Table of Contents

Editorial
Some people to celebrate
Peter Gerrand

The legal perils of being an Internet Service Provider
David Lindsay

Industry identities
Convergence: communications policy proposals for the digital economy: an interview with Malcolm Long
Liz Fell

Liability of ISPs and other Internet intermediaries
ISP liability for end-user copyright infringements: the High Court decision in Roadshow Films v iiNet
David Lindsay

On the (new) New Zealand graduated response law (and why it’s unlikely to achieve its aims)
Rebecca Giblin

Quelling P2P infringement – private American harbours or public French graduations?
David J Brennan

The key to dealing with P2P infringements: regulation, partnerships and education
Neil Gane

Internet users and copyright: should we have an industry code?
Holly Raiche

The footy killed Optus’ DVR
Warwick A Rothnie

Evaluating SOPA: who should enforce IP online?
Kimberlee Weatherall

Don't shoot the messenger: Wikileaks and the future of the Internet
Melissa de Zwart

The role of Internet Service Providers in combating botnets: an examination of recent Australian initiatives and legislative reform
Alana Maurushat

Broadband user experience
Consuming apps: the Australian woman’s slow appetite for apps
Scott Rickard, Clare Lloyd

About the authors

Our sponsors
SOME PEOPLE TO CELEBRATE

Peter Gerrand
Managing Editor, TJA

THE 2012 CHARLES TODD ORATION

Chris Chapman, Chairman and CEO of the Australian Communications and Media Authority (ACMA), will deliver the TSA’s 2012 Charles Todd Oration in Sydney at lunchtime on Thursday 30 August.

The ACS Telecommunications Society of Australia has been holding the Charles Todd Oration, named after the magnificent organiser of the Australian Overland Telegraph project of 1870-2, as the TSA’s major annual industry networking event since the 1980s, to provide a platform for the industry’s leading ‘movers and shakers’. Recent Charles Todd Orators have been Mike Quigley, head of NBN Co, in 2010 and David Thodey, head of Telstra, in 2011.

Those of us who remember Mike Quigley’s brilliant Oration on the NBN project, three days before the crucial 2010 federal election that decided the NBN’s fate, are confidently expecting that Chris Chapman will be prepared to publicly respond to the Final Report of the Convergence Review, one of whose controversial recommendations calls for the creation of a new regulator for the media and communications industries – which of course include telecommunications and broadcasting as well as the print media amongst their converging strands.

RICHARD EDMUND (DICK) BUTLER AM

While a sad occasion for Dick Butler’s family and friends, his death in Melbourne on 23 June 2012 at age 86 provides an occasion for the telecommunications industry to celebrate the life and career of this remarkable man. Dick was the first Australian to head a United Nations agency, in this case the International Telecommunications Union from 1983 to 1989. Such high level appointments have been rare for Australians: Francis Gurry’s appointment to head the World Intellectual Property Organization in 2008 is one of the few other examples. Dick had in fact been the highest ranking Australian on the UN staff since 1968, when he was appointed Deputy Secretary-General of the ITU, until his retirement in 1989. He made a point of personally welcoming many of the Australians who were sent to the technical standards-developing meetings of the ITU, the CCITT Study Group meetings, in Geneva.

The position of Secretary-General of the ITU is elected by the ITU’s member nations, and it is known that a key factor in Dick’s election to the top job in 1983 was his known commitment as Deputy Secretary (1968-83) to championing extending the benefits of affordable telecommunications infrastructure to Third World countries. In 1988 he was voted the world’s most influential telecommunications leader by the global industry. As his son Brendan said at Dick’s funeral, this was a remarkable feat for a former telegram delivery boy – that being his first job, in 1941, with the Australian Postmaster General’s Department.

After the war, he returned to work at the PMG and completed a public administration diploma at night at the Melbourne Technical College (now RMIT University). He progressed through
the ranks of the PMG to Chief Industrial Officer and from there by 1968 to Assistant Director General, before being seconded to the ITU.

After his retirement at age 63 from the ITU, Dick became involved in several initiatives aimed at extending satellite-based communications across South East Asia, and was an advisor to several governments, international agencies and corporations, as well as being appointed Chairman of two entrepreneurial companies in this sector, Airspace and Sky Station Australia. His colleagues have quoted him as having a particular interest in using low orbiting satellites and low cost receivers as a platform for education, health, capacity and community building in underdeveloped and remote communities, as well as supporting early warning and response systems for threats like tsunamis and the Ebola virus.

A much more comprehensive obituary for Dick Butler, contributed by his son Gerard Butler and son-in-law Mark Hoven, was published on 16 July in the Melbourne Age and the Sydney Morning Herald.

INTERVIEW WITH MALCOLM LONG

The interview in this August edition of the TJA follows on from the previous special June edition of the journal, focussed on the recommendations of the Australian Government’s Convergence Review, for which Malcolm Long was a member of the three-person Committee.

Malcolm Long has a distinguished history of participation in the broadcasting industry. In this interview, Liz Fell asks important questions, including the implications of the review for the telecommunications industry. The interview will be of great interest to all those who care about the future of media regulation, including the possible adoption of a ‘public interest’ test for media ownership, and what that might mean for media diversity in practice. The interview also includes interesting comments relating to the necessary ‘restacking’ of spectrum in the broadcasting services bands resulting from the digital transition.

While the Australian Greens have introduced a broadcasting bill into Parliament that incorporates a public interest test for new media licences, at the time of writing this editorial, the government’s response to the Convergence Review remains ‘opaque’. Much policy work still obviously needs to be done in this area before the Government and the Opposition develop viable media and communications policies to take to the next election.

THIS SPECIAL ISSUE OF TJA ON ISP LIABILITY

The TJA Editorial Board is grateful to Associate Professor David Lindsay from Monash Law School for his role as Guest Editor of this issue, in sourcing and helping manage the independent reviewing of such a comprehensive set of expert articles – including his own contribution – dealing with the implications of the Australian iiNet and Optus TV Now judicial decisions for ISPs and popular content providers; and with related issues concerning the liabilities of other Internet ‘intermediaries’ – such as banks and domain name registries – as a consequence of potential legislation in the USA and elsewhere.

We congratulate Dr Lindsay – and TJA author Dr Kimberlee Weatherall, Associate Professor at the Sydney Law School – in being recently appointed as expert advisors on copyright reform to the Australian Law Reform Commission.

iiNET BECOMES MAJOR SPONSOR OF THE TSA

And speaking of ISPs – and of the winner in this year’s historical legal battle between the ‘content industry’ and the Internet Service Providers, fought all the way to to the High Court – TJA is delighted to announce that iiNet, Australia’s third largest ISP (by customer numbers), has become a Silver Sponsor of the ACS Telecommunications Society of Australia, and hence a most welcome financial supporter of this Journal.
iiNet joins the other leading ‘corporate citizens’ of the Australian telecommunications industry – leading service providers Telstra and Optus, equipment vendors NEC and Alcatel-Lucent, and national research organisations CSIRO and NICTA – in supporting the industry-wide ‘learned society’ and networking activities of the TSA and its journal TJA.
EDITORIAL

THE LEGAL PERILS OF BEING AN INTERNET SERVICE PROVIDER

David Lindsay
Guest Editor

This edition of the TJA focuses on a range of stimulating and difficult legal issues that face intermediaries, especially ISPs, in performing their vital functions of providing access to communications content.

Over the past 15 or more years, we have become familiar with the radically destabilising impact of the Internet on established economic, social, legal and political structures. In relation to the delivery of information and entertainment content, the Internet has provided unprecedented and welcome access to all manner of content but, at the same time, decentralised Internet-based applications, especially P2P networks, have been engines for large-scale copyright infringement.

The highly politicised struggles over copyright – commonly known as the ‘copyright wars’ – are but one instance of the disruptive influence of the Internet on existing legal structures. An important aspect of these struggles arises from what is inelegantly referred to as ‘disintermediation’ – which, in this context, means the lessening influence of the traditional gatekeepers or intermediaries responsible for communications content, including publishers, the press and broadcasters. In place of the traditional intermediaries, which perform a role in the creation as well as the distribution of content, and therefore have an uncontested degree of legal responsibility for that content, we have seen the emergence of ‘new’ intermediaries, in the form of ISPs, search engines and social network service providers.

These new intermediaries have business models that rely essentially upon commercialising access to content. While they may well produce some content, in general they do not have to bear the costs of content creation. Nevertheless, given the costs and futility of bringing legal actions against individual end-users, the extent to which these intermediaries may be liable for the actions of their end-users has become one of the great legal issues of the Internet era. This issue inevitably raises complex policy issues relating to the proper role of access providers in ‘policing’ the behaviour of their users, the degree to which access/carriage providers should become involved in content issues, and the costs and benefits of enforcing offline legal rights in the online environment.

THE ‘GRADUATED RESPONSE’

From the mainstream emergence of the Internet in the mid-1990s, carriers and ISPs have been concerned about their potential liability for copyright infringements committed by their customers. As a result, telecommunications companies first became involved with international copyright policy-making in the negotiations leading to the adoption of the two ‘Internet treaties’ – the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) – in 1996. The concerns of carriers and ISPs that the potential for liability might adversely impact their role as access providers led to an Agreed Statement being added to the WCT, which provided that ‘the mere provision of physical facilities for enabling or making a communication’ would not, in itself, amount to an infringement of the exclusive right to communicate copyright material. Subsequently, in jurisdictions such as the United States and Australia, a degree of legal protection for some intermediaries was
established in the form of what is known as a ‘safe harbour’ regime, pursuant to which intermediary liability is limited provided an intermediary, such as an ISP, takes certain steps, such as adopting and implementing a policy for dealing with users who repeatedly infringe copyright.

Meanwhile, from the emergence of Napster in 1999, we have seen the evolution of generations of popular P2P file-sharing applications – culminating with the BitTorrent protocol – that provide efficient, decentralised mechanisms for end-users to distribute content, and which are difficult to police and control. The prevalence of end-user copyright infringements, and the failure of other means of controlling digital content, such as technological protection measures (TPMs), led the content industries, in the mid-2000s, to advocate a policy known as ‘graduated response’. The ‘graduated response’ strategy, which is also known as ‘three strikes’, aims to curb online copyright infringements by enlisting the help of ISPs in issuing warnings to repeat infringers, and ultimately suspending or terminating the accounts of recalcitrant end-users.

Versions of ‘graduated response’ have been introduced in a number of countries. In Australia, the complex copyright regime governing the liability of ISPs for end-user infringements was premised on the development of an industry code of practice, which would deal with the detail of how ISPs should respond to infringement notices issued by copyright owners. While representatives of copyright owners and the Internet Industry Association (IIA) entered into negotiations aimed at developing a code, nothing eventuated. Given this impasse, the Australian Federation Against Copyright Theft (AFACT), which is effectively the Australian investigation and education arm of the copyright owners, sent details of large-scale infringements committed by customers of iiNet, and ‘required’ that the ISP take appropriate action.

Following iiNet’s persistent refusal to take the action sought by AFACT, the copyright owners initiated an action claiming that iiNet’s inaction, in the face of the information provided by AFACT, rendered it liable for the infringements of its end-users. The first article in this edition, by Lindsay, analyses the landmark Australian High Court decision in *Roadshow Films v iiNet*. As the article explains, the clear result of the first decision on this issue, in any part of the world, by the highest court in a jurisdiction is that an ISP that does no more than provide Internet access will not be liable for end-user infringements, unless it does something unlikely, such as actively promoting unlawful downloading. As the article further explains, however, the judgments in the High Court have effectively changed the Australian law on secondary liability for copyright infringements, opening up a host of new legal questions.

The High Court decision in *iiNet* means that the implementation of a graduated response strategy in Australia depends, in the first instance, upon negotiations on a proposed code between the copyright owners and ISPs, with the Commonwealth Attorney-General’s Department brokering negotiations between AFACT and the Communications Alliance. A sticking point in the negotiations has been who should bear liability for the costs of implementing a graduated response regime. If the parties are unable to reach agreement, the future of graduated response in Australia will depend upon the willingness of the Parliament to introduce a legislative regime. At present, there is no indication that this seems likely. While the government has issued an important reference on copyright and the digital economy to the Australian Law Reform Commission (ALRC), the reference is confined to copyright exceptions, with the ALRC being specifically instructed not to duplicate work being undertaken on unauthorised distribution of copyright materials using P2P networks.\(^1\)

In contrast to the position in Australia, some jurisdictions – New Zealand, France, the United Kingdom, Taiwan and South Korea – have introduced laws implementing forms of graduated response, each of which has proven controversial. The second article in this edition, by Rebecca Giblin from Monash Law School, examines the New Zealand regime, which was implemented by the *Copyright (Infringing File Sharing) Amendment Act 2011*. After an analysis of the regime, Giblin concludes that it is unlikely to achieve the objective of deterring unauthorised file-sharing, given the costs of implementing the regime, an unintentional
loophole in the regime and the absence of any measures to encourage the creative industries to adapt to delivery of content via the Internet. More fundamentally, Giblin argues that graduated response strategies are flawed in that suspension or termination of Internet access is a disproportionate response which may infringe user rights and that they do not deal with the true source of the problem of unlawful downloading, which she identifies as the failure of copyright industries to provide timely and reasonably priced content.

In the following article David Brennan, from Melbourne Law School, compares and contrasts the voluntary graduated response regime, entered into between copyright owners and large ISPs in the United States, with the French legislative regime, which is known as HADOPI. After explaining that, under US law (as in Australia post-iiNet), it is unlikely that ISPs that merely provide access will be liable for end-user infringements, Brennan suggests that the US ‘five-strikes’ regime may have resulted from a ‘behind-the-scenes’ role played by the Obama administration, as well as the threat of possible legislative intervention. In contrast to the Giblin article, Brennan refers to a recent report from US academics which concludes that the introduction of HADOPI resulted in a significant increase in lawful downloads from iTunes in France. From the American and French experiences, Brennan draws the lesson that the threat of introducing a HADOPI-style law may be essential for a US-style voluntary regime to be negotiated in Australia. Whatever the case, it seems that, in regimes that have introduced graduated response regimes (whether private or public), we will face ongoing debates about the effects of those regimes on user behaviour, including debates about the methodologies employed in academic and industry studies.

INDUSTRY AND USER RESPONSES

The fourth article in this edition, by Neil Gane, the Managing Director of AFACT, explains how, from the point of view of copyright owners, graduated response is necessarily part of a broader strategy for dealing with the problem of P2P file-sharing. According to Gane, there is no silver bullet, but an effective strategy must involve regulation, partnerships between the content and telecommunications industries, and ongoing user education. Importantly, Gane points out that there is a growing commonality of interests between the telecommunications and content industries, as carriers and ISPs are increasingly concerned with monetising content. Nevertheless, drawing from comments made by Charleton J in the Irish High Court, he concludes that the decision in iiNet has revealed that the current Australian law is inadequate to deal with P2P file-sharing, and calls for legislative intervention.

In the following article, Holly Raiche, from the Internet Society, argues that the user-perspective has been missing from debates about the appropriate response to P2P file-sharing. While agreeing with Gane that education is an essential part of any solution to the problem, Raiche proposes elements of a regulatory response that would effectively incorporate user rights and interests. Apart from the importance of user input into any code development process, she maintains that, from a user perspective, any code must: not automatically equate the account holder with alleged infringers; respect the privacy of account holders; incorporate an effective appeals mechanism; and include account termination only as a last resort. Over and above the details of a proposed code, Raiche points out that the focus on unlawful downloading should not blind us to the integral role now played by the Internet in peoples’ lives, suggesting that any responses to the problem must be kept in proportion.

ADDITIONAL ONLINE COPYRIGHT DILEMMAS

Copyright controversies involving carriers, ISPs and other intermediaries are not confined to their potential role in relation to P2P file-sharing. Two further articles in this edition examine two recent important legal controversies.

Users are increasingly taking advantage of cloud computing to access material when and where (and on which device) they want it. The mismatch between cloud computing and copyright law in Australia has been highlighted by a service provided by Optus, known as TV
Now, which sought to take advantage of an exception to copyright that allows viewers to make copies of broadcasts for later viewing for their own private use. The Optus service enabled users to record television programs on an Optus server, which allowed users to access the recorded programs on their mobile and Internet devices. In practical terms, a user could access a live broadcast of a football game from a mobile or Internet device with only a two-minute delay. This obviously alarmed the rights owners in football broadcasts – Telstra, the AFL and the NRL – as, if Optus could take advantage of the private use exception it could effectively provide a service involving near-live streaming without paying the rights owners.

Warwick Rothnie, from the Victorian bar, clearly and thoroughly explains the complex legal issues in the Optus TV Now litigation, focusing on the decision of the Full Federal Court, which held that Optus was not entitled to the exception. As Rothnie points out, the decision gives rise to a number of significant legal issues for which the Copyright Act provides no clear answers. At the time of writing, an application for leave to appeal to the High Court has been made, but the outcome of the application is unknown. Regardless or whether or not the High Court agrees to hear the appeal, the scope of the private use exception relied upon by Optus will be dealt with in the ALRC copyright exceptions review, mentioned above.

