical outcomes under the 'expanded' authorisation regime as it would under the current law. However, it seems that the implicit intention is to downgrade the importance of a party's 'power to prevent' infringement, and to put greater emphasis on the relationship between infringer and alleged authoriser, and whether the alleged authoriser took 'any reasonable steps to prevent or avoid the infringing act'. If this is reflected in the legislative history (such as in an Explanatory Memorandum and the Parliamentary debates), with clear statements that the intention is to overrule both *Moorhouse* and *Roadshow v iiNet*, Australian courts might feel compelled to interpret the new form of 'authorisation' liability in such a way as to achieve that goal.

The effect of this change is unpredictable. An alleged authoriser's level of control over copyright infringement plays a complex, but important, role in the assessment of authorisation liability. In cases where the alleged authoriser has given a direct instruction or purported licence to perform an infringing act, or has expressly and unequivocally approved infringement *ex ante*,

---

16 AFACT in its original notices to iiNet demanded that iiNet '[p]revent the Identified iiNet Customers from continuing to infringe': *Roadshow v iiNet* (2012) 248 CLR 42, 57 [32] (French CJ, Crennan and Kiefel JJ), 75 [96] (Gummow and Hayne JJ). The case put in the Federal Court, and in the High Court, was that 'iiNet's technical and contractual relationship with its customers gave it the indirect power to control the use of its services – that is, to prevent continuing primary infringements (*through warnings, suspension of services and termination of contractual relations*)' (emphasis added): at 65 [58] (French CJ, Crennan and Kiefel JJ). As put by French CJ, Crennan and Kiefel JJ, 'the appellants' case on authorisation ultimately was that iiNet could not avoid secondary infringement unless it implemented a system designed to achieve the removal of infringing material by iiNet customers from the BitTorrent clients on those customers' computers': at 66 [59].

17 *Roadshow v iiNet* (2012) 248 CLR 42, 65 [58].

18 *Roadshow v iiNet* (2012) 248 CLR 42, 76 [99] (Gummow and Hayne JJ).

19 Cf Robert Burrell and Kimberlee Weatherall, 'Providing Services to Copyright Infringers: *Roadshow Films Pty Ltd v iiNet Ltd*' (2011) 33 *Sydney Law Review* 801, 814. In the High Court, AFACT/Roadshow et al did seek to argue that passing on notices would be a reasonable step, but insisted that it was not for AFACT/Roadshow to establish what reasonable steps ought to have been taken. AFACT/Roadshow et al's argument was that once *some kind* of reasonable step had been identified at a general level, *and* a general power to prevent infringement and relationship with the infringer were established, iiNet would be authorising infringement: in other words, iiNet could not 'stand by and do nothing' although the exact steps it should take were not for AFACT/Roadshow to specify: *Roadshow v iiNet* [2011] HCATrans 323 (30 November 2011). Reading the High Court transcript it is evident that both parties and court experienced difficulties in attempting to articulate what, exactly, it was anticipated iiNet should or could do, and what kind of order the court could grant to address the systemic issue of online infringement. This strongly suggests to us that authorisation is not an appropriate vehicle for addressing the problems of online infringement: see further Part 2(F) below.

the extent of a person's power to prevent infringement has not been particularly important.[20] In other cases, where authorisation is said to arise from the facilitation of infringement, say, by providing technology or means used by others to infringe, a person's power to control subsequent infringements has been central, both to holding defendants responsible in appropriate cases and also to limiting copyright law's interference with other legitimate businesses and with non-infringing activities. As Burrell and Weatherall have argued,

> *The central role of control in considering the defendant's 'power to prevent' infringement … makes sense as a matter of principle. The alleged authoriser's ongoing control enables it to prevent infringing activities, without restraining non-infringing activities. … Although the significance of this point is sometimes missed, it is important in ensuring that copyright law remains within its proper bounds, and does not prevent legitimate activities or hinder technological development. A focus on the defendant's power to prevent infringement untied to the capacity of the defendant to act to take steps to stop or reduce infringement without unduly harming legitimate activity runs the risk of stifling innovation, since many technologies have both legitimate and illegitimate uses.*[21]

It is difficult to predict the impact on business if authorisation were turned into a free-floating test turning entirely on whether a party could have taken 'reasonable steps' to reduce infringement. Taken at the extreme, the effect of the proposed amendment could be to turn the law of authorisation into a general duty, applicable to all businesses and all individuals, online and off, to take available and 'reasonable' steps to reduce infringement regardless of their involvement in the wrongful acts of copyright infringement.

It is hard to predict the scope of the claims that could be made under such a doctrine. Would libraries and art galleries be required to control use of mobile phone cameras by their patrons? Would companies selling electronic goods be asked to design those goods to limit copying? Would all businesses and all educational institutions be required to institute copyright training for all employees and students? Would libraries, councils, and cafes supplying Wi-Fi services need to limit their services or demand personal details from users? What reasonable steps would a courier or freight forward company be required to take to limit use of their services by infringing businesses and individuals? What additional steps would company directors and executives be required to take to ensure their businesses do not engage in copyright infringement? Would banks be required to take steps to ensure they do not fund companies that might engage in copyright infringement? No country of which we are aware would impose copyright liability so generally and with so little regard to the level of a party's involvement in the primary wrong of infringement.

D. Problems with seeking to bring about 'clarity' through legislative reform: lessons from recent copyright history

Recent history shows that the government should be cautious about attempting to 'clarify' authorisation through the type of legislative amendment being considered in Proposal 1. The 'Digital Agenda' amendments which introduced ss 36(1A)/101(1A) into the *Copyright Act* in 2001 were said to 'essentially codif[y] the principles in relation to authorisation that currently exist at common law (see in particular *University of New South Wales v Moorhouse* (1975) 133 CLR 1)'. Along with other amendments introduced at the same time, including ss 39B/112E, the amendments to authorisation were 'intended to provide a degree of legislative certainty about

[20] *Finn v Pugliese* (1918) 18 SR (NSW) 530, 541. For a recent example, see *EMI Songs Australia v Larrikin Music Publishing* (2011) 90 IPR 50, 107–11.

[21] Burrell and Weatherall, above n 19, 814.

liability.'[22] Experience over the last 13 years has demonstrated that these legislative amendments have been productive of constant, ongoing uncertainty.[23] Much angst has, for example, been expended on the meaning of the parenthetical '(if any)' in s 36(1A)(a).[24]

But the best example of the difficulties inherent in any attempt to 'clarify' authorisation through legislation lies in the history of ss 39B and 112E, also introduced in the 'Digital Agenda' amendments. The former provides:

> *A person (including a carrier or carriage service provider) who provides facilities for making, or facilitating the making of, a communication is not taken to have authorised any infringement of copyright in a work merely because another person uses the facilities so provided to do something the right to do which is included in the copyright.*[25]

Parliament's intention was that the sections would have the 'effect of expressly limiting the liability of carriers and carriage service providers for authorisations of copyright infringements on their networks'.[26] The Explanatory Memorandum stated that carriage service providers 'would benefit from the limitation on their liability for the authorisation of copyright breaches, and the resulting increased *certainty* in the industry about liability for copyright infringements on their facilities or network infrastructure' (emphasis added).[27] But why such an 'express limitation' was thought necessary was not made clear.