If one thing is certain, the copyright wars are far from static, with the strategies of owners and infringers continually evolving against a background of shifting technologies and markets. Earlier this year, controversial US legislative proposals for enlisting a range of new intermediaries – domain name servers, credit card providers and online advertising service providers – in online copyright enforcement, were withdrawn from Congress. The article by Kim Weatherall, from the University of Sydney, explains and analyses the most important of the US legislative proposals, known as SOPA. As Weatherall explains, if implemented, SOPA would have effectively enabled a ‘multi-system denial of service’ attack on ‘rogue’ websites, such as The Pirate Bay, by preventing the DNS from resolving to the site, requiring search engines to eliminate links to the site, requiring US credit card companies to refuse payments to site operators, and prohibiting US companies from advertising on such sites. While, following considerable online outrage, SOPA was withdrawn, Weatherall focuses on the fundamental implications of the proposed regime for more general arguments for imposing liability on intermediaries. On this, Weatherall concludes that the argument that liability should be attached to intermediaries on the basis that this is an efficient approach to enforcement – known as the ‘least cost avoider’ argument – is flawed, as it ignores other important considerations, including whether the overall costs of imposing liability outweigh any benefits, and longer term negative consequences that might follow from imposing liability. In addition to the important points made by Weatherall, the SOPA saga suggests that there may be real political limitations on the extent to which liability can be attached to access intermediaries, especially as the increased lobbying power of access providers, such as Google and Facebook, is effectively brought to bear.

OTHER ISSUES FOR INTERMEDIARIES

Controversies concerning the role, and potential legal responsibilities, of intermediaries are by no means confined to the copyright context. Two articles in this edition examine the role of Internet intermediaries in a broader context.

The first of these, by Melissa de Zwart from the University of Adelaide, focuses on one of the most prominent examples of disintermediation, WikiLeaks. As de Zwart explains, WikiLeaks is essentially an intermediary that was intended to be a mere conduit for the publication of material sourced from whistle-blowers, but which, because of circumstances, evolved so that Assange, the public face of WikiLeaks, assumed a more ‘hands-on’ role. Nevertheless, the relatively unmoderated nature of publication via WikiLeaks serves not only to distinguish it from traditional media, but also to explain much of the concern of governments, especially the US government, with the WikiLeaks model. The second part of the de Zwart article provides an interesting companion-piece to Weatherall’s analysis of the SOPA saga, in that it explains and analyses the use of financial intermediaries, including PayPal, Mastercard and VISA, to deny processing of payments to WikiLeaks. According to de Zwart, given that the financial
intermediaries denied payments on the basis of an allegation that WikiLeaks had breached their terms of service, this illustrates the troubling extent to which online regulation and enforcement has been privatised. In effect, the activities of WikiLeaks, which are located largely outside the US (and which may not be illegal even in the US), could be effectively denied resources without any proper legal process.

In the second of these articles, Alana Maurushat, from the UNSW Cyberspace Law and Policy Centre, examines the role of ISPs in combating botnets. The article summarises and explains the four main methods of tackling botnets, pointing out that ISPs play a role in all but one of these methods. As Maurushat points out, ISPs are generally not regarded as being responsible for the security of their customer’s computers, or for monitoring content. However, recent Australian proposals detailed in the article, including the e-Security Code, incorporate a greater role for ISPs in dealing with end-user security. Based upon the uncontested need to ensure network protection and security, Maurushat argues that effective botnet remediation programs can only be implemented with active intervention by ISPs. While necessary, such intervention should be restricted to protect users and their privacy by, for example, being limited to small and medium packet inspection and passive monitoring. Importantly, the article argues that ISPs cannot be expected to adopt a greater role in combating botnets without the protection of legal limitations on liability, which go beyond that conferred by the 2010 amendments to the *Telecommunications (Interception and Access) Act*. Read together with the other articles in this edition, the article illustrates not only the complexity of the issues involved with the legal liability of intermediaries, but the importance of avoiding high level generalisations, and taking into account the particular context, in developing laws and policies relating to the vital role of intermediaries in the online environment.

As guest editor for this edition of the TJA, I would like to thank each of the authors for the care, diligence and expertise with which they have addressed the particular issues dealt with in their contributions. Overall, the collection represents an important snapshot of many of the important ‘live issues’ in this area as of mid-2012.

ENDNOTES


Liz Fell

In December 2010 Malcolm Long was selected by the Australian Government as one of the three-committee members to review and develop a new policy framework for the converging media and communications sectors. After broad public consultation and hundreds of submissions, the committee’s Convergence Review was released publicly on April 30, 2012.

Long’s extensive media and communications experience spans the public and corporate sectors. He is currently chairman of the National Institute of Dramatic Art (2007-); chairman of the advisory committee of the Australian Centre for Broadband Innovation; and a director of the Broadcast Australia Group (2011-); and, formerly, the Macquarie Communications Infrastructure Group (2002-2009).

His career includes regulatory experience as a member of the Australian Communications and Media Authority (2005-2010) and the former Australian Broadcasting Authority (2000-‘05), as well as executive and managerial experience including: executive director, Australian Film Television & Radio School (2003-2007); managing director, SBS Corp. (1993-1997); deputy managing director, Australian Broadcasting Corp. (1992-1993); and director, ABC Radio (1985-1991). From 1975-85, he occupied various management and production roles with ABC Radio as a departmental head, executive producer and radio broadcaster, and earlier with West Australian newspapers as a journalist.

Long is principal of the consultancy, Malcolm Long Associates Pty Ltd (1998 ), and holds an LLB from the University of Western Australia. He is a Member of the Australian Institute of Company Directors (AICD).

Freelance journalist, Liz Fell, interviewed him for the TJA in mid-July in Sydney.

TJA: The present government has initiated a huge range of separate digital economy policy reviews including, among others, copyright, national classification, cultural policy, the independent media inquiry and convergence, but no separate telecommunications review...

Long: ... except the ACMA review of customer care and codes which has just recently hit the deck and was a pretty big exercise!

TJA: Yes, but an analysis of the telco or connectivity sector is missing from the overall convergence review. Why did you narrow down the field?

Long: Well, it was the government’s decision to split it up. The review could have covered the whole of communications, both the connectivity as well as the content delivery, but I suppose the advantage of the split was that we found it fairly challenging getting across all the inter-related issues that dealt with the delivery of content. Now that content is delivered on
every platform it would have been twice as complex to do the connectivity issues as well. We say in our report, towards the end when we talk about implementation, that clearly a next step for government if it wants to do it, is to take our report and consider the connectivity issues in telecoms, and try and align those. That wouldn’t be too difficult, actually, because the broad structure of the Telecommunications Act is pretty much a layered structure already, which is the approach, we’ve taken.

**TJA:** Reading the report I found myself wondering whether telcos such as Telstra will continue to need their existing carrier licences and, if so, would this licensing be the responsibility of a new communications regulator that you recommend rather than ACMA?

**Long:** On licensing our view was based on the ten principles that we derived after a fairly major interaction with the community and the players. The first of these principles, which had not really been articulated this clearly before in Australia, was that citizens and enterprises should be able to freely communicate. If that’s the case, we thought, then why do we have licences for communication of content?

We came to the view, as you can see in our report, that the licensing of content creation and delivery as such was neither really necessary nor appropriate in the new digital economy.

This, of course, doesn’t address the issue of the licensing of a scarce resource like spectrum which makes a lot of sense. Whether broader licensing in the telecommunications connectivity field is now necessary or appropriate would be a prominent theme, I think, for the next piece of work which the government may or may not do.

**TJA:** Leaving aside the allocation of spectrum for the moment, can you provide readers with the context for the convergence that your review addresses?

**Long:** Well, in the old analog days, there were two churches in the communications business: one was called broadcasting and the other was called telecommunications. In the broadcasting church, content was everything, and there were protections, legislative frameworks, and rules and laws to do with content. In the telecommunications church, content was almost a byproduct of connectivity and customer issues mostly related to connectivity. Content was generated by individuals when their connectivity, one-to-one, was achieved by the telco supplier.

The revolution that has occurred – and I think we captured it in the convergence review earlier than most – is that the days of seeing content as a broadcasting issue and not as a telecommunications issue, are over. Telecommunications providers provide professional content in large volumes both to individuals one-to-one and to groups through IP multicasting and other methods, and they are beginning to rival the amount of content delivered by broadcasters. So these days content, its delivery and its shape and, to some degree, its regulation is every platform provider's issue – from telecommunications providers to broadcasters. Now what we have said in the convergence review is that in the light of that, both sides need to accept that there are some rules that the community expects when professional content is delivered over networks to large numbers of people, and they are the rules that we recommend.

**TJA:** Who came up with the computer-speak term ‘content service enterprises’ to describe broadcasting and media organisations that could be subject to ownership regulation ‘in the public interest’? The phrase ‘content service enterprise’ is a mouthful...

**Long:** It’s not elegant, Liz, that’s for sure!

**TJA:** That must be an understatement! Indeed, I discovered via Google that Enterprise Content Management is computer-speak for a software package used by IBM, among others.

**Long:** Look, the problem is that in this new environment, what do you call these entities which operate on multiple platforms? They’re not just broadcasters.

**TJA:** Perhaps you could just call them ‘content’ providers...

**Long:** Well, is that any more or less elegant?
TJA: No.

Long: That’s the problem. We ran out of inspiration.

TJA: What about cultural services?

Long: Cultural sounds a bit highfalutin for this pretty broad thing. We thought that it was about content of all kinds, including high culture and other cultures; that it was about enterprises; that it was about big companies; and that it was about providing those services at the interface with the consumer, which is where the regulation is focused. So we took the easy way out and talked about them as content services enterprises, but I agree with you, it’s not necessarily the best label.

TJA: Still, it was a change to read your comment piece in the *Australian Financial Review* on the committee’s proposed public interest test of ownership diversity without baulking at that vacuous phrase, content service enterprises. Indeed, it was interesting to read that the committee found ‘Australians care deeply about the number of owners in the media because they know it is related to the range of news and opinion available to them.’

Long: Yes, I think it said ‘inexorable appetite’.

TJA: Goodness, I didn’t see you had said that!

Long: We didn’t quite say that! But that innate belief that people had a right to a selection of media run by a selection of different entities and individuals was very striking to us wherever we went, and we toured all over Australia.

TJA: Was there a majority view among those you consulted that the traditional electronic radio and TV content services should remain freely available to all citizens? As a former public broadcaster I assume you would adopt this view.

Long: Yes, I obviously see it as relevant and, even more broadly, I see the advertising-funded model of content delivery on electronic networks as relevant. My impression is that people want it all: they want to retain their public broadcasters, their advertiser-supported commercial broadcasters in radio and television, pay TV and their online services that are not subscriber-driven. They also understand that, for some things, they’ve got to pay something if you care enough for it.

Frankly, I think they have a much more sophisticated view of the mixed economy of content delivery than most commentators who tend to see the world either as ‘you pay for it’ or ‘it comes from the ABC and you pay, anyway, because you are a taxpayer’. As part of the world of the digital economy, people do understand the gradation of commercial engagement they have with content, and they understand that the business models are kind of ‘up for grabs’.

In this world, you could almost go so far as to say that many people out there who are just ordinary punters have as good an understanding of the world we are all involved in as the so-called experts.

TJA: Well, one of the experts in the telco sector is Henry Ergas whose commentary on the proposed regulation of media ownership focused on ‘market forces’ and suggested that an ‘uncertain’ public interest test would discourage media investment.

Long: Well, just to comment on that, the convergence report is profoundly de-regulatory. But the press, and some commentators – for whatever reason – have decided to build this view that it’s re-regulatory when, in fact, it reduces regulation. Our feedback -- and I received this at an event I spoke at the other day -- is that it’s the complexity of the existing regulation on ownership and control rules for broadcasters that deters capital and international players from getting involved. They look at the 4/5 rule, the 2 out of 3 rule, the 75 percent rule for broadcasters, and say that it is too complex. Now, in our report, we get rid of most of that regulation.

TJA: So was the review committee in favour of leaving the industry to market forces?

Long: Yes, to a considerable extent, right across the board, including the conversion of licences for commercial broadcasters to spectrum licences and so on. The fact is that
Australians expect a minimum range of rules to achieve certain public goals which they don’t believe are necessarily delivered by the market, and we had no evidence otherwise. One of those rules is the diversity of owners.

TJA: Still, Kim Williams, the CEO of Murdoch’s News Ltd, has threatened action in the High Court if the government accepts a ‘super regulator’ and a ‘public interest test’. What is your reaction to his comments?

Long: First, let me say that the existing media rules already include newspapers. The ‘2 out of 3’ rule affects existing newspapers so it’s not accurate to say that they are not affected by current media legislation. Let me describe briefly what we recommend in the area of broadcast and media ownership. We said, let’s get rid of most of those rules and have a much simpler approach where, at the local level, we keep a number of voices test like the current 4/5 test. That’s a metric test, which has certainty.

We endorsed that approach, although we believe that the number of different owners required might change as you bring in other media as relevant voices. At a national level, the ubiquity of the current media indicates the need for a national approach, since any television or radio station or newspaper in Australia today is, in fact, a national medium and can be picked up online anywhere in the country. Fairfax, News Ltd and so on are really looking, these days, at their digital readership on a national basis.

So we have suggested that we have a simple public interest test that would be based on a series of criteria. We’re not suggesting a public interest test which is just open slather and which is one of the mischievous aspects of the current debate in the newspapers. We suggested explicitly in the report that we should have a debate about what the criteria should be, and that we have a truly independent regulator. Just like the ACCC and a whole bunch of other agencies, when a business circumstance arises, the independent regulator applies the criteria and makes a judgment. In Australia, those kinds of public interest tests, in the broad sense, are applied every day.

TJA: Still, couldn’t this proposed ownership regime turn out to be almost as convoluted as the old scheme?

Long: Well, our approach was that the criteria that one would use would be about the number of players and the platforms they’re on. It’s really – and maybe we should have called it this – a diversity of owner test. But, of course, subsequent to our report coming out, with the Fairfax developments and so on, the question of whether that test might be applied in other ways to the beliefs of potential acquirers of companies and so on has got into the mix.

TJA: Does that mean the views of potential owners could be vetted?

Long: No-one suggested to us that the personal opinions of individual potential acquirers of media companies should somehow be vetted. I don’t believe that would occur. The range of owners is the best proxy for getting to diversity.

TJA: Meanwhile, the Greens have introduced the Broadcasting Services Amendment Public Interest Bill 2012 to the Senate. Have you read it?

Long: I’ve looked at it, yes.

TJA: Do you have any comments on it?

Long: Having done our report, said what we believe a 'diversity of owners' test should be based on, and argued why we believe that, I think it’s not particularly constructive for those of us who wrote the report to say much about the subsequent political bunfight other than to refer people to what we believe should be done in our report.

TJA: In the case of News Corp., would you need to combine all its media platforms and their revenues to decide whether it is classifiable as a content service enterprise and subject to the rules?

Long: Well, every large content provider in Australia is now on multiple platforms, so the notion of roping in an organisation which is not on a relevant platform is really quite
redundant. To survive in this business, they’ve got to be on more than one platform, and we didn’t find it convincing that any platform that any big player might be on should be somehow excluded from the very basic and pretty simple rules that we propose.

**TJA:** Looking at the opportunities opened up for Telstra by the convergence review recommendations, I read that the head of Telstra Media, Rick Ellis, was talking about decoupling the content assets from the network assets and using multiple delivery models. Did you follow that development for the review?

**Long:** I think that Rick Ellis is absolutely right to decouple content from its delivery platform. That is the fundamental philosophy of the convergence review. The days when content rules could be applied on particular platform owners but not on other platform owners – to the degree you have rules and, as I said earlier, we have deregulated many of those rules – so to the degree you need rules for public policy reasons, then the application of those rules has nothing to do with the platforms, whether they are old-world telecommunications platforms or old-world broadcasting platforms. In our view, it has everything to do with the size and penetration of the entity, the enterprise, that controls or generates that content.

**TJA:** What does this decoupling mean for Telstra’s status as a content service enterprise?

**Long:** Decoupling means dealing with content issues based on the fact that the enterprise is a provider of content rather than looking at the sort of platform it operates. What that means for a telco is that if, using its particular platforms, it provides and controls large amounts of professional content of the kind that was once provided to Australians only by broadcasters then, when it gets to a certain size, it falls into the same regulation based on the principle of parity as anyone else who provides content.

**TJA:** And this content doesn’t include talking with you over Telstra telephone lines or over wires?

**Long:** Nor does it include social media and Facebook and so on in the metric. It’s professional content.

**TJA:** What about the triple-play practice of bundling the purchase of a Telstra broadband connection and a Telstra mobile connection with the Telstra Media content?

**Long:** Bundling is fine.

**TJA:** Surely, it’s difficult to split the revenue from the content and from the connectivity?

**Long:** Not really, especially in organisations which are buying and then ‘broadcasting’ content. They know the metrics. Companies that buy AFL rights know what return they get on that investment otherwise they wouldn’t be buying it.

**TJA:** The decoupling of network connectivity and content services reminds me of the controversy over Telstra’s planned structural separation of its wholesale and retail arms!

**Long:** Well, we don’t believe the only obligations that content service enterprises have in the three areas we have identified as requiring market intervention – number of owners, content standards, and Australian and local content – are so onerous and so irksome that any organisation with its brand equity is going to peddle really hard to artificially avoid them. It’s not worth their public reputation to do that.

**TJA:** What is the status of an Internet service provider such as iiNet Ltd that has partnered with FetchTV to provide IPTV content to its customers? Which partner could be identified as a content service enterprise for some sort of regulatory oversight?

**Long:** Well, our approach is that the regulatable entity is the professional content provider that has the interface with the consumer. It’s fine if the ISP is just a pipe and a conduit for another business which, in fact, has the business relationship with the consumer. But I think there will be an issue for ISPs – as they get more and more into controlling the content distributed on their network, at some point they will become a regulatable entity. So it’s going to be a case of ‘suck it and see’.
TJA: And an ISP like iiNet may be interested in winning customers by bundling its connection with an unmetered product such as the ABC’s iView!

Long: Well, one would need to look at those three key tests; revenue, control and content. Applying those to the delivery chain, the regulator will then make a decision as to who is regulatable.

TJA: Moving to the allocation and licensing of spectrum by broadcasters and telcos, which is an area where you have knowledge and experience as a former member of ACMA and a director of Broadcast Australia.

Long: Well, let me make the general statement that it has been the case in the past, more so in broadcasting than in telecoms I think, that the issues of spectrum acquisition and management has been a bit of a ‘black art’ and has tended to be exercised by the technical rather than the general managers. I think that has had some strengths in that some really good spectrum outcomes were achieved for solid evidence-based technical reasons, but it has also had some weaknesses where, frankly, a lot of general managers in our communications organisations have not been intimately involved in some of the key, complex issues to do with spectrum. Now, of course, they’re scrambling on board fast because it’s becoming such a key conduit for any communications business.

TJA: I see the review’s first recommendation is for a market-based pricing approach that provides ‘greater transparency when spectrum may be used for public policy reasons’.

Long: Well, our approach was again coming from the ten principles that we outlined in the beginning of the report, which is that the use of spectrum in Australia must be in the public interest. It’s a public resource, it’s a resource which has massive calls on its use, and at the end of the day, there is no more of it, it’s a finite resource. In the areas dealing with spectrum in the report, and we mostly deal with spectrum as it relates to the broadcasters, we are focused on simply trying to maximise the efficient use of that resource.

TJA: The Minister has announced that early next year the mobile telcos will have the chance to take part in the auction of some of the former digital TV spectrum that they would use for their 4G mobile services...

Long: You mean the digital dividend spectrum?

TJA: Yes, apologies. I have always tried to avoid the term ‘dividend’ for the spectrum that is freed up by moving from analog to digital!

Long: Well, digital television is now well entrenched in the community. In areas where digital conversion has happened, 100 percent have access to digital television services, and the former analog spectrum is available for redeployment. So the auctions will occur and, soon after, analog will be switched off nationally.

TJA: Meanwhile, I understand that some of the digital TV services may have to be moved to new channels, a process known as restacking. Will that be easy?

Long: Yes, hopefully, it will be relatively easy. It’s got to be restacked so it creates a spectrum block in the 700 MHz band for it to be redepolyed by government for other purposes. For citizens, a vast number of them have digital TV sets thanks to the very rapid penetration of flat screens into Australia, and a very large number will have sets that will re-tune automatically very easily to the new frequencies.

TJA: Easily? I wonder about that!

Long: Well, there will need to be government information campaigns and assistance for people.

TJA: Staying with wireless, can we talk about the Broadcast Australia (BA) where you are a board director? But first, did you find it necessary to excuse yourself from the ACMA board or convergence review meetings for ‘conflict of interest’ reasons?

Long: Yes, strictly and punctiliously with the ACMA in the convergence review process, as were other members regarding potential
conflicts. The key was to have that out on the table so that everyone was aware of our other involvements and that the potential conflict of interest situation was being handled.

**TJA:** BA owns and operates an extensive wireless communications network across Australia that, among other activities, carries the ABC and SBS services. I was scanning ACMA’s carrier list recently and didn’t see its name so can I assume the company doesn’t require a licence for this network?

**Long:** Yes. The carriage of broadcasting is an exception to licensing under the *Telecommunications Act* and any spectrum-related licences are held with the service providers rather than BA.

**TJA:** What about the licensing of BA’s network of towers?

**Long:** The service providers usually hold apparatus licences.

**TJA:** I understand that some of BA’s towers in regional areas are too high for you to lease capacity on them to telcos! Is that correct?

**Long:** There are high sites, but depending on coverage needs we have leasing agreements with a range of telco operators for certain purposes. Cellular coverage is one. Backhaul is another. So our high sites are useful in the telecoms market for a range of purposes, and we have constructive business relationships with all the telcos.

**TJA:** BA has recently secured a contract to provide a private network for Ergon Energy in Queensland. Is that a carrier role it is playing?

**Long:** No. BA is an infrastructure provider and operator and the licensing, when it's needed, is normally held by the client who is the service provider.

**TJA:** Are there opportunities or advantages for BA’s network with the construction of the National Broadband Network?

**Long:** Absolutely. The NBN is becoming a big player in both the fibre and wireless areas so Broadcast Australia is really interested when it can see an opportunity to work with any of those players, including the NBN.

**TJA:** At one stage there was a proposal to include an RF feed in the NBN design for delivering free-to-air digital TV services to the home via the fibre network. Was BA involved with that proposal at any stage?

**Long:** No. The decision not to do that was made by the NBN for business reasons.

**TJA:** BA has been active offshore with its Transit Wireless project that is providing wireless connectivity for commuters in the New York City underground subways. That must have been an exciting contract?

**Long:** Yes. BA’s Transit Wireless project is installing mobile connectivity and Wi-Fi broadband connectivity into New York subway stations. The challenge in the wireless business is how to make connectivity truly ubiquitous and, in many subway systems in the world, you can’t use your mobile phone or iPad or any other wireless device either on the platform or in the tunnels.

**TJA:** Has BA been involved with a similar project Hong Kong?

**Long:** BA is a major shareholder in RFE which has done it in Hong Kong.

**TJA:** Where does Broadcast Australia move next?

**Long:** I think BA is in a very good position. It’s got one of the biggest wireless networks in the world in terms of broadcast – both radio and television right around Australia. Its core skills, of course, are 24/7 robust service; and as you know from broadcasting, to go off the air is the last thing you want to do. So the ability to maintain services as robustly as possible on a 24/7 basis is one of BA’s core capabilities and, of course, that is now becoming relevant in a whole lot of areas such as emergency services and private networks.
TJA: Finally, you have said that you took a ‘blank page’ approach to the review that it will try to provide a framework for.

Long: Yes. We had a choice of suggesting what I call ‘nipping and tucking’ of existing legislation, or of saying that the whole framework of carriage and content needed to be rethought and refined. We decided that our most useful contribution would be to say that in the light of the digital economy, where would we like to end up in terms of regulatory frameworks and settings in 20 years, and to take the lessons of the digital economy and apply them to a clean sheet approach to say ‘Well, where should we be going now?’

Now we could have gone the other way, but we believed that to put some markers down about how a regulatory framework might look as we go down this amazing adventure called the ‘digital revolution’, and would deal with the key issues of parity, multi-platform, content delivery, empowered individuals in social networks, was much more effective in terms of thinking about policy than suggestions to minor change to existing legislation. So we did that, and even produced a blueprint of how to get there in the report - in three stages essentially - and we hope the government, whichever government, will look at that and draw something from it.

TJA: The government took about one month before it released the report publicly. Did it change anything you wrote?

Long: Certainly not.

TJA: So did you enjoy doing the review that must have been a lengthy exercise with the various discussion papers, the submissions and consultation?

Long: Yes. It was stimulating and fascinating and enjoyable. What better thing for someone who has been involved in the broadcasting/communications industry all their life to be involved in suggesting a new way of approaching it!

TJA: Thanks for your time.
ISP LIABILITY FOR END-USER COPYRIGHT INFRINGEMENTS
THE HIGH COURT DECISION IN ROADSHOW FILMS v iiNET

David Lindsay
Faculty of Law, Monash University

In Roadshow Films v iiNet, the High Court unanimously held that iiNet was not liable for copyright infringements committed by its subscribers by means of the BitTorrent peer-to-peer file-sharing system. While the two judgments delivered by the High Court have clarified the extent to which ISPs may be liable for end-user infringements, they have created considerable legal uncertainty about authorisation liability, which is the main Australian doctrine under which a person may be found liable for the infringing conduct of another person. This article explains and analyses the two judgments delivered by the High Court in iiNet, focussing on the implications of the decision for ISPs, and for authorisation liability more generally.

The evidence establishes that detection ... followed by warning over three occasions and eventual discontinuance of Internet access will succeed in strongly alleviating the problem of Internet piracy.

EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd [2010] IEHC 377 at [71] per Charleton J.

Was it a reasonable step to require of iiNet that it monitor continually the activities of IP addresses to provide precise details of primary infringements that had been committed, and then take further steps to forestall further infringements? Warnings might or might not have that effect. Evidence was lacking of likely behaviour in that respect by users of ISP facilities.

Roadshow Films Pty Ltd v iiNet Ltd ((2012) 286 ALR 466, 498) per Gummow and Hayne JJ.

INTRODUCTION

In Roadshow Films Pty Ltd v iiNet Ltd ((2012) 286 ALR 466) (‘iiNet’) the High Court unanimously decided that iiNet, Australia’s second largest Internet Service Provider (ISP) provider of broadband services, was not liable for copyright infringements committed by end-user subscribers downloading files by means of the BitTorrent file sharing system. The decision is significant, both domestically and internationally, as it is the first time that a court at the apex of a national legal system has considered the liability of an ISP for infringements committed by its subscribers. As explained in this article, the outcome of iiNet is that, under Australian law, an ISP that does no more than provide Internet access will not be liable for the infringing activities of its subscribers unless it does something to actively promote those infringements.

This article explains, and critically analyses, the two judgments delivered by the Court in iiNet. First, the article introduces the context of the litigation by describing the international strategy promoted by copyright owners to address the problem of large-scale online infringements, known as ‘graduated response’. Secondly, the article introduces the relevant
facts in the case, including brief explanations of the BitTorrent protocol, as well as of the claim made against iiNet, which is essentially that iiNet was responsible for authorising end-user infringements. Thirdly, the difficulties in determining the meaning and scope of authorisation liability are explained by reference to the history of this area of the law, including the historical divergence of English and Australian law, and the way in which authorisation liability has been affected by legislative reform in Australia. Fourthly, the article explains and analyses the judgments in iiNet, including the judgments in the Federal Court. In analysing the High Court judgments, the article emphasises significant differences in the reasoning of the two judgments delivered by the Court. Fifthly, the article identifies the implications of the High Court’s decision for the liability of ISPs for the copyright infringements of their subscribers, as well as the more general implications for secondary liability for copyright infringement under Australian law.

THE ‘GRADUATED RESPONSE’

In the face of persistent large-scale copyright infringements by end-users, and of the relative lack of effectiveness of both actions brought against individual end-users and of Digital Rights Management (DRM) systems, since approximately 2008 the copyright industries have promoted a strategy of engaging Internet intermediaries, especially ISPs, in their campaign to reduce infringements. The strategy, which is known as ‘graduated response’, involves ISPs passing on warnings generated by copyright owners to allegedly infringing end-users, with the possibility of further actions, such as suspension or termination of an account, in the event of non-compliance with the warnings (Yu 2010).

Legislative regimes which embody some form of ‘graduated response’ have been introduced in a number of jurisdictions. In France, a law known as HADOPI (Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet) was introduced, in its current version, in 2010. The law, which embodies a form of ‘three strikes’ policy, provides that termination can only occur following a non-adversarial court decision (Lovejoy 2011). In the United Kingdom, the Digital Economy Act 2010 (UK) introduced a graduated response regime, with details to be dealt with by an Ofcom code, and with appeals available to a non-judicial body (De Silva and Weedon 2011). Other graduated response regimes have been introduced in South Korea (Korean Copyright Act, Article 133bis) and New Zealand (Copyright (Infringing File Sharing) Amendment Act 2011 (NZ)). In the US, on the other hand, in 2011 large ISPs and copyright owners entered into a voluntary ‘six-strikes’ regime, that is aimed at warning and educating end-users, and which may result in a subscriber’s account being throttled, but not terminated (Brenner 2012).

In Australia, the Digital Agenda reforms of 2000, and later the ‘safe harbour’ regime introduced in 2005, envisaged that ISPs would develop a code of practice that would establish processes for dealing with complaints by copyright owners about end-user copyright infringements. Although the copyright industry and ISP representatives initiated discussions aimed at developing an industry code, by 2007 negotiations had broken down, so that no industry code was ever developed ((2011) 275 ALR 1, 63-4 per Jagot J). In the absence of either a legislative regime or a voluntary ISP code, the strategy of promoting a version of graduated response in Australia depended upon establishing the legal responsibility of ISPs for infringements committed by their subscribers. As the circumstances, if any, under which an ISP might be liable for end-user infringements under Australian law were not at all clear, copyright owners initiated an action against an ISP – iiNet - that had refused to take any action in response to infringement notices.

THE FACTS IN iiNET

iiNet is a successful ISP, whose main business is supplying subscribers with communications services, especially Internet access. At the time of the trial in the case, it had 490,000 subscribers, and was the third largest ISP in Australia ((2012) 286 ALR 487). It has since
grown. By providing Internet access, an ISP provides access to a range of applications, which include P2P file-sharing services.

In a 2007 report cited in the first instance judgment, it was found that 57% of Internet traffic in Australia involved P2P services ((2010) 263 ALR 215, 238). It is common knowledge that a significant proportion of traffic over P2P networks involves unlawful uploading and downloading of copyright-protected material.

**THE BITTORRENT FILE-SHARING SYSTEM**

The BitTorrent protocol was designed by Bram Cohen, and is far and away the most popular system of P2P file-sharing. As clearly explained in the first instance judgment, the protocol consists of three essential elements:

- the BitTorrent client;
- .torrent files; and
- the tracker.

The BitTorrent client is the computer program that must be downloaded to a user’s computer so that the user can download and upload files using the BitTorrent protocol. There are many BitTorrent clients some of which may be downloaded for free, including KTorrent, Limewire and Vuze, and other clients which are proprietary, including BitTorrent and uTorrent. While the features of each BitTorrent client differ, the software all works in essentially the same way.

To be able to locate files, such as films or music, the BitTorrent client must use a .torrent file. A .torrent file is simply a small file that contains the necessary information to identify and locate content files. Each .torrent file has two sections, known as the ‘announce’ section and the ‘info’ section. The ‘announce’ section contains the URL of the ‘tracker’, which is explained below. The ‘info’ section contains metadata about the file that the user is seeking, including the file name, the size of the file, the hash value of the file and the hash value of pieces of the file, which are used to verify the integrity of the files. A .torrent file must be accessed by the BitTorrent client from various websites that make such files available.

The third component of the protocol is the ‘tracker’ computer program. The .torrent file directs the client software to the URL for the tracker program for the requested file. The tracker program has the Internet Protocol (IP) addresses of end user computers (or ‘peers’) that are currently transferring copies of the requested file. The BitTorrent client uses this information to connect with the peers that have accessible copies of the file, and to commence downloading pieces of the file. While downloading bits of the file from diverse peers, the BitTorrent client will also make bits of the file available to other end users using the BitTorrent protocol. This is called participating in a ‘torrent swarm’. In what is known as a ‘tit for tat’ scheme, the more data an end user makes available to other peers, the faster are that end user's download speeds.