Courts and lawyers have struggled to give meaning to ss 39B and 112E. In *Roadshow v iiNet*, French CJ, Crennan and Kiefel J[28] considered that these provisions implemented the agreed statement concerning art 8 of the WIPO Copyright Treaty,[29] namely that '[i]t is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention'. In *Sharman*, Wilcox J noted an argument by the applicant copyright owners that, in introducing s 112E, the Parliament recognised that the amendments to authorisation expanded liability, such that merely providing facilities *could* make a party liable but for the presence of that defence.[30] Justice Wilcox also thought that the effect of s 112E might be to overturn the High Court decision in *Telstra v APRA.*[31] Still other commentators have argued that ss 39B and 112E were redundant, in that mere provision of facilities could never ground liability.[32]

Thus the statutory provision intended to clarify the law became a bone of contention in litigation in ways which, if anything, muddied the waters. Ultimately, commentators arguing for redundancy proved correct, with all High Court judges in *Roadshow v iiNet* holding that s 112E

---

22 Explanatory Memorandum to the Digital Agenda Bill 1999 (Cth) [56].

23 David Lindsay, 'Internet Intermediary Liability: A Comparative Analysis in the Context of the Digital Agenda Reforms' (2006) 24 *Copyright Reporter* 70, 77.

24 Rebecca Giblin, 'The Uncertainties, Baby: Hidden Perils of Australia's Authorisation Law' (2009) 20 *Australian Intellectual Property Journal* 148, 158–62 and cases discussed therein.

25 Section 112E is in similar terms, but deals with Part IV subject matter.

26 Explanatory Memorandum to the Digital Agenda Bill 1999 (Cth) [59].

27 Explanatory Memorandum to the Digital Agenda Bill 1999 (Cth) part 4.2.2.

28 *Roadshow v iiNet* (2012) 248 CLR 42, 55 [24].

29 Art 8 provides that 'authors ... shall enjoy the exclusive right of authorizing any communication to the public of their works'.

30 *Sharman* (2005) 220 ALR 1, 89 [361]; contrast this to the arguments of the respondents in the case, at 95 [390] ff.

31 *Telstra Corporation Ltd v Australasian Performing Right Association Ltd* (1997) 191 CLR 140; see *Sharman* (2005) 220 ALR 1, 96–7 [396]–[399].

32 See, eg, Jill McKeough, Andrew Stewart and Philip Griffith, *Intellectual Property in Australia* (3rd ed, 2004) 237; Lionel Docker, 'The Ghost of *Moorhouse*' (2002) 7 *Media and Arts Law Review* 113; Lindsay, above n 23.

'seems to have been enacted from an abundance of caution … it is difficult to see how the activity it describes, without more, could amount to authorisation'.[33]

A court could treat the Proposal 1 amendments in the same way. Notwithstanding the government's stated intention to 'expand' authorisation, as we have argued above, there is nothing in the *text* of the proposal that would prevent courts reaching identical outcomes to the present.

In addition, part (b) of the proposed list of factors to which a court would have regard in assessing 'reasonable steps' seems to create as much scope for uncertainty and overreaching arguments as ss 39B/112E and ss 36(1A)/101(1A) have provided since 2000. Proposal 1 suggests that in determining whether 'reasonable steps' have been taken a court should have regard to:

> *whether the person or entity was complying with any relevant industry schemes or commercial arrangements entered into by relevant parties.*

There is endless room for argument about whether a given commercial arrangement has been entered between 'relevant parties' and it is not at all clear how a court is meant to interpret such a concept. What makes a party or commercial arrangement 'relevant'? If one school reaches a deal with one set of copyright owners about steps to be taken to combat infringement, is that 'arrangement' automatically relevant for all schools? Or only schools with equivalent resources or equivalent problems of infringement? Is it 'relevant' for universities, since they are also educational establishments? Can we be confident that a court will have all the relevant facts to assess the relevance of an arrangement if it is entered into by entities not party to the litigation, especially if aspects are confidential? While general industry codes or practices might be relevant, it is very hard for us to see how particular commercial arrangements between particular parties should set or even influence the legal treatment of completely separate parties.

This is not to say that this is an area of the law in which legislative intervention is always inappropriate. For instance, the introduction of ss 39A and 104B in the wake of *Moorhouse* has been successful in providing comfort to libraries, in providing that if they take certain steps in relation to their copying equipment, they will not be taken to have authorised any infringement committed by users of that equipment simply because of the provision of that equipment. Those amendments have worked because they spell out in detail the exact steps a party must take to avoid infringement. Proposal 1 in the Discussion Paper is the exact opposite – it attempts to expand liability, using general, imprecise language. It will not afford a potentially affected party any certainty as to what it must do to avoid liability.

E. The interaction between extended authorisation liability and other provisions in the Copyright Act must be considered

Proposal 1 singles out one piece of the complex statutory puzzle that governs ISP liability in copyright, and fails to consider how the amendments to ss 36 and 101 would interact with the other provisions. In our view, the fact that no thought has been given to the ongoing role, if any, that ss 39B and 112E might play is a problem, but a far greater issue is the relationship between extended authorisation liability and the statutory 'safe harbours' in Part V Div 2AA. Later in the Discussion Paper, Proposal 3 suggests expanding the safe harbours, which are currently limited to 'carriage service providers', to all 'service providers' carrying out the specified acts. As

[33] *Roadshow v iiNet* (2012) 248 CLR 42, 81 [113] (Gummow and Hayne JJ). See also at 55-6 [26] (French CJ, Kiefel and Crennan JJ).

discussed below, we think this is entirely sensible and would finally ensure that the safe harbours operate as intended in light of the AUSFTA. But we think insufficient attention has been paid to the way the safe harbours could undermine the government's intentions for extended authorisation.

The safe harbours in Part V Div 2AA shelter ISPs[34] that provide network access[35] from monetary remedies,[36] provided the ISP complies with the conditions set out in s116AH:

(a) the ISP must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers;

(b) the ISP must comply with any industry code relating to standard technical measures used to protect and identify copyright materials;

(c) any transmission of copyright material must be initiated by or at the direction of a person other than the ISP; and

(d) the ISP must not make substantive modifications to copyright material transmitted.