As the trial judge, Cowdroy J, explained, the advantages of the BitTorrent system are as follows:

*The BitTorrent protocol is able to efficiently distribute data because each peer is connected to many other peers, the file is split into many small pieces, and peers download pieces from other peers as well as uploading pieces. The BitTorrent logic operates so as to ensure that the rarest piece in a swarm is the first to be sought after, to average out the availability of pieces and minimize blockage or bottleneck which would occur if there were certain pieces of the file that many peers requested. By this mechanism the traditional problem with the client/server model is obviated. ... in the BitTorrent model, generally speaking, the more people wanting a file and therefore the bigger the swarm, the faster each individual peer receives the file. It is a highly sophisticated and efficient means of distributing data.* ((2010) 263 ALR 215, 234).
AFACT’S INVESTIGATIONS AND NOTICES

The Australian Federation Against Copyright Theft (AFACT) provides services for copyright owners in the film industry, which include investigation and educational services. From 2007, AFACT used the services of DtecNet Software APS (‘DtecNet’), which is currently owned by a Californian company, MarkMonitor, Inc. DtecNet collected data by means of software, known as the DtecNet Agent, which operated much like a BitTorrent client, except that it detects the IP address of computers from which it was able to download requested films. The information collected by DtecNet was stored on secure servers in Copenhagen, then compiled into spreadsheets by the solicitors for copyright owners in the downloaded films. By using DNS lookups, it was possible to determine IP addresses that were allocated to iiNet.

As a result of these investigations, the executive director of AFACT emailed iiNet claiming that its customers were involved with infringing copyright, and attaching a spreadsheet that allegedly identified iiNet subscribers who were ‘repeat infringers’. The email ‘required’ iiNet to take action to prevent continuing infringements, including action available under iiNet’s Customer Relationship Agreement (CRA). The iiNet CRA included the following relevant clause:

4.2 You must not use, or attempt to use, the Service:
(a) to commit an offence, or to infringe another person’s rights;
…
(e) for illegal purpose or practices;
or allow anybody else to do so.

Under another clause of the CRA, iiNet could cancel, suspend or restrict a service on a number of grounds, including if it reasonably suspected illegal conduct.

Thereafter, AFACT sent updated infringement notices on a weekly basis, and also sent DVDs, which included further information uncovered by DtecNet. The notices did not include an explanation of the methodology used by DtecNet to collect information about the alleged infringements.

IIINTERN’S RESPONSE

In response to AFACT’s infringement notices, iiNet pointed to the lack of explanation in the notices as one factor in support of its decision not to take any action against its subscribers. In addition, iiNet pointed out that an IP address does not necessarily identify a person, and that the police were the appropriate authorities to deal with allegations of illegal conduct. In one email, iiNet stated that:

The vigilante approach being promoted by AFACT is rejected by iiNet Ltd ... If AFACT is not willing to invest its own resources to protecting [sic] its rights using the correct channels available iiNet [sic] is not going to. ((2011) 263 ALR 215, 257).

In evidence presented at the trial, it became clear that iiNet had formed the view that no matter how much information was provided by AFACT, it was not going to pass on warning notices to its subscribers.

THE CLAIM

Following iiNet’s consistent refusals to act in response to the AFACT infringement notices, the owners of copyright in particular identified films brought an action against iiNet claiming that it was liable for the copyright infringements of its subscribers by virtue of providing an Internet access service, and failing to take any action in response to the AFACT infringement notices. Additional matters relied upon by the copyright owners included a radio advertisement for iiNet which referred to downloading of episodes of the television program,
The Golden Girls, and a press release issued by iiNet on the day proceedings were commenced against them which stated that iiNet could not disconnect a customer on the basis of a mere allegation.

While, as explained further below, the main claim against iiNet was that it was liable for authorising the infringements committed by its subscribers, the litigation raised a number of complex legal issues, including: how the public communication right is infringed by downloads that use the BitTorrent protocol; whether or not iiNet was prevented from using information about its customers to prevent infringements pursuant to confidentiality provisions of the Telecommunications Act 1997 (Cth); and, if it was determined that iiNet was liable, whether or not the ISP was entitled to protection under what is known as the ‘safe harbour’ regime, which limits the liability of ISPs in certain circumstances. By the time of the appeal to the High Court, the legal issues had narrowed to the question of whether or not iiNet was liable for authorising copyright infringements.

AUTHORISATION LIABILITY

In certain circumstances, a person may be liable for the unlawful actions of another person. This is known as secondary liability. The main form of secondary liability for copyright infringements in English-oriented legal systems is liability for authorising the infringements of another. It is impossible to understand the High Court judgments in iiNet without some background on the complex history of this form of liability.

EARLY HISTORY OF AUTHORISATION

Authorisation, as a separate form of liability, was first introduced by the Copyright Act 1911 (UK), which was adopted in Australia in 1912. Prior to this, it was an infringement, under UK copyright law, for a person to cause an infringing work to be performed or printed. The case law held that a person could only cause another person to infringe copyright if the other person was an employee or an agent. Following the 1911 Act, it has been accepted that liability for authorising infringements extends beyond liability for employees and agents, but there have been differences about the circumstances in which infringing conduct will be found to have been authorised.

As a number of the early cases concerned infringing public performances at venues such as concert halls, the cases were complicated by another provision, also introduced in the 1911 Act, which established liability for a person who, for private profit, permitted a theatre or other place of entertainment to be used for an infringing public performance, unless the person had no reasonable grounds for suspecting that the performance was infringing. Particular difficulties arose in determining whether or not a person who was not actively involved with an infringement, but who was indifferent about infringing behaviour, may have authorised or permitted the infringements.

The early confusion about what is meant by authorisation is illustrated by the reasoning of the English Court of Appeal in Performing Right Society v Ciryl Syndicate ([1924] 1 KB 1). In that case, the defendant, the managing director of a theatrical company, was granted a licence to stage plays at a London theatre, which was leased by the theatrical company. The managing director agreed with the company to produce a play at the theatre, and the company agreed to provide an orchestra to perform during intervals. The copyright owners of two musical works brought an action against both the company and the managing director in relation to infringing performances by the orchestra. On learning of the infringing performances, the copyright owners had written to the managing director, who was overseas at the time, but who denied any involvement in the infringements.

The trial judge, Rowlatt J, held that the managing director was liable for authorising the infringements, even though the orchestra were not his employees or agents. In reaching this conclusion, the judge decided that the managing director had authorised the infringing performances because he had the power to prevent them. But this decision was unanimously
overturned by the English Court of Appeal, which essentially held that the managing director was not liable because the members of the orchestra were neither his employees nor agents.

For the most part, the Court of Appeal in Cyril’s case conflated the reasoning on authorisation liability with the reasoning on permitting a performance, with the judges finding the managing director’s lack of awareness of the infringements especially relevant. Although not essential to the reasoning, Bankes LJ, referring to the managing director’s lack of active involvement in the infringements, acknowledged that ‘indifference, exhibited by acts of commission or omission, may reach a degree from which authorization or permission may be inferred’ ([1924] 1 KB 1, 10). In this case, while it was clear in his responses to the letters from the copyright owners that the managing director was indifferent to potential infringements, Bankes LJ held that, in the absence of agency, it was impossible to infer authorisation or permission from the indifference.

Following Cyril’s case, English courts accepted that the 1911 Act had extended liability beyond the circumstances where another person is an employee or agent. For example, in Evans v Hulton ([1924] All ER 224), Tomlin J rejected a submission that ‘authorise’ meant to sanction the actions of a servant or agent as too narrow, and approved the Oxford Dictionary definition of authorise as ‘to give formal approval to, to sanction, approve, countenance’ (at 225). This broad definition has created difficulties in subsequent cases.

In Falcon v Famous Players ([1926] 2 KB 474) the English Court of Appeal unanimously held that authorisation has a wider meaning than the pre-1911 law, extending beyond employment and agency relations. In that case, the Court had to decide whether or not the American producers of a film, who had imported the film to England and entered an agreement with a cinema owner for the public exhibition of the film, had authorised infringements of the English play on which the film was based.

Holding that the producers had authorised infringing performances, Atkin LJ held that to authorise means ‘to grant or purport to grant to a third person the right to do the act complained of’ (at 499). Applied to the facts, the production company had obviously purposed to grant a right to the cinema owner to show the film. While reaching the same conclusion, Bankes LJ applied the dictionary definition of authorise to conclude that the producers had sanctioned, approved and countenanced the performances (at 491).

Not long after this, the Australian High Court considered similar issues in Adelaide Corporation v APRA ((1928) 40 CLR 481). In that case, APRA claimed that the Adelaide Corporation, which had hired out the Adelaide Town Hall to JC Williamson, was liable for infringing performances of musical works. Although the case was argued on the basis that the defendant was liable for permitting the hall to be used for infringing performances, and not on the basis that it was authorising the performances, the High Court decision has been referred to in many subsequent Australian cases on authorisation liability, including iiNet.

The High Court, in a 3/2 split decision, held that the Adelaide Corporation had not permitted the use of the hall for the performances. The majority reached this conclusion despite the fact that the Corporation was clearly indifferent about the infringing performances: it had ignored correspondence from APRA warning of the potential infringements, and it knew that the offending song would be performed. In the majority, Higgins J held that mere indifference or omission could not be permission, unless it was coupled with both a power to permit the performance and a duty to interfere. In concluding that the Corporation had neither a relevant power nor a duty, he concluded that it had no standing to bring an action against Williamson’s and, effectively, that it had no duty to ‘police’ the Copyright Act on behalf of the copyright owners. Agreeing with Higgins J, Gavan Duffy and Starke JJ, held that the Corporation had no relevant control over the performance, its only power being to terminate the lease.

The dissenting judges in Adelaide Corporation agreed, in broad terms, that a person would permit an infringing performance if they knew, or had reason to suspect, that an infringing performance would occur, they had a legal power to prevent it, and they failed to prevent it. The minority, however, differed in both their interpretation of these criteria, and in the application of the law to the facts. Isaacs J, for example, considered that the Corporation’s
right to terminate the agreement was a relevant power to prevent a performance. In addition, he held that it was not a harsh or unreasonable use of the power of cancellation to insist that Williamson complied with the law. In addition, he differed from the majority in concluding that a failure to prevent a performance may amount to permission even where there is no obligation to prevent the performance.

MOORHOUSE

Prior to iiNet, the main Australian authority on authorisation liability was the High Court decision in University of NSW v Moorhouse ((1975) 133 CLR 1; (1975) 6 ALR 193) (‘Moorhouse’). In that case the Australian author, Frank Moorhouse, claimed that the University of NSW was liable for infringing copies of a short story in his collection, The Americans, Baby, which had been made by a Mr Brennan by use of photocopy machines at the university library. The High Court held that, by providing effectively unsupervised photocopy machines, the university was liable, in the circumstances, for authorising infringements made by people using the machines. As with some of the cases referred to above, the university was not actively involved in the infringements, but was indifferent to any infringements, especially as the copyright information in notices on the photocopy machines was inaccurate and there was no supervision. Although the decision in Moorhouse was unanimous, the two concurring judgments were based on very different reasoning.

Jacobs J (with whom McTiernan ACJ agreed) first held that authorisation extends beyond agency, and has the dictionary meaning of ‘sanction, approve, countenance’ (at 207). Apparently assimilating the analyses of authorisation and permission, he held that authorisation has a ‘wide meaning’, applying both where there is an express permission or invitation to do the infringing act, and where an implied permission or invitation can be inferred from the circumstances. In relation to any implied permission or invitation, Jacobs J approved the statement of Bankes LJ in Cyril’s case that authorisation could be inferred not only from positive acts, but from indifference as shown by acts of omission (at 208). Moreover, he held that, where authorisation is inferred from the circumstances, it is unnecessary to establish that the authorising party knows that a particular infringing act will occur.

Applying this approach to the facts, Jacobs J concluded that, although there was no express invitation to do the infringing acts, by making the photocopy machines available to the public, there was an implied invitation to users to make use of the machines as they saw fit, which extended to infringing copyright in books kept on the library shelves. As the implied invitation to use the machines was not limited to copying that would not infringe copyright, he held that knowledge of infringing acts was irrelevant to whether or not there was an authorisation; knowledge of infringements only being relevant where the invitation was qualified so as not to extend to copyright infringements. Consequently, if the university had effectively qualified the open invitation in either library guides or copyright notices, it might have escaped liability if it could establish that it was unaware the machines were being used to infringe copyright. By providing an unqualified invitation to Brennan to use the machines for photocopying library books, Jacobs J held that the university had authorised the infringements.

Although Gibbs J thought that the case was of ‘limited significance’ (at 199), his judgment played a greater role in the subsequent development of the Australian law that the judgment of Jacobs J. Like Jacobs J, he adopted the dictionary definition of authorisation as ‘sanction, approve, countenance’ (at 200). Beyond this, and relying on the assimilation of ‘authorisation’ and ‘permission’ in Adelaide Corporation, Gibbs J held that authorisation can also mean ‘permit’. Adopting the analysis of permission from Adelaide Corporation, he held that there could be no authorisation of copyright infringement unless there was some power to prevent it. Like Jacobs J, Gibbs J acknowledged that, in some circumstances, authorisation could be inferred from indifference, although he cited Adelaide Corporation as authority for this and not Cyril’s case. But, as opposed to Jacobs J, he held that ‘to authorise’ necessarily includes a mental element, meaning that authorisation cannot be inferred from inactivity
unless the person knows or has reason to suspect that the infringing act will occur (at 200). Following from these principles, Gibbs J drew the conclusion that:

... a person who has under his control the means by which an infringement of copyright may be committed – such as a photocopying machine – and who makes it available to other persons, knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorize any infringement that resulted from its use (at 200-201).

On the facts before the Court, Gibbs J first held that the university made available the means for infringing copyright in the form of the library books and the photocopy machines. Moreover, as the university had control over both access to the books and the machines, it had power to prevent infringements. Secondly, Gibbs J found that the university must have known or suspected that the machines were likely to be used to infringe copyright. Given both the power to prevent infringements, and notice of infringements, he held that it could be inferred that the university authorised infringements, unless it had taken reasonable steps to prevent infringements.

As the university guides provided to students were inadequate, the notices on the machines were inaccurate and there was no effective supervision of the machines, Gibbs J held that the cumulative measures taken by university were not reasonable steps to prevent infringements. In particular, although he did not go so far as to find that adequate notices would have excused liability, he stated that ‘the fatal weakness in the case for the University is the fact that no adequate notice was placed on the machines for the purpose of preventing infringements of copyright’ (at 204). Therefore, as Gibbs J found that, as the university had (by providing the means for infringing copyright) the power to prevent infringements, knew or suspected that the machines were being used to infringe copyright, and had taken no reasonable steps to prevent infringements occurring, he concluded that it was liable for authorising infringements.6

ENGLISH LAW

In Moorhouse, therefore, the Australian High Court adopted an expansive interpretation of authorisation which extended beyond the test proposed by Atkin LJ in Falcon v Famous Players, that to authorise an infringement means to grant or purport to grant the right to do that act. Even on the approach of Jacobs J in Moorhouse, the Australian approach is broader, as an invitation does not necessarily imply that a person is granting a right.7 This has led to a divergence between English and Australian law.

The meaning of authorisation under English law first came before the House of Lords in CBS Songs v Amstrad ([1988] AC 1013; 12 IPR 1). In that case, the copyright owners of musical works and sound recordings alleged that Amstrad, which manufactured and sold consumer tape recording equipment, was liable for authorising infringements committed by the use of the equipment, by virtue of either supplying the equipment to the public or advertising the capabilities of the recorders.

Lord Templeman held first that, although selling the recorders might facilitate copyright infringement, it did not amount to authorising infringements. The position in relation to the advertisements was less clear-cut, as Amstrad had, for example, highlighted the ability to make duplicate cassettes. Lord Templeman, however, held that the advertisements fell short of sanctioning, approving or countenancing infringements (at 1054). More significantly, adopting Atkin LJ’s interpretation of authorisation, he held that it was impossible for consumers to infer that Amstrad possessed, or purported to possess, the authority to grant the right to make copies (at 1053). As Lord Templeman put it, ‘Amstrad conferred on the purchaser the power to copy but did not grant or purport to grant the right to copy’ (at 1054). Referring to the approach adopted by Gibbs J in Moorhouse, without expressly endorsing it, he observed that Amstrad had no control over the use of the machines once they were sold.
As suggested by Lord Templeman, in many cases, the application of the different approaches adopted under Australian and English law would not necessarily result in different conclusions. In *Australian Tape Manufacturers v Commonwealth* ((1993) 176 CLR 480), for example, in the course of determining whether or not a levy imposed on blank tapes was constitutional, the High Court considered whether or not the sale of blank tapes would infringe copyright. Referring to *CBS v Amstrad*, Mason CJ, Brennan, Deane and Gaudron JJ held that the manufacture and sale of consumer equipment, such as blank tapes and video recorders, would not amount to an authorisation of infringements committed by use of this equipment, even if the manufacturer or vendor knew or suspected that the equipment would be used for this purpose as, once sold, the manufacturer or vendor had no effective control over the equipment (at 498).