The safe harbours shield ISPs from liability for both direct infringement and infringement by authorisation. Assuming that we are dealing with the same facts as in *Roadshow v iiNet*, if Proposal 1 increases an ISP's risk of authorisation liability in such circumstances, this potentially gives the safe harbour provisions a greater role to play than at present. For example, assuming that no 'relevant industry schemes or commercial arrangements' exist, an ISP will not be able to know whether any steps that it has taken are sufficient for it to avoid a finding of authorisation, meaning that it might well seek to shore up its position by complying with the safe harbours. And even if such 'relevant industry schemes or commercial arrangements' were to be developed, an ISP is still likely to look to the safe harbours, given the uncertainty of the reach of the new 'expanded' authorisation doctrine in the absence of court decisions.

However, a major complication is that in order to rely on the safe harbour, the ultimate penalty the ISP has to be prepared to impose for repeat infringement *must* be termination of service.[37] This sits very uncomfortably alongside the government's stated expectation in the Discussion Paper that whatever schemes are worked out between industry stakeholders should *not* 'impose … any measures that would interrupt a subscriber's internet access' (p 4).

To explain why this is a problem, our starting point is that what an ISP would need to do to rely on the safe harbours is unclear. The intention when the safe harbours were created was that ISPs should determine the contours of their own policy on termination. The Explanatory Memorandum that accompanied the *US Free Trade Agreement Implementation Act 2004* (Cth) stated that '[t]his policy is to be determined by the carriage service provider'[38] (in contrast with the notice-and-takedown regime, which is governed by detailed regulations[39]). This is

---

[34] Strictly, the safe harbours are currently limited to carriage service providers: ISPs are carriage service providers entitled to rely on the safe harbours. Proposal 3, discussed below, would extend this to all service providers engaged in the relevant functions.

[35] *Copyright Act 1968* (Cth) s 116AC. Other activities are also protected, namely caching, hosting third party content, and providing information location (ie, search) services: ss 116AD–116AF.

[36] Other orders can be made, as set out in 116AG. In the case of an ISP carrying out Category A activities, the available orders are (a) an order requiring the CSP to take reasonable steps to disable access to an online location outside Australia; and (b) an order requiring the carriage service provider to terminate a specified account: s 116AG(3).

[37] *Copyright Act 1968* (Cth) s 116AH(1), item 1.1.

[38] Explanatory Memorandum to the US Free Trade Agreement Implementation Bill 2004 (Cth) 161 [699].

[39] *Copyright Regulations 1969* (Cth) Part 3A. The specificity of the notice and takedown regime, compared to the brevity of the obligation to have a 'policy' for termination 'in appropriate circumstances,' suggests the legislature

consistent with the US approach.[40] American service providers have tended to adopt very broad, general policies regarding repeat infringers, and US courts have left details to service providers, on the basis that Congress intended 'to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined.'[41] A US service provider is not required to communicate ahead of time who would count as a repeat infringer, or exactly when termination will occur: in fact, not doing so recognises the reality that circumstances can vary greatly, as can the seriousness of infringement.[42] Only in rare cases have US courts denied safe harbour protection to service providers that failed to terminate relationships in the face of blatant infringement, and none of these cases relate to ISPs.[43]

The Full Federal Court in *Roadshow v iiNet*[44] took a different approach when considering the safe harbours. In that case, iiNet argued that if the court were to find it liable for authorising infringement, it could take advantage of the safe harbour, arguing that its policy was to terminate the accounts of repeat infringers in three circumstances: (1) when ordered to do so by a court; (2) when a customer admitted to infringing copyright, or (3) when a customer was found by a court or other authority to have infringed.

All three judges rejected iiNet's argument. The judgments raised two substantive criticisms of iiNet's policy. The first was that it was insufficiently specific: that it failed to identify who would be treated as a 'repeat infringer' and the circumstances in which termination would occur.[45] Second, a majority held that the policy failed to provide for termination in some circumstances where it would be appropriate: namely, where iiNet was aware of knowing, repeated infringements by customers on a commercial scale.[46]

We believe that in taking it upon themselves to establish minimum requirements for an appropriate policy, the Full Federal Court undermined the differentiated protections the legislature intended to establish through Part V Div 2AA of the *Copyright Act* for different online service providers. Unfortunately, this aspect of the Full Federal Court's decision was not appealed to the High Court and it is important to emphasise that, given the Full Federal Court's finding on authorisation, its discussion of the safe harbours was *obiter dicta*.

For present purposes, the important point is that, *either way*, the safe harbours in Part V Div 2AA could easily undermine the government's intentions for Proposal 1. The government's stated preference in the Discussion Paper is for increased enforcement online, via a process that is negotiated with copyright owners, which provides due process for users, and which does not

---

was ready and able to prescribe detail where appropriate. It deliberately decided not to include proscriptive standards for CSPs' termination policies.

40 Under the equivalent US provision 17 USC §512. Section 512 is the source of art 17.11.29 of AUSFTA.

41 *Corbis Corp v Amazon.com, Inc*, 351 F Supp 2d 1090, 1101 (WD Wash 2004); see also *UMG Recordings, Inc v Veoh Networks, Inc*, 665 F Supp 2d 1099 (CD Cal 2009).

42 *Corbis Corp v Amazon.com, Inc*, 351 F Supp 2d 1090, 1101 (WD Wash 2004).

43 *Perfect 10, Inc v CCBill LLC* 481 F 3d 751, 760 (9th Cir 2007), in which the 9th Circuit held that 'an internet service provider who receives repeat notices that substantially comply with the [legislative requirements] about one of its clients, but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy'. *CCBill*, however, and other cases which adopt similar reasoning, involve Category C (hosting) conduct, which is very different from situations involving ISPs acting as mere conduits. The reasoning in *CCBill* proceeds on the basis that the alleged infringements are publicly available (for example, on a website), that detailed notices from the copyright owner asserting infringement on penalty of perjury have been sent in accordance with the notice and takedown regime (17 USC §512(c)(3)), and that the user or subscriber has been made aware of, and had the opportunity to respond to, the allegation of infringement (17 USC §512(g)(2)). To similar effect see *Perfect 10, Inc v Cybernet Ventures*, 213 F Supp 2d 1146, 1176 (CD Cal 2002).

44 (2011) 194 FCR 285.

45 See in particular at (2011) 194 FCR 285, 405 [520] (Jagot J) and 464-5 [805] (Nicholas J).

46 See in particular at (2011) 194 FCR 285, 345 [264] (Emmett J) and 465 [806] (Nicholas J). Justice Jagot did not consider what features would be necessary in an acceptable policy. Instead, she relied on her view that iiNet had not, as a matter of fact, adopted any policy: at 405 [520]–[521].

result in termination of internet service. On the US interpretation of the safe harbours, where ISPs set their own repeat infringer policy, iiNet's policy could pass muster,[47] thereby giving a strong incentive to ISPs not to take the 'reasonable steps' under the expanded authorisation regime and instead seek to rely on the safe harbour. This would likely frustrate the government's overarching goal of increasing enforcement. Following the Full Federal Court's approach in *Roadshow v iiNet*, the ISP determines the details of its policy for terminating repeat infringers and need not negotiate with rights holders, meaning there is still an incentive to rely on the safe harbour. But the legislation requires termination as a penalty and the Full Federal Court's *obiter* statements seem to require that termination be a reasonably prominent part of that policy. Since the court showed a willingness to reject policies deemed insufficiently stringent, the tendency *could* be for cautious ISPs to adopt *overly* stringent policies, with over-use of the penalty of termination of service.[48]

The termination condition in the safe harbour cannot simply be removed: it is a mandatory provision of AUSFTA. Article 17.11.29 of AUSFTA is unequivocal on this point.[49] Short of re-negotiating this part of AUSFTA with the US,[50] Australia is obliged to have safe harbours covering ISPs, and is required to condition those safe harbours on having a policy including termination. This strongly suggests that insofar as the government's goal is to increase enforcement of online infringement but *without* termination, amending the law of authorisation in such a way as to give the safe harbours a greater role to play is not the appropriate mechanism.

F. Authorisation is not the right vehicle to achieve the stated policy goals

In *Roadshow v iiNet* French CJ, Crennan and Kiefel JJ stated:

> *the concept and the principles of the statutory tort of authorisation of copyright infringement are not readily suited to enforcing the rights of copyright owners in respect of widespread infringements occasioned by peer-to-peer file sharing, as occurs with the BitTorrent system. The difficulties of enforcement which such infringements pose for copyright owners have been addressed elsewhere, in constitutional settings different from our own, by specially targeted legislative schemes, some of which incorporate co-operative industry protocols, some of which require judicial involvement in the termination of internet accounts, and some of which provide for the sharing of enforcement costs between ISPs and copyright owners.*[51]

---

47 This follows from the reasoning from *CCBill*, discussed above n 43, where it was held that while a service provider could *choose* to adopt a more stringent process of its own volition, termination is only *required by law* following a process, involving notice to the user, so as to establish knowing, repeated or blatant infringement: *Perfect 10, Inc v CCBill LLC*, 481 F 3d 751 (9th Cir 2007). It is hard to see how this could apply to a Category A provider. Evidence in *Roadshow v iiNet* suggests that copyright infringement notices in general could not be relied on to provide reliable information.

48 Since any internal policy adopted by ISPs will necessarily have some internal costs, it may be that concessions by copyright owners on the question of costs (eg, offering to bear some proportion of the costs) could change this dynamic.

49 Article 17.11.29 states that '…each Party shall provide, consistent with the framework specified in this Article…(b) limitations in its law regarding the scope of remedies available against service providers for copyright infringements that they do not control, initiate, or direct, and that take place through systems or networks controlled or operated by them or on their behalf, as set forth in this sub-paragraph'. Under art 17.11.29(b)(vi), '[e]ligibility for the limitations in this sub-paragraph shall be conditioned on the service provider … adopting and reasonably implementing a policy that provides for termination in appropriate circumstances of the accounts of repeat infringers'.

50 Renegotiation might be possible on this point: AUSFTA is now a decade old, and the voluntary industry scheme which has recently started operating in the US does not include termination as a penalty.

51 *Roadshow v iiNet* (2012) 248 CLR 42, 71 [79].

What is most telling about this recognition of the limitations of the law of authorisation in the context of 'enforcing the rights of copyright owners in respect of widespread infringements occasioned by peer-to-peer file sharing' is that the judges did *not* call for the law of authorisation to be reformed. To the extent that a concern can be detected in this statement that more could be done to address 'widespread infringements' online, it is notable that the judges referred to 'specially targeted legislative schemes' overseas.[52]

We would suggest that if the government's goal is to address the specific situation of internet access providers who are not actively inducing or otherwise taking active steps to facilitate or promote infringement, the proposed indirect approach of tinkering with the generally applicable statutory factors a court is required to take into account in determining authorisation liability is not a productive way forward. The better option would be to leave authorisation liability as is and to seek to achieve that goal directly, for example by way of separate standalone provisions.

Part 3: Australia's international obligations do not require this change

Even if it is accepted that 'expanded authorisation' is entirely uncertain in application and is highly unlikely to lead to the outcomes hoped for by the government, there is the question of whether Australia needs to amend its law of authorisation to ensure compliance with obligations under various trade agreements. The Discussion Paper states that '[e]xtending authorisation liability is essential to ensuring the existence of an effective legal framework that … is consistent with Australia's international obligations' (p 3), the strong implication being that the current law is not currently compliant. We take this to be a suggestion that the AUSFTA, the Singapore-Australia Free Trade Agreement (SAFTA), and, if ratified, the Korea-Australia Free Trade Agreement (KAFTA) and/or the Japan-Australia Economic Partnership Agreement (JAEPA) require reversal of the High Court's decision in *Roadshow v iiNet*. This aligns with the view recently expressed by the Department of Foreign Affairs and Trade.[53]

The idea that Australian law is inconsistent with our international obligations and needs to be reformed for this reason is plainly incorrect.

As Mihaly Ficsor (formerly Deputy Director General of WIPO in charge of copyright and related rights) noted long ago, in general, questions relating to liability are very complex; for the most part therefore, 'international treaties on intellectual property rights [including the WIPO Copyright Treaty of 1996] understandably and rightly, do not cover such issues of liability.'[54] No obligation, therefore, to impose liability on ISPs could arise from Australia's multilateral treaty obligations. If there were such an obligation, it would have to come from AUSFTA.

---

[52] See also above n 19, noting the difficulties the High Court and counsel encountered attempting to shape the doctrine of authorisation to address a systemic issue involving many potential interested parties.

[53] Hansard, House of Representatives (Treaties Committee), 5 August 2014, 18 (representative of DFAT stating 'all three of these agreements [AUSFTA, SAFTA and KAFTA] require Australia to provide a legal incentive for cooperation between ISPs and copyright owners. Currently that is given effect through sections 36 and 101 of the Copyright Act. As has been discussed in this committee, the decision in *Roadshow v iiNet* cast some doubt on the effectiveness of those provisions in giving effect to that obligation. The position that we have taken now is that we think it would be prudent to make some amendments to those provisions to make sure that they operate effectively to create that legal incentive.')

[54] Mihaly Ficsor, 'Copyright for the Digital Era: The WIPO "Internet" Treaties' (1997) 21 *Columbia-VLA Journal of Law and the Arts* 197, 214.