Applying the narrow English approach, however, it is doubtful whether the university in *Moorhouse* could be regarded as purporting to grant a right to infringe. In fact the approach adopted to authorisation in *Moorhouse*, and especially the reasoning of Gibbs J, is broader than in other common law jurisdictions. In particular, in *CCH Canadian v Law Society of Upper Canada* ((2004) 236 DLR (4th) 395) (‘CCH’), the Canadian Supreme Court criticised *Moorhouse*, on the basis that it ‘shifts the balance in copyright too far in favour of the owner's rights and unnecessarily interferes with the proper use of copyrighted works for the good of society as a whole’ (at [41]).

**POST-MOORHOUSE AUSTRALIAN LAW REFORM**

With the emergence of the Internet in the mid-1990s, attention focussed on uncertainty about the potential liability of intermediaries, such as ISPs, for copyright infringements committed by end users. At the international level, these concerns led to the adoption of an Agreed Statement to the 1996 WIPO Copyright Treaty (the ‘WCT’) that:

> It 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.

This agreed statement relates to Article 8 of the WCT, which established a new right of communication to the public (see Samuelson 1997; Lindsay 2000). The debates at the 1996 Geneva conference that led to the WCT provide the background to national laws that were subsequently introduced to regulate the liability of online service providers, such as ISPs.

Law reform of the regime regulating liability of online intermediaries for copyright infringements occurred in two main stages. First, the Digital Agenda reforms of 2000, which came into effect in 2001, attempted to provide a degree of certainty by partially codifying authorisation liability and introducing a defence for facilities providers. Secondly, pursuant to the Australia-US Free Trade Agreement, a regime, modelled on the US ‘safe harbour’ regime, was introduced in 2005 to limit the liability of certain Internet intermediaries.

According to the Explanatory Memorandum (EM) to the Digital Agenda Bill, the reforms to the liability of Internet intermediaries, such as ISPs, were designed to provide ‘greater certainty about the responsibilities of carriers and ISPs to copyright owners and the steps they need to take to avoid infringing copyright’ (EM, Outline). With this in view, the reforms introduced new sections 36(1A) and 101(1A) to the Copyright Act, which listed the following three non-exclusive factors, which must be taken into account in determining whether or not a person has authorised an infringing act:

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

(b) the nature of any relationship existing between the person and the person who did the act concerned;

(c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry code of practice.
As the EM pointed out, this was intended, in part, to give statutory form to common law principles relating to the meaning of authorisation, especially as interpreted by Gibbs J in *Moorhouse*. Following from the overall objectives of the reforms, the EM further explained the objectives of the partial codification of the list of factors as follows:

They are intended to provide a degree of legislative certainty about liability for authorising infringements. Additional certainty in relation to third party liability for copyright infringement is provided by new s. 36(1A)(c). This paragraph specifies that compliance with relevant industry codes of practice is a factor in determining whether the person took reasonable steps to prevent or avoid the infringement (EM, para 56).

Given the different approaches taken by the courts to the meaning of authorisation, and especially the differences between the two judgments in the *Moorhouse* case, explained above, an attempt to codify the common law was never going to be straightforward. Moreover, rather than adding certainty, the partial codification clearly incorporates the reasoning of Gibbs J in *Moorhouse*, while effectively ignoring the very different reasoning of Jacobs J, who was in the majority in that case. By codifying one approach to the interpretation of authorisation, while asserting that the reform was not intended to alter the common law, the legislation created a potential dilemma for courts required to apply the partial codification: how to reconcile the new legislatively mandated factors with alternative interpretations, and especially the approach applied in the Jacobs J judgment? Prior to the *iiNet* litigation, however, the courts tended to gloss over this problem, and generally simply applied the Gibbs J approach.

Despite the weaknesses with the Australian reforms, greater certainty could have been achieved for carriers and ISPs if, as clearly anticipated by the reforms, the industry had developed a code of practice, which clarified industry obligations. As explained in the judgment of Jagot J in the Full Federal Court in *iiNet*, following the reforms, voluntary discussions took place between representatives of large copyright owners and the Internet Industry Association (IIA), which represents ISPs, with a view to developing a code, but these negotiations broke down. As the judgment further explained, by mid-2007, AFACT had concluded that there was no point in continuing negotiations as the IIA’s position was that no ISP ‘should be required to take action against their subscribers who are engaging in copyright infringement over their networks’ ((2011) 275 ALR 1, 64). The combination of the imperfectly drafted and poorly explained partial codification, and the failure of industry to develop a code, meant that it was unlikely that the main objective of the reforms – greater certainty for carriers and ISPs – would be achieved.

If anything, the second relevant reform introduced by the Digital Agenda reforms increased the uncertainty relating to ISP liability. The amendment, which was based on the Agreed Statement to the WCT extracted above, introduced a defence to authorisation liability for a person who does no more than provide communications facilities. As set out in sections 39B and 112E of the Copyright Act, the defence provides that:

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 ... merely because another person uses the facilities so provided to do something the right to do which is included in the copyright.

As explained by the EM to the Bill, the defence was intended to have ‘the effect of expressly limiting the liability of carriers and carriage service providers for authorisations of copyright infringements on their networks’ (EM, para 59). The problem created by the defence was that, in order to be given some practical operation, it raised the possibility that it might have the effect of making a facilities provider liable for infringements committed by use of its facilities even where it does no more than provide those facilities. Otherwise, the defence would provide protection where none was needed.
The liability regime applying to Internet intermediaries was further complicated by the detailed scheme, known as the ‘safe harbour’ regime, which was introduced to comply with obligations under the Australia-US Free Trade Agreement, and which came into effect on 1 January 2005. While the regime does not provide a complete defence for carriage service providers, such as ISPs, it limits their liability for copyright infringements that occur in the course of carrying out certain activities – known as Category A-D activities – provided that the intermediary complies with specific statutory conditions that relate to that activity. In relation to all categories of activity, to be entitled to limited liability, the intermediary must comply with the following two conditions:

- adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers; and
- comply with relevant provisions of any industry code that relate to not interfering with standard technical measures used to protect and identify copyright material.

For those such as iiNet providing transmission and connectivity services, the specific, Category A conditions were limited and easily satisfied when simply carrying transmissions initiated by others.

As no industry code has been adopted, the second condition does not apply. Accordingly, the most important condition is the requirement to adopt and implement a repeat-infringer policy.

As the EM to the Bill that introduced the ‘safe harbour’ regime made clear, failure to qualify for the regime, such as a failure to comply with the conditions, does not mean that the intermediary is liable for copyright infringement, as a copyright owner must still establish that the intermediary has infringed copyright. The concomitant of this is that, the combination of the Digital Agenda reforms and the ‘safe harbour’ regime means that a complex, tiered regime applies in determining the liability of Internet intermediaries for copyright infringements committed by end users: first, it must be established that the intermediary is liable for authorising the infringements; secondly, it must be determined whether or not the intermediary is entitled to the facilities provider defence; and, thirdly, if the intermediary is liable, and the defence does not apply, the availability of the ‘safe harbour’ regime must be examined. The iiNet litigation tested each of these aspects of the tiered liability regime.

**iiNet**

In *iiNet*, the High Court unanimously held that iiNet was not liable for authorising copyright infringements committed by its end users and, in doing so, confirmed the decisions of the trial judge and of the majority of the Full Federal Court. Although the same conclusions were reached by 8 of the 9 judges who considered the case, there are significant differences in the reasoning of the judgments leading to these conclusions. This section of the article briefly explains the reasoning of the judgments in the Federal Court, before moving to a more detailed explanation of the two judgments delivered in the High Court.

**Cowdroy J**

At first instance, Cowdroy J essentially held that iiNet had not authorised the end-user infringements as it did not provide the ‘true means’ of infringement, but merely a ‘necessary precondition’ of infringement, in the form of Internet access. In addition, he concluded that iiNet did not have a relevant power to prevent infringements as, despite the existence of a contractual power to terminate an access service, termination or suspension of a service would not, in the circumstances, be a reasonable step. On these points, Cowdroy J’s reasoning has been criticised by commentators on the basis that it is contrary to established precedent (Brennan 2010; Lindsay 2010) and, for this reason, it was not followed on appeal.
THE FULL FEDERAL COURT

The Full Federal Court, by a 2/1 majority, confirmed that iiNet had not authorised the end-user infringements, but adopted a more conventional analysis of authorisation liability than that applied by Cowdroy J in reaching this conclusion. Explaining the legal regime that applies to intermediaries, such as iiNet, Emmett J, who was in the majority, applied the partial codification in s 101(1A), together with the reasoning in Moorhouse, to endorse the following analytical steps:

- Identify the acts that constitute infringement of copyright;
- Identify what was done by the alleged authoriser in relation to those infringing acts;
- Consider each of the three matters referred to in the partial codification (s 101(1A)); and
- Consider the facilities provider defence (s 112E) ((2011) 275 ALR 1, 40).

In applying this analysis, Emmett J first held that iiNet had a power to prevent infringements by use of its service in the form of a right to terminate the Customer Relationship Agreement (CRA) with its customers, as well as the technical capability to suspend and terminate accounts ((2011) 275 ALR 1, 43). The key consideration, however, leading him to conclude that iiNet had not authorised end-user copyright infringements, was that, in the circumstances, issuing warnings to subscribers and, ultimately, suspension or termination of a subscriber’s account were not reasonable steps. In particular, Emmett J considered that the information provided in the AFACT infringement notices was inadequate for it to be reasonable to require iiNet to take such steps. In this respect, he said that ‘(i)t was not reasonable to require iiNet to undertake the immense amount of work, cost and effort required in order to set out, review and analyse the allegations in the information provided in the infringement notices ((2011) 275 ALR 1, 47).

Over and above this analysis, in the absence of an applicable industry code, Emmett J went on to set out, in some detail, the circumstances in which he considered it would be reasonable to require an ISP to take steps such as suspending or terminating a subscriber’s account. In addition to providing an ISP with sufficient information to allow it to independently verify the allegations made in infringement notices, Emmett J considered that, in order for suspension or termination to be reasonable, copyright owners must undertake to reimburse an ISP for the reasonable costs of verifying the allegations, and to indemnify the ISP for any liabilities arising from mistakenly suspending or terminating a service ((2011) 275 ALR 1, 48-9).

Nicholas J agreed with Emmett J that iiNet was not liable for authorising end-user infringements as, in the circumstances, a failure to issue warning notices, or suspend or terminate accounts, was not unreasonable, especially given the inadequacies with the AFACT notices ((2011) 275 ALR 1, 173). While he also agreed with Emmett J that, if the notices contained adequate information, it might be reasonable to expect an ISP to issue warning notices, and to suspend or terminate accounts, he considered that, in the absence of an industry code, ISPs should be given ‘considerable latitude’ in working out how to respond to infringement notices ((2011) 275 ALR 1, 167). In this respect, Nicholas J considered that an ISP could escape liability if it acted in good faith to take steps against subscribers that it was satisfied had used its facilities for flagrant infringements.

As opposed to the majority, Jagot J was the only judge to consider the issue to conclude that, in the circumstances, iiNet had authorised the infringements committed by its customers. The main reason for Jagot J coming to a contrary conclusion to the majority was that she formed the view that the AFACT infringement notices were sufficiently detailed to require a response from iiNet. Moreover, in reaching the conclusion that iiNet had authorised the infringements, Jagot J rejected an argument, accepted by Cowdroy J, that the judgment of Higgins J in Adelaide Corporation meant that a contractual power to completely terminate a relationship was not a relevant power to prevent infringements. On this point, she effectively concluded that the wording of s 101(1A)(a) - which refers to ‘the extent (if any)’ of a power to prevent – meant that it extended to an absolute power to prevent, such as the termination of a legal relationship ((2011) 275 ALR 1, 100). Finally, Jagot J held that this case could be
distinguished from *Adelaide Corporation* because iiNet’s responses to AFACT, including that it was clear that there were no circumstances in which iiNet was prepared to take action, and the press release issued on the day that proceedings indicating that it had no obligations to disconnect subscribers, went beyond mere indifference to at least ‘tacit approval’ ((2011) 275 ALR 1, 110).

**THE HIGH COURT**

In two concurring judgments – delivered by French CJ, Crennan and Kiefel JJ (the ‘French judgment’) on the one hand, and Gummow and Hayne JJ (the ‘Gummow judgment’), on the other – the High Court unanimously dismissed an appeal against the decision of the Full Federal Court. In concluding that iiNet had not authorised infringements, the two judgments only addressed questions relating to authorisation liability and the facilities provider defence, with other issues, including the potential application of the ‘safe harbour’ regime, not being subject to the appeal. Although the two judgments agree on the general approach to be applied in determining whether or not a person is liable for authorising infringements, there are significant differences in the detailed reasoning.

**The French judgment**

The French judgment, which is less detailed than the Gummow judgment, commences its explanation of authorisation with a survey of the relevant case law, much of which is dealt with above. In the course of this survey, the judgment, without citing the source of its analysis, affirms a distinction drawn by Laddie (2000, 1773), between a wide and a narrow meaning of authorisation, derived from the judgments of Bankes LJ and Atkins LJ, respectively, in *Falcon v Famous Players*. As explained above, while Bankes LJ adopted a dictionary definition of authorise as ‘sanction, approve, and countenance’ – which Laddie describes as the wide meaning - Atkins LJ proposed the test eventually applied by the House of Lords in *CBS Songs v Amstrad*, that to authorise means to grant or purport to grant the right to do an infringing act – which Laddie describes as the narrow meaning. Following this, the judgment referred to the distinction drawn by Higgins J, in *Adelaide Corporation*, in his analysis of the meaning of ‘permit’, again explained above, between a direct power to prevent infringements and an indirect power, such as by terminating a contractual relationship.

These two observations form the background to the judgment’s relatively brief analysis of the application of the law to iiNet’s alleged indifference to the AFACT infringement notices. The starting point for the analysis is the proposition that the main inquiry involves applying the three factors required to be taken into account by the partial codification, which the judgment, referring to observations made by Gavan Duffy and Starke JJ in *Adelaide Corporation*, characterises as ‘largely questions of fact’ ((2012) 286 ALR 466, 483).

In analysing the first factor, iiNet’s power to prevent infringements, the French judgment distinguished between iiNet’s technical power over infringing conduct and its contractual power to suspend or terminate an Internet access service. In relation to iiNet’s technical power, the judgment observed that iiNet has no power over the BitTorrent system, and nor can it monitor infringements by use of BitTorrent. Consequently, the judgment concludes that iiNet had no direct technical power to prevent a customer from infringing copyright by using the BitTorrent system.

Examining iiNet’s contractual power to prevent infringements, the French judgment pointed out that the provision in the iiNet CRA stating that the service must not be used ‘to commit an offence or to infringe another person’s rights’ meant that iiNet was ‘not thereby purporting to grant to the customer any right to use the internet to infringe another person’s rights’ ((2012) 286 ALR 466, 483). While not expressly saying so it seems, from this, that the judgment concluded that the narrow-Atkins LJ test for authorisation could not be satisfied.

Turning to the wide test, of ‘sanction, approve, countenance’, the judgment apparently accepted that it could be argued that iiNet had ‘countenanced’ infringements, on some meanings of that term. Nevertheless, adopting comments in UK and Canadian authorities, including *CBS v Amstrad* and *CCH*, the French judgment points out that not all meanings of
‘countenance’ are co-extensive with authorisation. Moreover, the judgment casts doubt on the use of dictionary definitions to determine the meaning of authorisation, referring to ‘the danger in placing reliance on one of the synonyms for “authorise” to be found in a dictionary’ (2012) 286 ALR 466, 484). Returning to iiNet’s contractual power, the French judgment observed that there was no direct power to prevent individual infringements, with the power consisting only of an indirect power to terminate the contractual relationship. Consequently, although iiNet had some technical and contractual power to prevent infringements, its powers were limited and indirect.

The French judgment emphasised the limited and indirect nature of iiNet’s power over its customers’ activities in its analysis of the third of the non-exclusive factors required to be taken into account: whether or not iiNet had taken reasonable steps. The main focus of the judgment’s analysis of this factor was whether or not, in the circumstances, it would be reasonable to require iiNet to issue warnings to its customers. The judgment identified three considerations as relevant to its conclusion that this would not be a reasonable step: any warning notices would not be effective, as a customer could simply engage another ISP; in order to determine whether or not a warning was effective, iiNet would need to understand and apply the DtecNet methodology for detecting infringements, and the AFACt notices were inadequate for this purpose; and terminating, or threatening to terminate, a customer’s Internet service would expose iiNet to liability for wrongful termination. On the last point, the French judgment, apparently referring to both the serious consequences of terminating a customer’s account and the problems of an ISP making a determination about whether or not a customer has infringed copyright, stated:

These considerations highlight the danger to an ISP, which is neither a copyright owner nor a licensee, which terminates (or threatens to terminate) a customer’s internet service in the absence of any industry protocol binding on all ISPs, or any, even interim, curial assessment of relevant matters. ((2012) 286 ALR 466, 485).