The relevant obligation in AUSFTA art 17.11.29 (which is titled '*limitations* on liability for service providers'[55]) states that:

> *Consistent with Article 41 of the TRIPS Agreement, for the purposes of providing enforcement procedures that permit effective action against any act of copyright infringement covered under this Chapter, including expeditious remedies to prevent infringements and criminal and civil remedies, each Party shall provide, consistent with the framework specified in this Article:*
>
> *(a) legal incentives for service providers to cooperate with copyright owners in deterring the unauthorised storage and transmission of copyrighted materials; and*
>
> *(b) limitations in its law regarding the scope of remedies available against service providers for copyright infringements that they do not control, initiate, or direct, and that take place through systems or networks controlled or operated by them or on their behalf, as set forth in this subparagraph.*

AUSFTA art 17.11.29(a) is a high level obligation referring to service providers generally. It does not require specific 'incentives' for specific types of service provider. The better interpretation is that Australia fulfils its obligations under art 17.11.29(a) by ensuring that service providers that have significant involvement in copyright infringement (that is, the ones who would be liable under current copyright law) risk liability.

Even assuming, for the sake of argument, that art 17.11.29(a) requires Australia to have legal incentives *specifically* for ISPs, Australian law meets that minimal requirement. As outlined extensively in Part 2 of this submission, ISPs do not have a general exemption from liability. *Roadshow v iiNet* stands for the proposition that authorisation liability is a highly fact-specific inquiry and that, in the circumstances of that case, iiNet was not required to take action to pass on warnings and ensure (through termination of service and other means) that the specified repeat infringers identified in the proceedings ceased their infringements.[56]

Nor is art 17.11.29(a) specific as to the kind of legal incentives or cooperation required. Copyright infringement can be deterred in a number of ways, including through direct infringement actions brought against individual infringers. Australian law requires service providers to cooperate with legal processes that copyright owners might seek to bring against individual infringers through the mechanism of preliminary discovery.[57] The fact that the form of cooperation required or incentivised by Australian law is not rights holders' currently preferred form of cooperation does not on any view put Australia in breach of international treaty obligations.

It is also inconceivable that AUSFTA requires ISPs in Australia to be subjected to a higher risk of liability than those in the US. In no case has a general purpose ISP been sued or held liable for use of BitTorrent or file-sharing by its users in the US. Given the state of US law, it is impossible to imagine iiNet being held liable for copyright infringement under identical facts.

Nor do more recent free trade agreements change this position. KAFTA art 13.9.28 provides:

> *Each Party shall provide measures to curtail repeated copyright infringement and related right infringement on the Internet*.

---

55 Our emphasis.

56 Notably, in another case, an ISP which was more actively involved in infringement *was* held liable for authorising copyright infringement: *Cooper v Universal Music Australia Pty Ltd* (2006) 156 FCR 380.

57 *Federal Court Rules 2011* (Cth) r 7.22.

Like AUSFTA art 17.11.29(a), this is a high level obligation to provide 'measures'. Australia has many such 'measures', including:

- Procedures to enable copyright owners to enforce their copyright against direct infringers (including repeat infringers) and including the potential for additional damages against flagrant infringers;[58]
- A provision to facilitate proof of harm in online copyright actions;[59]
- Criminal provisions that can be applied against online infringers lacking a commercial motivation;[60] and
- Liability for authorisation of copyright infringement, with the cases showing that liability will be readily imposed on providers of software and websites which are designed to facilitate widespread infringement.[61]

Once again, the fact that Australian law does not include 'measures' currently preferred by copyright owners does not put Australia in breach of its international obligations. If an obligation on ISPs to pass on notices or discipline customers was intended, this could have been specifically included in the text.

JAEPA art 16.16 provides:

> *Each Party shall take appropriate measures to limit the liability of, or remedies available against, Internet service providers for copyright infringement by the users of their online services or facilities, where the Internet service providers take action to prevent access to the materials infringing copyright in accordance with the laws and regulations of the Party.*

This is a truncated provision relating mostly to safe harbours (the focus of the provision is on limitations on liability). Two points may be made about this provision. First, it relates to 'internet service providers' generally, and not just 'internet access providers' (which we tend, in Australia, to call ISPs). As used in international IP law, 'internet service providers' includes search engines, web hosts, online auction sites, online stores, and others who are providing services in an online environment. It is the equivalent of 'online service providers' in AUSFTA. Thus, as with the KAFTA provision, as long as there are measures in place relating to online service providers (and as long as there are limitations on liability) Australia will comply with art 16.16. Second, the provision defers to domestic law: that is, internet service providers need only 'prevent access … *in accordance with the laws and regulations of the Party*'. This is not a specific obligation to require internet access providers to limit access to infringing material. Any obligations to limit access are a matter for domestic legislators to determine.

Part 4: Extended Injunctive Relief

Proposal 2 in the Discussion Paper is to legislate for 'extended injunctive relief' in relation to websites operating outside Australia. This proposal would 'enable rights holders to apply to a court for an order against ISPs to block access to an internet site operated outside Australia, the dominant purpose of which is to infringe copyright. Rights holders would be required to meet any reasonable costs associated with an ISP giving effect to an order and to indemnify the ISP against any damages claimed by a third party' (p 6). Proposal 2 seems

58 *Copyright Act 1968* (Cth) s 115(4).
59 *Copyright Act 1968* (Cth) s 115(5)–(6).
60 *Copyright Act 1968* (Cth) s 132AC.
61 *Sharman* (2005) 220 ALR 1; *Cooper v Universal Music Australia Pty Ltd* (2006) 156 FCR 380.

to have been inspired by European initiatives such as art 8(3) of the *Information Society Directive*[62] and s 97A of the *Copyright, Designs and Patents Act 1988* (UK) ('CDPA').

The government asks one question in relation to this aspect of its Discussion Paper: 'what matters should the Court consider when determining whether to grant an injunction to block access to a particular website?' In responding to this question, we have concentrated on the principles that ought to frame the operation of extended injunctive relief. In taking this starting point we are clearly open to the proposition that Australia amend the *Copyright Act* to introduce a provision with similar effect to the European initiatives. However, there must be adequate checks and balances to ensure that any such provision is not misused. In that respect we have a number of concerns about the scope and wording of the provision suggested in Discussion Paper.

In cases like *Roadshow v iiNet*, rights holders have sought to deal with infringing content appearing on file-sharing and other websites not by instituting proceedings against those who operate or use those websites, but by suing ISPs on the basis that, by providing the platforms on which infringing content is distributed and accessed, they have authorised infringement. However, another way to deal with *iiNet*-style facts is that found in the government's second proposal: to permit enforcement processes which do not rest on the ISP *itself* being liable for infringement, but which require it to take some action in relation to infringing content, such as blocking websites.

As presented in the Discussion Paper, Proposals 1 and 2 appear to be cumulative: that the *Copyright Act* be amended to expand the circumstances in which an ISP is liable for infringement by authorisation *and* the circumstances in which it can be ordered to block content. One might ask whether such dual reform tips the scales too far in one direction. As discussed above, we are strongly of the view that the government should leave authorisation as it is.[63] However, we are open to the position that the *Copyright Act* be amended to permit extended injunctive relief, so long as any new provision contains limits to reflect the extraordinary circumstances in which a blocking order is appropriate.