Following from this analysis, the French judgment concluded that iiNet’s inactivity, on receipt of the AFACt infringement notices, was based not on indifference about the infringements of copyright, but on an assessment of the risks of taking steps against its customers on the basis only of the information in the AFACt notices. In a sense, then, the French judgment, like the judgments of the majority in the Full Federal Court, is based upon the conclusion that the information in the AFACt notices was insufficient for it to be reasonable for iiNet to issue warning notices. Over and above this, however, the difficulties noted in the judgment relating to the ineffectiveness of warning notices, and the burdens imposed on ISPs to determine whether or not a customer was continuing to infringe copyright, strongly suggest that, on this analysis, there are no circumstances, short of active promotion or encouragement, in which an ISP could, in providing an Internet access service, be liable for end-user infringements.

This assessment is reinforced by the conclusion reached by the judgment on the narrow English test for authorisation, that it would be impossible for iiNet’s customers to infer from the ISP’s inactivity that it was in a position to grant a right to do any of the acts that would infringe copyright. It is further reinforced by the way in which the French judgment concludes with an apparent call for a legislative scheme for dealing with the problem of P2P file sharing, based on the statement that, ‘the concept and the principles of the statutory tort of authorisation of copyright infringement are not readily suited to enforcing the rights of copyright owners in respect of widespread infringements occasioned by peer-to-peer file sharing, as occurs with the BitTorrent system’ ((2012) 286 ALR 466, 486).

The Gummow judgment

Like the French judgment, the Gummow judgment includes a survey of the case law on authorisation liability; but the reasoning in the Gummow judgment is much more complex than the reasoning in the French judgment. The judgment’s analysis of the law relating to authorisation initially focuses on two issues: the extent to which liability might arise from an omission to take action and, relatedly, the extent to which a person might have a duty to prevent infringements.
As explained above, in Cyril’s case, Bankes LJ had stated that authorisation might be inferred from indifference as shown by an omission to act, a statement that was subsequently adopted by Jacobs J (and, arguably, also by Gibbs J) in Moorhouse. The Gummow judgment, however, appears to reject the relevance of Cyril’s case to authorisation liability, as it concludes that the primary current significance of that case in Australia lies in its treatment of the liability of directors for the wrongful acts of a company ((2012) 286 ALR 466, 491). This casts some doubt on the extent to which liability may arise from inactivity although, as explained below, the judgment does not question the decision in Moorhouse.

Associated with this, the Gummow judgment places some emphasis on a general principle of tort law – the area of the law relating to non-contractual civil wrongs – that, in the absence of a special relationship, the law is reluctant to impose a positive duty on a person to control the activities of another person so as to prevent harm to a third person ((2012) 286 ALR 466, 492). Relying on an analogy, drawn by Landes and Posner (2003), between secondary liability for copyright infringement and the tort of inducing a breach of contract, the judgment concludes that, as a general principle, there can be no liability from a failure to prevent a wrongful act without either actual knowledge of the wrongful act or, at least, constructive knowledge ((2012) 286 ALR 466, 492).

Turning from the analysis of liability arising from an omission to act, the Gummow judgment considered that the argument for imposing liability on iiNet was essentially equivalent to imposing liability for negligence, in the sense that it would amount to imposing a duty of care on ISPs to prevent harms to copyright owners. Rejecting this form of liability, the judgment concluded that such a wide duty would create an impermissibly uncertain legal standard for ISPs. Moreover, on this point, the judgment was concerned that termination or suspension of a subscriber’s Internet account would not be a remedy available to copyright owners if end-users were sued directly.

In the course of this analysis which, drawing from general principles of tort law, clearly cuts down the scope of authorisation liability previously accepted in Australia, and especially as accepted by Gibbs J in Moorhouse, the Gummow judgment addressed the role of the facilities provider defence in section 112E. Rejecting the argument that the defence assumes that an ISP might be liable merely by providing facilities, the judgment approved the view of Nicholas J in the Full Federal Court, that the defence was introduced from ‘an abundance of caution’, meaning that it has no operative effect whatsoever ((2012) 286 ALR 466, 493).

While, as explained above, the French judgment drew a distinction between the wide and narrow meanings that had been attributed to authorisation, the Gummow judgment identified a third approach to authorisation liability, which was the subject of a 2011 article by Lim (Lim 2011). This approach, which can be traced to Lord Templeman’s judgment in CBS v Amstrad, is essentially that authorisation will be found where, according to Lim, a person sells, supplies or hires out items that ‘could only or predominantly be used for infringing purposes’ (Lim 2011, 100). In Amstrad, Lord Templeman had explained the facts in Evans v Hulton, where the defendant sold rights to publish a manuscript in which he did not have the copyright, and in Falcon v Famous Players, in which a film based on the plaintiff’s play was hired out to a cinema, as examples of conduct that was ‘bound to infringe’.

The main significance of this third, ‘bound to infringe’ approach, is that it might lead to a finding of authorisation, even where the defendant has no control over the actual use of the item or service. As an example of its practical operation, while the provision of a P2P file sharing service might be interpreted as being ‘bound to infringe’, the provision of an Internet access service, such as that supplied by iiNet, and which could be used for many lawful purposes, would not be ‘bound to infringe’. As opposed to Lim’s analysis of this as a distinct approach to liability, however, in Amstrad, Lord Templeman seemed to regard this as subsidiary to the analysis of whether or not there was a grant, or purported grant, of a right to do an infringing act. The Gummow judgment therefore represents the first time that a court has clearly adopted the ‘bound to infringe’ theory as a potentially distinct (as opposed to subsidiary) basis for authorisation liability.
Turning to the Australian authorities, the Gummow judgment acknowledged that, in cases such as *Moorhouse*, it had been accepted, first, that authorisation extends beyond an employment or agency relationship and, secondly, that the courts had applied the dictionary definition of ‘sanction, approve, countenance’. Like the French judgment, the Gummow judgment doubts the usefulness of the dictionary definition and specifically cautions against the application of a broad approach to the meaning of ‘countenance’ to expand the scope of authorisation ((2012) 286 ALR 466, 495). On this point, the judgment specifically states that:

> After a century, the selection of the term “authorise” to identify the activity constituting secondary infringement continues to give rise to difficulty. But the difficulties, which reflect both technological developments and changes to business methods are unlikely to be resolved merely by recourse to a dictionary. ((2012) 286 ALR 466, 494).

Furthermore, the judgment points out that, in *Falcon v Famous Players*, Atkin LJ had not joined with Bankes LJ in adopting the dictionary definition. In this respect, then, the Gummow judgment, like the French judgment, seems to prefer the narrow English test for authorisation.

Finally, in rejecting the use of the term ‘countenance’ to extend liability, the judgment emphasised that, in *Moorhouse*, where Jacobs J had adopted the dictionary definition, it was considered relevant, in both judgments, that the university controlled not only the photocopying machines, but also access to the library books. The implication of this analysis is that, while provision of photocopying machines, without any steps to control their use, might be regarded as ‘countenancing’ infringements committed by the use of the machines, something additional is required in order to establish that the infringements have been authorised. Applying this to the facts in *iiNet*, the Gummow judgment apparently accepts that *Moorhouse* could be distinguished as, in that case, the university had control of the library books (in addition to the photocopying machines), whereas in *iiNet*, the ISP had no control of the BitTorrent protocol ((2012) 286 ALR 466, 497).

The Gummow judgment, like the French judgment, therefore apparently endorses the test formulated by Atkins LJ, and adopted by the House of Lords in *Amstrad*, that to authorise means to grant, or purport to grant, a right to do an act comprised in the copyright. In addition, the judgment appears to accept that, apart from the narrow English test, infringements will be authorised by a person who provides an item or service that is ‘bound to infringe’. An obvious difficulty confronting the adoption of a narrow interpretation of authorisation under Australian law, however, is the statutory endorsement of the much wider interpretation of Gibbs J in *Moorhouse*, by the partial codification in sections 36(1A) and 101(1A). The Gummow judgment refers to the difficulties in reconciling a narrow approach to authorisation with s 101(1A) in stating that:

> A further element of complexity for this appeal has been provided by an addition to s 101 of the Act apparently made as some further and general legislative response to Moorhouse. ((2012) 286 ALR 466, 497).

From this comment, it might be inferred that the judgment would prefer for the law in this area to be developed by the courts, and not to be confined by legislative attempts at codification.

Nevertheless, given the mandatory statutory criteria, following the analysis of the common law meaning of authorisation, the Gummow judgment concludes by dutifully (if grudgingly) applying the factors in the partial codification. First, in examining *iiNet*’s alleged power to prevent infringements, the judgment essentially agreed with the French judgment that, while there was some power, this was limited (or ‘attenuated’), as *iiNet* had no direct control over the use of the BitTorrent system. Secondly, the Gummow judgment concluded that suspending or terminating subscribers’ accounts would not be not reasonable steps, essentially for the same reasons as those given in the French judgment. Thus, like the French judgment, the Gummow judgment questioned the effectiveness of warning notices and considered that it would not be reasonable to require *iiNet* to take action based on the inadequate explanations
in the AFACT notices. Furthermore, acknowledging that the only practical step that iiNet could take to effectively prevent infringements would be to terminate the contractual relationship with its customers, the judgment concluded that this would be an over-reaction, as it would extend to preventing use of the iiNet service for non-infringing activities, and as customers could readily evade it, by simply engaging another ISP.

Returning to the claim, based on the statements of Bankes LJ in *Cyril’s case*, that iiNet’s apparent indifference reached the level where authorisation could be inferred, the Gummow judgment concluded that any indifference to copyright infringements on the part of iiNet was that of a party that did not consider it was their business to interfere, as infringements were a matter for the copyright owner, and not the sort of indifference that might result in liability. In reaching this conclusion, the judgment expressly rejected Jagot J’s conclusion that iiNet had at least tacitly approved infringements, on the basis that iiNet’s press release was meant to communicate its intention to defend the action, and not approval of infringing conduct ((2012) 286 ALR 466, 499). Finally, applying the one clear basis on which it accepts that authorisation may arise from a failure to act – that the activity or service is ‘bound to infringe’ – the judgment concluded that iiNet’s business of providing Internet access was not ‘bound’ to result in copyright infringements ((2012) 286 ALR 466, 500).

**IMPLICATIONS OF iiNET**

The decision of the High Court in *iiNet* has important implications both for the regime applying to the liability of Internet intermediaries, and especially ISPs, for copyright infringements committed by end-users and, more generally, for authorisation liability for copyright infringement. This concluding section of the article explains and analyses both of these issues.

**IMPLICATIONS FOR ISP LIABILITY**

The decision in *iiNet* has clarified the extent to which ISPs may be found liable for copyright infringements committed by their customers, such as by means of P2P file-sharing systems. In general, in the absence of any positive steps that actively incite infringements, ISPs that provide Internet access (as opposed, for example, to hosting services) will not be liable for authorising copyright infringements committed by their subscribers (or those using their accounts).

The essential reasons for this conclusion, which are common to both judgments in the case, arise from the analysis applied to the mandatory statutory factors in the partial codification of authorisation liability. First, in relation to an ISP’s power to prevent end-user infringements, both the technical power to control infringements, such as by means of the BitTorrent system, and the contractual power over users, is limited and indirect. Although both the French and Gummow judgments seem to acknowledge that the right to terminate the contractual relationship with customers confers some power, both agree that this is merely an indirect power and, therefore, apparently of limited significance.

Secondly, both judgments agree that, in the circumstances of the case, issuing warning notices to customers and, ultimately, suspending or terminating customer accounts, were not reasonable steps. While the judgments in the High Court agree with the majority of the Full Federal Court that the inadequacies of the AFACT notices, and especially their failure to disclose the methodology used to detect infringements, meant that it was not reasonable for iiNet to rely on them, the two judgments go some way beyond this. Thus, both judgments seriously question the effectiveness of sending warning notices to customers, at least in circumstances where other ISPs do not apply, or are not bound by, similar policies. Furthermore, while the French judgment was concerned with the extent to which actions taken by iiNet might expose it to liability for wrongful termination of its contract with a customer, the Gummow judgment was clearly concerned that termination of Internet access might be a disproportionate response, which would not be available to copyright owners in actions brought directly against the primary infringers. Consequently, even if copyright
owners were to take the steps proposed by Emmett J in the Full Federal Court – by including adequate information in infringement notices, by compensating ISPs for their costs, and by indemnifying ISPs for wrongful termination – applying the analysis common to both High Court judgments, an ISP would still not be liable for authorising infringements.

This interpretation of the High Court judgments is confirmed by important statements in both judgments that question the suitability of authorisation liability as a means for dealing with copyright infringements by means of P2P file-sharing systems. Thus, the French judgment concludes with the statement:

... 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. ((2012) 286 ALR 466, 486).

Similarly, the Gummow judgment states that:

The history of the [Copyright] Act since 1968 shows that the Parliament is more responsive to pressures for change to accommodate new circumstances than in the past. Those pressures are best resolved by legislative processes rather than by any extreme exercise in statutory interpretation by judicial decisions. ((2012) 286 ALR 466, 494).

Interestingly, a similar conclusion was reached, although in stronger terms, by Charleton J of the Irish High Court in EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd, who stated that:

Legislative intervention is required, if the Oireachtas ... [Parliament] ... see fit, to protect constitutional rights to copyright and foster the national resource of creativity. ([2010] IEHC 377 at [131]).

The clear consequence of this analysis is that, if ISPs in Australia are going to have any involvement in dealing with the problem of infringements committed by P2P file-sharing systems, it will have to be either as a result of obligations imposed by a voluntary industry code of practice, or a new statutory ‘graduated response’ regime. The problem with the first option is precisely that which compromised the reliance placed on industry codes in both the Digital Agenda reforms and the ‘safe harbour’ regime: that, in the absence of any real possibility that ISPs will be found liable, there is no statutory incentive for them to voluntarily assume obligations under a non-mandatory industry code. At the same time, however, the absence of a statutory regime has not prevented the introduction of a voluntary regime in the US.

While it may now be left to the legislature to determine whether or not it is desirable to introduce a ‘graduated response’ regime in Australia, the legal conclusions reached by the High Court expose inconsistencies in the current regime that governs the liability of Internet intermediaries, such as ISPs. First, as explained above, it might be assumed that the facilities provider defence, in sections 39B and 112E of the Copyright Act, is premised on an assumption that ISPs may be liable for authorising infringements merely by virtue of providing communications facilities. Both judgments in the High Court, however, agreed that these provisions introduced a defence where none is needed, as there are no circumstances in which an intermediary, such as an ISP, that provides communications facilities, can be liable, merely by virtue of that provision, for authorising infringements ((2012) 286 ALR 466, 474; 493).

It could also be argued that the ‘safe harbour’ regime, in so far as it applies to what are known as category A activities, assumes that intermediaries like ISPs may face liability for copyright infringements. As explained above, the ‘safe harbour’ regime limits the liability of an ISP in relation to certain activities provided the ISP complies with certain conditions. Relevantly, section 116AC of the Copyright Act defines a category A activity as ‘providing facilities or services for transmitting, routing or providing connections for copyright material, or the intermediate and transient storage of copyright material in the course of transmission, routing
or provision of connections’. As further explained above, the conditions that must be
complied with by ISPs undertaking category A activities include adopting, and reasonably
implementing, a policy that provides for termination, in appropriate circumstances, of the
accounts of repeat infringers.

The reasoning of the two High Court judgments in iiNet, which collectively mean that it is
difficult to envisage any realistic circumstances in which an ISP that undertakes category A
activities will be liable for the copyright infringements of end-users, effectively removes any
statutory incentive for ISPs to comply with the conditions that apply to category A activities,
including the adoption of a repeat infringer policy. The clear implication of the conclusions
reached by the High Court is, therefore, that the elements of the current regime regulating ISP
liability – the partial codification of authorisation liability, the facilities provider defence and
the ‘safe harbour’ regime – were introduced with insufficient understanding of how these
provisions would apply to ISPs, leading to some incoherence.

**IMPLICATIONS FOR AUTHORISATION LIABILITY**

While the High Court judgments in iiNet have clarified the liability of ISPs for end-user
copyright infringements, the reasoning in the judgments, and potential inconsistencies
between the judgments, have the potential to significantly increase the uncertainty about the
meaning and scope of authorisation under Australian law. Some of this uncertainty results
from issues on which there is substantial agreement between the judgments.