In this section we have considered some of the key principles that ought to govern the operation of extended injunctive relief. In doing so we have drawn heavily from the now extensive body of EU (and UK) case law to consider art 8(3) of the *Information Society Directive*, s 97A of the CDPA and similar provisions in other EU member states.

A. There is a serious case of infringement that cannot be stopped through legal action against those directly responsible

Given the potentially far-reaching effects of injunctions that block entire websites, we propose that the circumstances in which they are granted be limited to situations where:

(1) the infringement is of a serious nature; and

---

[62] That is, *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society* [2001] OJ L167/10. Article 8(3) provides: 'Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.' Note, too, recital 59 of the same instrument, which recognises that 'In the digital environment…the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end.'

[63] Our analysis on this aspect is set out in detail in Parts 2 and 3.

(2) legal action against those directly responsible for the infringement (*the primary infringers*) has been, or is likely to be, ineffective in halting that infringement because:
   (a) it is not reasonably practicable to institute legal proceedings against the primary infringers; or
   (b) it would be impossible to enforce any judgment against them.

The proposal in the Discussion Paper is that extended injunctive relief only be available in the case of internet sites operated outside Australia. Clearly, this is one situation in which direct action against those responsible may not be possible, but it may be desirable to express this in a more targeted way – for example, by requiring evidence of reasonable attempts to identify the hosts of the website and, if they are identifiable, to contact or (if reasonable) bring proceedings against them. This would ensure that the provisions do not become a legal shortcut to avoid expensive legal proceedings: for example, in the case of large, well-established websites which do, for example, respond to copyright owners' takedown notices.[64]

Careful consideration will have to be given to drafting the threshold to which infringement would need to rise in order to justify the blocking of a website. Our view is that a combination of confining the measures to serious infringement, *coupled with* a requirement that any order does not impact adversely on access to lawful content (discussed below), will *together* ensure such orders remain appropriately confined. We note that in the US, proposed legislative provisions have required that a blocked site 'has no significant use other than engaging in, enabling, or facilitating the… reproduction, distribution, or public performance of copyrighted works, in complete or substantially complete form, in a manner that constitutes [criminal] copyright infringement'.[65]

B. The order does not impact adversely on the ability of users to distribute and gain access to lawful content, and ensures that their personal data remains protected

An obvious risk with blocking orders is that they may be over-inclusive and prevent legitimate forms of access. The guiding principle that legitimate forms of access not be curtailed may be relevant at a number of points, most obviously: (1) when identifying the website(s) to be blocked; and (2) when considering how ISPs are to comply with the order.

For instance, in the European context, recent decisions by the CJEU have emphasised that when ISPs adopt measures to comply with injunctions, they must respect the fundamental rights of internet users to impart and receive information.[66] This right may be affected if the blocking measures employed are not able to distinguish adequately between lawful and unlawful content, and block the former.[67] The measures taken must therefore be strictly targeted so that

---

[64] We note that when website blocking was proposed as one element of the *Stop Online Piracy Act* HR 3261 (112th Congress) ('*SOPA*') in the US, one early criticism was that it gave no protection to websites that were in full compliance with notice-and-takedown processes under the *Digital Millennium Copyright Act* or equivalent overseas legislation.

[65] This drafting comes from the *Protect IP Act* S 968 §2(7) (112th Congress) (definition of 'Internet site dedicated to infringing activities'). An alternative draft piece of legislation, *SOPA*, was criticised and eventually rejected for its much broader drafting, which would have applied where the site was committing or facilitating the commission of criminal copyright infringement. Since criminal copyright infringement can arise where a single infringing copy is made or distributed for profit, this was not sufficiently limited to the really serious, 'worst of the worst' sites intended to be targeted.

[66] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* (C-314/12) [2014] ECDR 12, [55] ('*Telekabel*').

[67] *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (C–360/10) [2012] 2 CMLR 18, [48]-[50] ('*SABAM v Netlog*').

they bring to end any infringing activities by third parties but in a way which does not affect other users who are using the ISP's services to lawfully access information. In order to prevent the latter from occurring, the CJEU has stated that rules must be put in place to allow users to assert their rights before the court once it is aware of the implementing measures to be put in place.[68]

In relation to user privacy, the CJEU has also warned against injunctions requiring filtering systems which involve identification, analysis and processing of information connected with profiles on social networks, as being an infringement of the right to protection of personal data.[69]

In UK cases relating to orders under s 97A, the Court has considered whether such orders are appropriate and proportionate, bearing in mind the need to balance property rights and the fundamental rights of individuals. Orders which are 'narrow and targeted' have been found to be proportionate.[70]

C. The order does not impact adversely on the ability of ISPs and other entities to run a business

In addition to having a potentially adverse impact on the rights of internet users, blocking orders have the potential to impact on ISPs and other economic agents. The CJEU has therefore emphasised the importance of ensuring that, in the course of protecting property rights, injunctions do not impact adversely on the freedom of ISPs to conduct a business. The Court has suggested this freedom extends to the right of a business to use its available economic, technical and financial resources, within the limits of liability for its own acts.[71]

In *SABAM v Netlog*, for example, the injunction was found to amount to a serious infringement of the freedom of the ISP in question to conduct its business because it required it to install a complicated, costly, permanent computer system at its own expense.[72] This would also be in breach of art 3(1) of the *Enforcement Directive*,[73] which provides that *inter alia* 'measures, procedures and remedies [for the enforcement of the intellectual property rights as required by the Directive] *shall be fair and equitable and shall not be unnecessarily complicated or costly*, or entail unreasonable time-limits or unwarranted delays' (emphasis added). Likewise, the cost of implementing measures has been a factor considered by UK courts in deciding whether the orders in question are proportionate.[74]

D. Steps are taken to protect natural justice and procedural fairness

Consideration needs to be given to the nature of any proceeding, the parties likely to be in court, and the kind of evidence that may be put before the court. Since ISPs may not have incentives to ensure the due process rights of those who operate websites, some protections will need to be built into the court process. Important issues include:

---

68 *Telekabel* [2014] ECDR 12, [56]-[57].

69 *SABAM v Netlog* [2012] 2 CMLR 18, [47]-[51]; *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (C-70/10) [2011] ECR I-11959, [51].

70 *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch), [107].

71 *Telekabel* [2014] ECDR 12, [49]; *SABAM v Netlog* [2012] 2 CMLR 18, [39]-[44].

72 *SABAM v Netlog NV* [2012] 2 CMLR 18, [46].

73 *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights* [2004] OJ L157/45.

74 *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch), [102], [107]; *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch), [200].

- Is the proceeding going to be *ex parte*? If so, special obligations need to be placed on the party seeking the order, including an obligation of full disclosure to the court of matters that may not assist the applicant's case, much as with applications for Anton Piller (search) orders.
- How many websites can be notified in one proceeding? It is vital to ensure that the court will have adequate time to consider the application fully as regards all the websites listed in the proceeding.[75]
- Will orders be time-limited or open-ended (that is, will they allow addresses to be added, and if so, using what process)?
- Will the court be entitled to make orders by consent without a hearing, and if so, will those orders be published and readily available to the public? We would be concerned if it became impossible to determine, through consultation of relevant published judgments, the number and nature of websites actually being blocked in Australia.

In order to ensure that right holders have proper incentives to take care in identifying relevant websites, it may be worthwhile considering whether some (perhaps pre-established) penalty should apply should websites or website addresses be incorrectly listed or blocked.

E. The order gives the ISP discretion to determine the particular technological measures that it will adopt by way of compliance

In the March 2014 *Telekabel* judgment, the CJEU confirmed that blocking orders need not specify the particular measures to be taken in order to block access, leaving ISPs under an obligation to take 'all reasonable measures' to prevent unauthorised access by users, provided these measures do not unnecessarily deprive individuals of their fundamental rights.[76] It approved the form of the injunction in question which did not specify the measures that an ISP must take. This was found to comply with EU law as it allowed the ISP to determine the specific measures to be put in place in a way which allowed it to tailor the measures to the resources and abilities available to it and was compatible with the other obligations and challenges which it would encounter (ie, the rights of users). Further, the Court was in favour of an injunction which would allow an ISP to avoid incurring coercive measures for breach of that injunction if it could show it had taken all reasonable steps to comply. The Court observed that 'the possibility of exoneration clearly has the effect that the addressee of the injunction will not be required to make unbearable sacrifices.'[77]

In contrast, as mentioned above, in *SABAM v Netlog* the injunction issued by the national court was found to be precluded by European law because it required it to install a filtering system which was expensive, complicated, indiscriminate and not limited in time.[78]

---

[75] We would be concerned, for example, if lists of hundreds of sites were presented to the court for urgent blocking, as has occurred in India: see for example *Multi Screen Media Pvt Ltd v Sunit Singh et al*, CS(OS) 1860/2014 (23 June 2014), in which a list of 472 sites was presented to the court for blocking. It seems unlikely that the court had time to consider all 472 sites fully, an inference supported by the fact that the list was later revised down to 219 sites in an order made in July 2014.

[76] *Telekabel* [2014] ECDR 12, [64]. Similar discretion can be seen in later drafts of the US proposals cited above n 64–65 after earlier drafts were criticised for their specificity.

[77] [2014] ECDR 12, [52]-[53].

[78] *SABAM v Netlog* [2012] 2 CMLR 18, [46].

F. Any provision should be subject to a sunset clause to ensure that, as a minimum, this issue is thoroughly revisited in light of evidence of how extended injunctive relief is working in Australia and in other jurisdictions

As yet the evidence as to how extended injunctive relief is working in other jurisdictions is unclear. Since the first such order was granted in the UK in 2010 in the *Newzbin* litigation,[79] the number of applications and the speed at which they have been processed seems to have increased.[80] This has been welcomed by the content industries which see the remedy as an effective means by which to stem the flow of infringing content.[81] It is too early to say whether they might become subject to abuse, although the observation that ISPs in the UK are no longer seeking to resist s 97A injunctions does raise red flags for those concerned with procedural fairness and possible misuse.

Conversely, although ISP blocking orders appear to be somewhat effective at present, this may be because the majority of internet users are unable to circumvent blocks on access. However, technically-capable users can already employ methods in order to circumvent restrictions and some of these methods are simple enough that less technically-capable users may well be able to pick them up over time. It is therefore clear that any new provision that allows for extended injunctive relief should be reviewed in something like 5 years after its introduction. The best way to ensure a full and comprehensive review is to make any new provision subject to an express time limit.[82]

Part 5: Extended safe harbours

Proposal 3 is a long-overdue reform that will finally bring Australian law into compliance with its obligations under art 17.11.29 of AUSFTA.

Under AUSFTA, Australia is required to provide 'limitations in its law regarding the scope of remedies available against service providers for copyright infringements that they do not control, initiate, or direct, and that take place through systems or networks controlled or operated by them or on their behalf, as set forth' in art 17.11.29(b). Limitations are required to preclude monetary relief for service providers in relation to 'the following functions', listed in art 17.11.29(b)(i)(A)–(D). The relevant functions include caching, remote storage (web hosting) and the provision of information location tools (ie search). These are functions provided by a wide range of entities, but Australia's safe harbours, in Part V Div 2AA, are limited to 'carriage service providers'. This 'extremely complex term',[83] interpretation of which 'takes us on a merry chase through the provisions of' the *Telecommunications Act 1997* (Cth), in essence limits the safe harbours to 'phone companies'.[84] This gives rise to a ridiculous situation where actual

---

79 *Twentieth Century Fox Film Corporation and others v Newzbin Ltd* [2010] EWHC 608 (Ch).

80 See TorrentFreak, *UK Piracy Blocklist Expands with YIFY, Primewire, Vodly and Others* (November 22, 2013), available at http://torrentfreak.com/uk-piracy-blocklist-expands-with-yify-primewire-vodly-and-others-131122/.

81 'Website blocking measures implemented by ISPs have been effective. Between January 2012 and July 2013, European countries where blocking orders are in place saw BitTorrent use decline by 11 per cent, while European countries without such orders saw BitTorrent use increase by 15 per cent (comScore/Nielsen). The effect was especially pronounced in two countries, Italy and the UK, where the highest number of illegal services have been blocked': *IFPI Digital Music Report 2014: Lighting Up New Markets* (2014) 41, available at http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf.

82 The *Copyright Act 1968* (Cth) is already littered with enforcement provisions that are not used, such as, for example, the Infringement Notice provisions. A fixed expiry date would avoid this problem.

83 Lindsay, above n 23, 80.

84 Jane Ginsburg and Sam Ricketson, 'Separating Sony Sheep from Grokster (and Kazaa) Goats: Reckoning Future Business Plans of Copyright-dependent Technology Entrepreneurs' (2008) 19 *Australian Intellectual Property Journal* 10, 29–30.

search engines, and actual web hosts, cannot take advantage of safe harbours designed and intended to protect them from liability.