First, the judgments both reject the usefulness of resorting to dictionary definitions of
‘authorise’ and, in particular, reject recourse to the wider meanings of the term ‘countenance’.
Similarly, in *Amstrad Consumer Electronics PLC v British Phonographic Industry Ltd*,
Lawton LJ, in the English Court of Appeal, also rejected the use of dictionary meanings and,
in doing so, referred to Atkin LJ’s formulation, stating that, ‘this comes much nearer to my
understanding of the meaning of the word “authorise” than the synonyms approved by Bankes
LJ and the High Court of Australia’ ([1986] FSR 159, 207). The rejection of dictionary
definitions by both judgments in iiNet therefore seems to imply a rejection of what Laddie
referred to as the wide English meaning of authorisation. This interpretation is confirmed by
the apparent approval of Lawton LJ’s judgment on this issue by Gummow J in a 1987

Secondly, and consistently with the first point, both judgments prefer the narrow Atkin LJ
interpretation of to ‘authorise’ as to grant, or purport to grant, a right to do the infringing act.
Thus, the French judgment expressly states that iiNet’s customers could not draw an inference
from either iiNet’s refusal to act or its press release ‘that iiNet was in a position to grant those
customers rights to make the appellants’ films available online’ ((2012) 286 ALR 466, 485).
The Gummow judgment, while not expressly referring to the narrow test in its conclusions,
extracts the section of the Atkin LJ judgment in *Falcon v Famous Players*, which formulated
the test, in full, before stating that the test has a significance not always appreciated in those
later cases, including Moorhouse, which repeat the phrase “sanction, approve, countenance”
((2012) 286 ALR 466, 496). At least impliedly, therefore, both judgments in iiNet reject the
wider approaches to authorisation adopted by Jacobs J and Gibbs J, respectively, in
Moorhouse.

Thirdly, both judgments accept, appropriately, that the three statutory factors in the partial
codification must be applied in determining whether or not a person is liable for authorising
infringements. The French judgment clearly regards the application of these factors as
determinative of the appeal ((2012) 286 ALR 466, 482). As explained above, however, the
Gummow judgment appears to apply the partial codification somewhat reluctantly, as it adds
a ‘further element of complexity’ ((2012) 286 ALR 466, 497). The combination of the narrow
English approach to authorisation with the application of the statutory criteria gives rise to the
most important problem raised by the case: as the statutory criteria derive from the judgment
of Gibbs J in Moorhouse, they appear to endorse a wide approach to authorisation.
The judgments in *iiNet* appear to deal with the inconsistency between the narrow English approach to authorisation and the statutory criteria by applying the pre-*Moorhouse* law to the interpretation of the criteria. Thus, in examining the extent of iiNet’s power to prevent infringements, the French judgment essentially applies the distinction between a direct and indirect power to prevent made by Higgins J in *Adelaide Corporation*, concluding that iiNet ‘had no direct power to prevent the primary infringements and could only ensure that result indirectly by terminating the contractual relationship it had with its customers’ ((2012) 286 ALR 466, 484). Although the Gummow judgment does not expressly refer to *Adelaide Corporation* on this issue, it nevertheless emphasises iiNet’s limited power over both its subscribers and the BitTorrent system ((2012) 286 ALR 466, 498). Furthermore, as both judgments suggest that iiNet’s power was limited by the extent to which subscribers can simply sign-up to another ISP, this raises the question of whether or not a person must have an absolute power to prevent infringements in order to be liable for authorising those infringements.

In any case, the approaches adopted to the statutory criteria in *iiNet* raise the question, which is not answered in the judgments, of whether or not there can ever be liability for authorising an infringement where there is only an indirect power to prevent infringements, such as the power to end a contractual relationship. Given the importance placed on the reasoning of the majority in *Adelaide Corporation* by both judgments in *iiNet*, it is potentially important to bear in mind that *Adelaide Corporation* was concerned with permission, not authorisation. Moreover, while the judgment of Gibbs J in *Moorhouse* refers, with apparent approval, to the dissenting judgments of Knox CJ and Isaacs J in *Adelaide Corporation*, it does not refer to the judgment of Higgins J, thereby casting some doubt on the status of that judgment prior to *iiNet*. The reasoning in the two judgments in *iiNet*, however, clearly now casts significant doubt on the ongoing authority of the reasoning of both judgments in *Moorhouse*.

The final point on which both judgments in *iiNet* appear to agree is in distinguishing the facts in *iiNet* from those in *Moorhouse*. Before the High Court, iiNet argued that the facts in *Moorhouse* were distinguishable as, in that case, UNSW had control of the library books, as well as the photocopiers. The Gummow judgment expressly endorses this distinction ((2012) 286 ALR 466, 497), while the French judgment does not dispute it. Therefore, while apparently rejecting the reasoning in both judgments in *Moorhouse*, as opposed to the Canadian Supreme Court in *CCH*, the *iiNet* judgments do not question the outcome in that case ((2012) 286 ALR 466, 479-80; 497). This seems, at least, to imply that a person who omits to act, or is indifferent to infringements, may still, in some circumstances, be liable for authorising infringements. Following *iiNet*, however, any such liability must apparently depend upon a narrow interpretation of the statutory criteria in the light of the English test of whether or not the person has granted, or purported to grant, a right to do infringing acts.

In addition to the difficulties of reconciling the two judgments in *iiNet* with the statutory criteria and, via that, with the judgments in *Moorhouse*, additional uncertainty is created by differences between the judgments. The Gummow judgment, in particular, gives rise to a number of unresolved questions. First, in drawing an analogy between secondary liability for copyright infringement and inducing breach of contract, the Gummow judgment seems to suggest that actual or constructive knowledge is an essential element of the tort of authorising copyright infringements ((2012) 286 ALR 466, 492). The judgments therefore fail to resolve a difference between the judgments of Gibbs J and Jacobs J in *Moorhouse*, where Gibbs J held that a mental element was necessary, but Jacobs J did not. Secondly, the Gummow judgment introduces the possibility of a separate basis for authorisation liability where a person supplies a product or service that is ‘bound to infringe’. The relationship between this proposed new basis for authorisation liability and the narrow English approach to infringement is unresolved, raising a number of new questions. For example, if, as the Gummow judgment seems to suggest, a mental element is required for authorisation liability, this would not seem to be relevant to liability that arises from conduct that is ‘bound to infringe’. Yet, at the same time, the judgment seems to approve the approach of Lord Templeman to both the narrow English test and the ‘bound to infringe’ test.
CONCLUSION

From the introduction of authorisation liability in the 1911 UK Act, there has been considerable uncertainty about the meaning and scope of this form of liability, which is the main form of secondary liability for copyright infringements. The emergence of the Internet, and especially P2P file-sharing, as the major channel for copyright infringement, focussed attention on the extent to which intermediaries, such as ISPs, may be secondarily liable for the infringements of their subscribers. As part of a global strategy for dealing with large-scale infringements via P2P systems, copyright owners have embraced a strategy, known as ‘graduated response’, of encouraging ISPs to assist in deterring infringements by passing on warnings to subscribers and, ultimately, suspending or terminating accounts. In Australia, in the absence of an industry code of practice, or a legislated graduated response regime, copyright owners attempted to establish that ISPs, under certain conditions, would be liable for authorising the infringements of their subscribers if they did not implement a form of ‘graduated response’, resulting in the iiNet litigation.

The High Court decision in iiNet clarifies the liability of ISPs for the infringements of their subscribers by essentially holding that, unless an ISP is actively involved in infringements, such as by actively procuring or facilitating infringements, an ISP that provides Internet access will not be liable for authorising infringements. This effectively means that those sections of the Copyright Act aimed at limiting the liability of ISPs in relation to some activities – the facilities provider exception and the ‘safe harbour’ regime that applies to category A activities – are unnecessary. It also means that the future of ‘graduated response’ in Australia depends upon either the development of an industry code of practice that imposes obligations on ISPs that are not imposed under copyright law, or the introduction of a legislative regime that imposes obligations on ISPs. At the time of writing, it is extremely uncertain whether or not either of these potential responses to the decision will eventuate. Although the Communications Alliance has supported an education-based scheme for passing on infringement notices to subscribers (Communications Alliance 2011a), the copyright owners and ISPs have failed to agree on how to apportion the costs of the proposed scheme (Communications Alliance 2011b).

In reaching the conclusion that ISPs will generally not be liable for end-user infringements, the High Court adopted a narrow approach to authorisation liability, essentially concluding that to authorise means to grant, or purport to grant, a right to do the infringing act. This approach, which would bring Australian law generally into line with English law, creates a degree of uncertainty, as the partial codification of authorisation in the Digital Agenda reforms seemed to endorse a much wider approach to authorisation. The High Court appears to have dealt with this potential tension between the common law and the statutory criteria by applying the pre-Moorhouse case law to the interpretation of the statutory criteria while, at the same time, not expressly over-ruling the outcome in Moorhouse.

The approach adopted to authorisation by the High Court - which includes applying the reasoning of Higgins J in Adelaide Corporation in interpreting the extent to which a person has the power to prevent infringements – also sits a bit uncomfortably with the reasoning in a recent English decision on authorisation liability. In that case, Twentieth Century Fox v Newzbin ([2010] FSR 21), Kitchin J held that the operators of a Usenet indexing service, which included categories clearly related to copyright infringements, was liable for authorising infringements committed by members of the service. While the facts in that case are quite different to those which involve ISP liability, in the course of determining that the service provider had ‘purported to grant’ a right to infringe, Kitchin J stated that the circumstances in which a purported grant may be implied include ‘the nature of the relationship between the alleged authorizer and the primary infringer, whether the equipment or other material supplied constitutes the means used to infringe, whether it is inevitable it will be used to infringe, the degree of control which the supplier retains and whether he has taken any steps to prevent infringement’ (at [540]). In applying these criteria, which Kitchin J
consiously adopted from Australian law, he specifically did not apply the restrictive interpretation of authorisation liability applied by the High Court in *iiNet*. Neither did he apply the ‘bound to infringe’ test. This not only suggests that there are considerable uncertainties with the application of the narrow English test, which seem to have been overlooked in the judgments of the High Court in *iiNet*, but raises the possibility that English courts may end up applying a wider approach to authorisation than that applied by the High Court in *iiNet*. Moreover, even without the complexities arising from the partial codification in Australia, the apparent attempt to harmonise Australian law with English law may prove little more than a mirage.

In any event, the decision of the High Court in *iiNet* is now the main Australian authority on authorisation. Lawyers advising their clients, and lower courts required to apply the decision, will need to deal with the considerable uncertainties arising from the decision, including those that arise from the differences in the two judgments. What is abundantly clear is that, first, the attempt to clarify the law by partially codifying authorisation liability has conspicuously failed and, secondly, that it will take some time for the courts to resolve the considerable legal uncertainties arising from the decision.

**ACKNOWLEDGEMENTS**

The author would like to thank the two referees of this article for their valuable comments.

**REFERENCES**


BIBLIOGRAPHY


ENDNOTES

1 The Irish High Court, which is not at the apex of the Irish legal system, has considered similar issues in two 2010 decisions: EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd [2010] IEHC 377 and EMI Records v Eircom Ltd [2010] IEHC 108.

2 Copyright Act 1911 (UK) s 1(2).

3 See Literary Copyright Act 1842 (UK) s 15; Dramatic Copyright Act 1833 (UK) s 1.

4 See, for example, Karna v Pathé Frères (1909) 100 LT 260.

5 Copyright Act 1911 (UK) s 2(3). The current Australian Act retains this form of liability: see Copyright Act 1968 (Cth) s 39.
6 Following Moorhouse, a new s 39A was promptly introduced into the Copyright Act, which effectively protects libraries from authorisation liability where a notice is fixed on photocopy machines.

7 While Burrell and Weatherall (2011) tend to assimilate the Jacobs J judgment with the Atkins LJ formulation, the two approaches are different.

8 A different approach seems to have been accepted by Branson J in Cooper v Universal Music (2006) 21 IPR 1, 5.

9 See Copyright Act 1968 (Cth), Part V Div 2AA.

10 Copyright Act 1968 (Cth) s 116AH(1), Item 1.


12 See Performing Right Society v Cyril [1924] 1 KB 1, 9 (per Bankes LJ); CBS Inc v Ames [1982] Ch 91, 112.

13 The scheme proposed by the Communications Alliance does not provide for termination of Internet accounts, or any other punitive sanctions.
ON THE (NEW) NEW ZEALAND GRADUATED RESPONSE LAW (AND WHY IT'S UNLIKELY TO ACHIEVE ITS AIMS)

Rebecca Giblin
Monash University

In 2011 New Zealand controversially introduced a 'three strikes' graduated response law. Under this law, the holders of Internet service accounts which are detected as having infringed copyright via P2P file sharing technologies three times within a specified time period can be ordered by the Copyright Tribunal to pay content owners up to NZ$15,000. The law also provides for Internet access to be suspended, though these provisions are currently inactive pending determination of the efficacy of the financial penalty regime. This paper explores the contours of the NZ graduated response regime – and then outlines a number of technical and practical reasons why it's unlikely to achieve its aims.

I: INTRODUCTION

New Zealand recently enacted a graduated response law as a low-cost, high volume alternative to traditional methods of copyright enforcement. A number of other jurisdictions, including Taiwan, France, South Korea and the UK, have similar graduated response laws that can culminate in disconnection of the account holder's Internet access. The NZ regime does not currently provide for termination of the Internet access of recidivist infringers. Instead, it involves a 'slim' quasi-judicial process and empowers a Tribunal to award financial penalties against an Internet account holder in certain circumstances. Disconnection provisions are contained within the Act, but they're currently dormant, and can only be brought into force by an Order in Council. The NZ Government has indicated that it will move to do so only if the notice-and-financial-penalty combination does not prove to be a 'sufficient deterrent to illegal file-sharing'.

In addition to providing that deterrent, the legislation aims to 'provide appropriate protection for creative industries' and to ensure that such industries 'adapt to changing technologies and the changing market place for creative works'. The NZ scheme is likely of particular interest to the Australian government, which is under considerable pressure to institute a similar statutory scheme in the wake of the Australian High Court's recent finding that there is no common law obligation for ISPs to act on allegations of infringement. However, Australia should not rush to mimic the NZ regime: after providing a comprehensive overview of the scheme's intended operation and procedural contours, this paper explains why that scheme will have limited success in achieving those aims.
II: OVERVIEW OF THE SCHEME

NATIONAL CONTEXT

The Copyright (Infringing File Sharing) Amendment Act 2011 was actually New Zealand's second attempt at creating a graduated response regime. The first occurred three years earlier via the Copyright (New Technologies) Amendment Act 2008. Section 92A of that Act imposed an obligation on ISPs to 'adopt and reasonably implement' policies that provided for termination of Internet access to repeat infringers. Commonly referred to as the 'guilt upon accusation' law, s92A quickly became controversial for its far-reaching scope, lack of due process, and absence of any presumption of innocence. Before it came into operation, a tremendous groundswell of opposition led to the Government of the day giving the legislation a complete overhaul.

The result was the Copyright (Infringing File Sharing) Amendment Act 2011. It amended the Copyright Act 1994 (the Act) by repealing the controversial s92A and replacing it with a new graduated response regime. The new scheme utilises a three-notice framework which relies on rights owners to alert Internet providers to copyright infringements committed via their connections, and then obliges those providers to send notices alerting the relevant account holder. If three notices are received by a single account holder in relation to the same rights holder within a defined period, the legislation's enforcement provisions kick in.

'IPAPs' NOT 'ISPs'

One of the aspects of the original graduated response legislation most vehemently objected to was its overly-expansive definition of ISPs, which would have imposed onerous compliance burdens on organisations that had little direct involvement in the provision of Internet access. This definitional problem was addressed in the revised version, which only imposes obligations on Internet Protocol Address Providers (IPAPs). IPAPs are defined as those who operate a business that, other than as an incidental feature of its main business activities, offer the transmission, routing and providing of connections for digital online communications, allocate IP addresses to their account holders, charge those account holders for their services, and are not primarily operated to cater for transient users. This definition 'is intended to exclude universities, libraries, and businesses that provide Internet access to their members or employees but are not in the nature of a traditional ISP'.

DETECTION, WARNING AND ENFORCEMENT NOTICES

After a rights holder makes an allegation of copyright infringement regarding a subscriber, the IPAP has seven days to match the IP address to the subscriber to which it was assigned at the relevant time, and issue the appropriate infringement notice to that person.

The first time an IPAP matches an account holder to an IP address at which a rights owner alleges an infringement to have occurred, it must issue a detection notice. Detection notices expire nine months after issue or at the end of the quarantine period (defined below), whichever comes sooner.