As David Lindsay noted back in 2006, limiting Part V Div 2AA this way was 'clearly a mistake'.[85] The error and the anomalies to which it gives rise has been recognized multiple times, including in a 2005 Issues Paper from the Attorney-General's Department,[86] and by the Department of Broadband, Communications and the Digital Economy in 2009.[87] Jane Ginsburg and Sam Ricketson in 2008 recognised that it would appear to put Australia in contravention of AUSFTA:

> *It … appears that Div 2 is narrower in its coverage than the equivalent provisions in the DMCA and, indeed, is narrower than the obligations contained in the AUSFTA.*[88]

Ricketson and Ginsburg concluded that 'clearly, the category of persons and entities who are to be entitled to the remedial safe harbours needs to be revisited and extended'.[89]

Limiting the safe harbours this way has also put Australian law out of step with other jurisdictions. The safe harbours enacted in the US under the *Online Copyright Liability Limitation Act 1998*, which are the model for the provisions in AUSFTA, apply to 'service providers', a term defined very broadly in the legislation.[90] Similar safe harbours in European law are available to 'information society service providers', a definition that clearly extends to ecommerce sites, web hosts, search tools, and others.[91] Similar protections in Canadian law are similarly broadly granted.[92] As the Discussion Paper states, the issue should be function, not the nature of the entity involved.

In short, Proposal 3 is not only desirable, it is necessary and long-overdue.

Part 6: Direct answers to the questions posed

In this final section we set out our answers to Questions 1-7 of the Discussion Paper, building on the analysis set out in Parts 2-5.

Question 1: What could constitute 'reasonable steps' for ISPs to prevent or avoid copyright infringement?

Answer: The logically prior inquiry is dealt with in question 3 of the Discussion Paper. As will be seen from our response to that question, we conclude that it would be unwise to provide

---

85 Lindsay, above n 23, 81.

86 Attorney-General's Department, *Part V Division 2AA of the Copyright Act 1968 Limitation on Remedies Available Against Carriage Service Providers: Does the Scheme Need to be Expanded?* (Issues Paper) (August 2005).

87 Department of Broadband, Communications and the Digital Economy, *Australia's Digital Economy: Future Directions* (2009) 21.

88 Ginsburg and Ricketson, above n 84, 31 (our emphasis). See also at 37.

89 Ibid, 40.

90 17 USC §512(k)(1)(A) and (B). The legislation has two definitions, one for 'mere conduits' (that is, under Australian law, one which is offering services falling into Category A) which requires that the service provider be an 'entity offering transmission, routing, or providing connections for digital online communications, between or among points specified by a user, without modification to the content'. The broader definition, applying to the other categories of activities, designates a service provider as 'a provider of online services or network access or the operator of facilities thereof'.

91 An 'information society service providers' is a person who provides 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of the recipient of a service': Directive 98/34/EC (as amended by Directive 98/48/EC), art 1(2).

92 See in particular *Copyright Act* (RSC, 1985, c C-42) (Canada) s 41.27.

further legislative guidance as to what constitutes reasonable steps in the context of authorisation liability. Further guidance can, in our view, only sensibly be provided by the courts. There is nothing to be gained in the context of this review in setting out our view as to how the courts might usefully develop the law of authorisation as regards ISPs or any other class of potential defendant.

We also note that the way this question has been framed, namely, 'what could constitute "reasonable steps" for ISPs' goes to the heart of one of our concerns with the Government's suggested approach. Amendments to the general law of authorisation will have implications in both digital and analogue environments. If the aim is to deal with the specific question of the obligation of ISPs to help block access to material that infringes copyright it would make sense to deal with this question through a bespoke regulatory regime, not through amendments to the general law of authorisation.

Question 2: How should the costs of any 'reasonable steps' be shared between industry participants?

Answer: The mere fact that this question has been asked also suggests that there is a mismatch between the Government's apparent aims and the legislative amendments that are being proposed. The Government's appears to want to create a scheme that allows for a balancing of interests between different stakeholders: copyright owners, carriage service providers, other online service providers and consumers.

Authorisation is simply not the right vehicle to create such a scheme: it is a highly fact dependent enquiry that rests on an established body of case law and extends to a huge range of different scenarios. However, it has ultimately been aimed at parties that have 'done the wrong thing': defendants that have encouraged or at least facilitated copyright infringement. This context would surely suggest that compliance costs should fall on the party that needs to avoid a finding of legal liability, such that the costs of any 'reasonable steps' should logically be borne exclusively by the ISP. Admittedly there might be cases where a court might take account of an offer of financial assistance from a copyright owner when determining what steps were reasonable in the first place, a point touched on in the *iiNet* litigation. Any cost sharing regime would, however, have to be the exception.

If it is thought that copyright owners should be required to share a significant proportion of the costs in every case then this would also point towards the need for a more carefully tailored regime.

Question 3: Should the legislation provide further guidance on what would constitute 'reasonable steps'?

Answer: It is important here to avoid the fallacy of thinking that adding more and more detail into copyright legislation will create additional certainty. Ultimately an assessment of 'reasonableness' must rest on a fact dependent enquiry. Creating a long list of factors that go to the question of reasonableness is unlikely to make litigation outcomes more predictable. On the contrary, the more factors that are identified, the more likely it is in any given case that the parties will be able to point to some factors that go one way, some the other. There is therefore no need for further guidance in this regard to this question.

Question 4: Should different ISPs be able to adopt different 'reasonable steps' and, if so, what would be required within a legislative framework to accommodate this?

Answer: The fact intensive enquiry that characterises authorisation cases and determinations of reasonableness more generally would inevitably produce this result. Again, the very fact that this question has been posed suggests that the Government's aims would be better achieved through a bespoke regulatory regime.

Question 5: What rights should consumers have in response to any scheme or 'reasonable steps' taken by ISPs or rights holders? Does the legislative framework need to provide for these rights?

Answer: Existing case law suggests that the impact on non-infringing uses is one factor that may influence whether liability for authorising infringement is made out. However, once such a finding has been made it is difficult to see how individual consumers or representative organisations could be given standing to intervene so as to *enable authorisation of copyright infringement to continue*.

Again, the mere fact that this question has been posed suggests that there is a deep-seated confusion about the Government's aims: the desire appears to be to create a regulatory regime that will weigh the interests of copyright owners, carriage service providers, other online service providers and consumers. Authorisation is a very poorly suited vehicle for such a regime.

Question 6: What matters should the Court consider when determining whether to grant an injunction to block access to a particular website?

Answer: Further to our analysis in Part 4 we propose that the circumstances in which such injunctions are granted be limited to situations where:

(1) the infringement is of a serious nature; and

(2) legal action against those directly responsible for the infringement (the primary infringers) has been, or is likely to be, ineffective in halting that infringement because:
   (a) it is not reasonably practicable to institute legal proceedings against the primary infringers; or
   (b) it would be impossible to enforce any judgment against them.

We must, however, emphasise that these recommendations should be read against the background of the other principles that we identify in Part 4 that should be guiding the law reform process in this area more generally.

Question 7: Would the proposed definition adequately and appropriately expand the safe harbour scheme?

Answer: We are satisfied that the proposed definition is adequate.