If an IPAP then matches the same account holder to an IP address at which the same rights owner alleges an infringement to have occurred, and if that infringement occurred at least 28 days after the date of the detection notice, but before it expires ('the on-notice period'), it must send a warning notice. Warning notices also expire nine months after issue or at the end of the quarantine period. An enforcement notice must be issued by an IPAP if, for a third time, it matches the account holder to an IP address at which a rights owner alleges an infringement to have occurred. Again, this only applies so long as it occurred outside the on-notice period. Enforcement notices are valid for 35 days ('the quarantine period'), after which they expire. Once the
quarantine period expires, the 'three strikes' cycle begins anew: the next infringement (if any) detected with reference to that account holder will trigger a fresh detection notice.\textsuperscript{16}

IPAPs are entitled to charge rights owners a fee to cover the ongoing costs associated with the operation of the graduated response regime.\textsuperscript{17} Regulations currently cap that fee at $25 per notice.\textsuperscript{18} The scheme also provides a safe harbour for ISPs that allows them to escape liability for their users' infringement as long as they comply with their obligations under the legislation.\textsuperscript{19}

**THE 'ON-NOTICE' PERIOD**

The 'on-notice period' exists in recognition of the fact that sometimes the account holder might not be the individual personally carrying out any infringement. Where that is so, it is likely that it would take some time for the account holder to identify the actual infringer and/or to take steps or institute procedures to prevent further breaches of copyright. If further 'strikes' could accumulate against that account holder without providing it the opportunity to do so, the scheme would be less educative and more punitive in effect. It would also reduce the moral justification for holding the account holder liable.

**CHALLENGES AND EXEMPTIONS**

The rights holder is not obliged to provide evidence in support of an allegation of infringement. However, the account holder is entitled to dispute an infringement notice by sending a 'challenge' to the issuing IPAP within 14 days.\textsuperscript{20} Compliant challenges must be sent to the relevant rights owner. If the rights owner does not reject the challenge within 28 days, it is deemed to be accepted.\textsuperscript{21} If the challenge is rejected by the rights owner, the account holder has no further recourse at that time, but may re-raise its objections during any subsequent enforcement proceedings.\textsuperscript{22}

The Act contains no specific exemptions to protect special classes of organisation such as universities or libraries. The Commerce Committee expressly recommended against them out of concern that they may create loopholes within the scheme.\textsuperscript{23} Instead, the law provides for the Tribunal and Court to refuse to make an order to fine an account holder or disconnect their Internet account where they consider it 'manifestly unjust' to do so.\textsuperscript{24}

**ENFORCEMENT – FINANCIAL PENALTIES**

As noted above, the legislation's disconnection provisions are currently dormant. This paper focuses on the standalone financial penalty provisions.

To alert rights owners to the fact that a 'third strike' has accrued to an account holder, the IPAP is required to provide it with a copy of the enforcement notice. After the issue of that notice, the rights holder has between 7 and 21 days to make an application to the Copyright Tribunal ('the Tribunal') for an order that the account holder pay it a sum of money.\textsuperscript{25} Unless it considers it 'manifestly unjust' to do so,\textsuperscript{26} the Tribunal is required to make such an order where it is satisfied that the allegations that triggered the infringement notices related to infringements of the rights owner's copyright, were committed from an IP address assigned to the account holder, and that the notices were validly issued.\textsuperscript{27}

The sum awarded is to be determined in accordance with the regulations,\textsuperscript{28} which have largely adopted the approach preferred by the Ministry for Economic Development in its call for submissions.\textsuperscript{29} Regulation 12(2) requires the Tribunal to assess:

a) for each work in which the Tribunal is satisfied that the copyright has been infringed at the IP address of the account holder,

i. If the work was legally available for purchase in electronic form at the time of the infringement, the reasonable cost of purchasing the work in electronic form at that time; or
ii. If the work was not legally available for purchase in electronic form at the time of the infringement but was available in some other form, the reasonable cost of purchasing that work in another form at that time; or

iii. If neither subparagraph (i) nor subparagraph (ii) applies, the amount claimed by the applicant in respect of the work, or any other reasonable amount determined by the Tribunal.

b) the cost of any fee or fees paid by the rights owner to the IPAP in respect of the infringements to which the application relate; and

c) the cost of the application fee paid by the rights owner to the Tribunal; and

d) an amount that the Tribunal considers appropriate as a deterrent against further infringing.

In assessing the figure referenced in r 12(2)(d) in any given scenario, the Tribunal must consider:

a) the flagrancy of the infringement; and

b) the possible effect of the infringing activity on the market for the work; and

c) whether the sum of the amounts referred to in subclause (2)(a) to (c) would already constitute a sufficient deterrent against further infringing.

It may also consider any other relevant circumstances. The Tribunal can then order an account holder to pay the lesser of the sum calculated in the manner described above, or the ceiling amount of NZ$15,000 (approx US$11,000 or €8,000).

The new regime came into effect in September 2011 (except for cellular networks, which will not be obliged to comply until September 2013). The first valid complaints were received by ISPs by 1 November 2011. As yet, there has been little opportunity for data to be collected regarding its efficacy, although some New Zealand ISPs reported a drop in the amount of Internet traffic in the days after the law came into operation.

**III: WHY THE LAW WON'T ACHIEVE ITS AIMS**

As noted above, the scheme is intended to deter infringement, to 'provide appropriate protection for creative industries' and to ensure that those industries 'adapt to changing technologies and the changing market place for creative works'. Determining what is 'appropriate' protection for creative industries is highly subjective, and there is no fixed answer. In the context however, it appears that by 'appropriate' protection, the moving Minister was referring to more effective protection of copyrights by means of making enforcement simple and cheap enough to be feasible. For a number of reasons however, the graduated response scheme is likely to fail to achieve these aims.

**IMPRACTICALITY OF ACHIEVING THREE STRIKES**

The first reason why not arises from a combination of two independent factors: the costs to right holders of enforcing their rights under the scheme, and the way in which IP addresses are typically allocated to users.

ISPs can charge right holders a maximum of NZ$25 to defray its costs of performing the functions required of it under the Act. Some reports suggest that this is not necessarily even sufficient to cover the IPAP's costs of issuing each notice. It appears that right holders are obliged to pay that fee even if it turns out that the relevant account holder is within the on-notice period, and thus the IPAP does not actually have to send a notice.

Infringing accounts are identified by matching the account holder to the IP address at which infringement was alleged to have occurred. IPAPs each have a pool of IP addresses which they allocate to customers as necessary. The IP address is the only piece of information
available to right holders to identify putative infringers. Some customers (usually businesses) have an unchanging or 'static' IP address allocated to them for the term of their subscription, for which they generally pay a higher fee, but most users receive IP addresses on a dynamic or ad hoc basis. That means that there is usually no fixed point on the Internet which is constantly referable to a particular account. An account holder might one day be allocated IP address 110.173.160.0. An hour later it might be switched to 110.173.162.343, and the next day it could just as easily be 110.173.163.723. When not in use by that account, those same IP addresses will be allocated to others. Thus IP address 110.173.162.343 could well be detected as having been used for infringement on dozens of separate occasions in any given period, assigned to a different account holder each time. And a single user might commit dozens of infringements whilst having a different IP address for each of them.

This system means that right holders have no way of targeting specific accounts, such as those which have been previously detected infringing. They can only take a scattergun approach, and hope to hit the same account holder three times in order for the enforcement provisions to kick in. When combined with the $25 fee that must be paid to IPAPs, this new method is not much more practical to enforce than the traditional remedies within the Copyright Act.

This can be demonstrated with some simple modelling. New Zealand has a population of some 4.5 million people. Assume, conservatively, that 2% of the population is detected committing two infringements via P2P file sharing technologies per week. That equates to 180,000 infringements each week. If notices were to be issued for each, it would cost right holders $4.5m per week, or $234m per annum. Obviously that is unfeasible, so right holders will have to be selective.

The blind approach dictated by the nature of IP address allocation and the cost of issuing notices means that there is a real likelihood that the scheme will fail to provide an effective deterrent. The sheer number of infringements detected, and lack of consistency between IP addresses, means that recidivist infringers may well never receive a single notice. Even if the same account is detected infringing multiple times, the existence of on-notice periods (during which any notices will not contribute towards a further 'strike') makes it even more unlikely that three valid strikes will accrue. In these circumstances it seems unlikely that a significant enough number of notices will be issued to provide an effective deterrent. The cost of issuing notices and the likely low effect they will have means that the scheme is unlikely to provide any more effective protection than the previous law.

Having said that, a technical change is coming which might change the above equations in favour of right holders. It has not been feasible for ISPs to allocate static IP addresses to all customers for some time, because the number of such addresses is so limited. Under the prevailing 32-bit IPv4 standard, only $2^{32}$ (some 4.29 billion) separate addresses exist, which must be shared amongst all Internet-connected devices on the planet. Those addresses are now all but exhausted. That is triggering a change to a new 128-bit standard called IPv6, which will make $2^{128}$ addresses available — a very large number indeed, equating to 'about 1,500 addresses for every square foot of the earth's surface'.

As ISPs switch over to IPv6, it will become more and more feasible for all customers to receive their own static IP addresses for each of their Internet-connected devices. If ISPs choose to do this, it would become much easier for right holders to compile infringement data with regard to particular accounts. This would enable them to determine in advance whether a particular account has received any strikes, whether it is currently within an 'on-notice' period, and whether there has been any apparent reduction in infringement as the result of any previous notices.

This kind of targeted knowledge would make the $25 fee much less prohibitive, because right holders (and account holders) would know that the chance of enforcement action (and thus the chance of recovering those costs) was much greater. Accounts that were detected engaging in isolated infringements would likely be left alone in favour of large-scale recidivists. If a wholesale move to static IP addresses occurred, it would be considerably easier to identify repeat infringers. That would have significant follow on effects, by making the law much
more likely to have a significant deterrent effect, and of providing more effective copyright protection via easier enforceability.

The equation might also change if efforts to create a centralised notice system at a significantly reduced per-notice cost come to fruition. As matters now stand however, recidivist infringers don't need to be too worried about their chances of being hauled before the Tribunal, and, as a practical matter, right holders don't have much more effective protection than they did without the graduated response law.

**Switching tools**

The second reason why the graduated response scheme is likely to fail to achieve its aims arises from a Brobdingnagian loophole within the legislation, introduced despite the Commerce Committee's avowed intention of avoiding them. That loophole is the fact that the graduated response law is limited in scope to infringement carried out via peer-to-peer file sharing technologies.

Let's say that a user is actually detected infringing on several occasions, and receives one or even two notices. It's certainly possible that infringement will cease from that account. But the way the scheme operates means that it's perhaps just as likely that infringers will simply change their behaviour to avoid the reach of the scheme whilst still achieving their desired result.

They can do this by simply switching to non-P2P tools of infringement, and there is already evidence that they're doing exactly that. The most likely alternatives are 'file lockers', online file hosting websites, which allow users to store content on their servers for download by themselves or others. Such services have been growing enormously in popularity and number over the last few years as the cost of storage per gigabyte sinks. A recent report found that just three such sites – Rapidshare, Megavideo and Megaupload – are being visited more than 21 billion times each year. A separate report recently found that file locker transfers comprise some '7% of all Internet traffic', though this figure may reduce in the aftermath of the Megaupload takedown.

Online forum discussions demonstrate that users are very aware of the distinction between technologies that fall within and outside the NZ scheme: an online discussion about the early lack of notices saw one user comment that '[p]eople I know appear to have switched to other means of obtaining the things they were interested in. They are still getting it. Just not via Bittorrent'. Other users have observed, 'with that new law in place, http downloads are the way to go if you want to stay below the radar', and that they '[h]ad to start using usenet because of that piracy law'.

Another anti-regulatory innovation being adopted by Kiwis is the 'seedbox'. Seedboxes are high-speed remote servers, hosted in jurisdictions with lax copyright laws, which are used for sharing torrent files. The desired content is downloaded to the seedbox via BitTorrent, and the user can then transfer it to their own computer via a http connection. Thus, for a small monthly subscription fee, users can still obtain content via P2P networks whilst still technically falling outside the graduated response regime.

The previous section demonstrated that it was unlikely that many account holders would ever receive the first two valid notices under the graduated response regime. Even if they do, this section has demonstrated that they can easily bypass the operation of the scheme by switching to different tools for their infringement. Especially savvy users who have been detected infringing under the scheme might continue using P2P technologies until the end of the on-notice period referable to their second notice, if one ever arrives, knowing that they cannot be pursued in the Tribunal until after that point. Then, when that notice expires, they switch right back and begin the cycle anew. Admittedly, the less informed are unlikely to pursue these options. However, it is extremely easy to find out how to bypass the law: as the above-quoted forum extracts demonstrate, a quick google search will result in an enormous amount of advice on how to do so. And if enough users decide that the benefits of doing so outweigh the costs, it's likely to drastically reduce the efficacy of the legislation.
THE IP ADDRESS ALLOCATION LOOPHOLE

A third reason why the law is unlikely to achieve its aims arises from another loophole, this time contained within the regulations. Regulation 4(6) provides that,

'[a]n IPAP may ignore, for the purposes of its obligations under section 122C of the Act, any IP addresses identified in a rights owner notice that are not IP addresses that the IPAP allocates, or allocated at the relevant time, and the IPAP is not required (despite section 122T(2)(a) of the Act) to retain any information relating to those IP addresses.'

Thus, if an account holder has an IP address allocated by other than its Internet service provider, it will effectively fall outside the scope of the graduated response scheme.

To understand the significance of this, it's necessary to understand that IP addresses can be allocated directly to organisation or individuals. In the Asia Pacific region, this is done by the APNIC organisation. If a company or individual wished to avoid all risk of liability under the scheme, they could simply obtain IP addresses from APNIC. A minimum of 256 can be obtained, at a current cost of around AU$4175 in the first year and $1180 for each yearly renewal.

Whenever an organisation provides Internet access to end users, there is a risk that the organisation may be hauled before the Copyright Tribunal and obliged to pay a fine. Depending on the size of the organisation (and the number of infringements) that risk may be considerable.

There appears to be only two ways of eliminating that risk. The first is to block P2P from the organisation's network completely. However, that might have negative implications for non-infringing uses, particularly those involving applications or services that require the blocked ports to operate. And this method might not be entirely effective: it's always possible that some infringement may sneak through, especially if new or existing P2P protocols are modified to ports other than the ones that have already been blocked. Recent detection of infringement apparently originating at companies such as Sony Pictures Entertainment and NBC Universal highlights the difficulty of blocking infringing uses entirely.

The second method is for the organisation to have its IP addresses allocated by APNIC instead of its IPAP. It would need to have the resources to manage the addresses itself, rather than delegate this task to its Internet service provider, because otherwise the ISP could be seen to have 'allocated' the IP addresses and the strategy would fail. Then, if its users engaged in P2P copyright infringement, its IPAP could ignore requests from right holders to deal with the matter courtesy of regulation 4(6). This would effectively allow the organisation to opt-out of the graduated response system completely, while giving it the ability to retain access to useful technologies. The costs and procedures involved make this strategy unfeasible for household accounts, but it may well be an attractive option at the enterprise level.

One factor limiting the practical significance right now is the shortage of IPv4 IP addresses, as discussed above. As the number of IP addresses available explodes with the advent of IPv6, it's likely that the uptake of this loophole will also.

WHERE'S THE CARROT WITH THAT STICK?

The above analysis has focused on the ways in which the legislation is unlikely to achieve its related aims of deterring end user infringement, and of providing more effective copyright protection through ease of enforceability. Its third aim is to ensure that creative industries 'adapt to changing technologies and the changing market place for creative works'. In its current form however, the scheme does little to forward this aim.

New Zealand citizens currently have relatively limited access to much popular content. Greens MP Gareth Hughes, one of the strongest opponents of the legislation, has observed...
that New Zealand is often 'at the end of US or European-based supply chains. We can wait months or sometimes years to get access to content that is freely available overseas'. 56 It has been reported that prices paid by Kiwis for digital content can be 50% higher than for identical content purchased overseas. 57 Furthermore, Netflix recently ruled out a launch of its service in New Zealand, with one of its reasons being that it was unable to obtain the necessary rights. 58

Various proposals were suggested to make a link between availability of remedies under the graduated response law and improved access to content. Hughes suggested at the second reading stage that it might have been appropriate to introduce a zero-dollar penalty for infringing against international products that are not available in New Zealand [in order to encourage] rights-holders to provide digital content sooner to Kiwis. 59 InternetNZ, a non-profit organisation focused on protecting and promoting the Internet, made a similar suggestion in its submission to the Ministry of Economic Development on the regulations necessary to the graduated response law. It proposed a link between availability of content and availability of substantial damages. If a work was not available for sale in NZ at the time of the infringement, it proposed that the copyright owner should only be entitled to its reasonable costs of enforcement. 60 However, neither of these suggestions nor any similar proposals were adopted.

The introduction of the graduated response regime was a great opportunity for the legislature to encourage content owners to improve access to legitimate content by tying access to increased enforcement options to reasonable availability of content. However, it failed to do so, and thus will apparently do little more than pay lip service to its aim of ensuring that creative industries adapt to changing technologies and markets.

PART IV: CONCLUSIONS AND CONSEQUENCES

This paper has argued that the NZ graduated response law is unlikely to provide much of a deterrent, or to achieve its other aims. The NZ government has indicated that, if the law does fail to 'sufficiently' deter infringement, that will trigger activation of the regime's disconnection provisions. However, in the event that this paper's prognostications come to pass, it should think carefully before implementing that strategy.

As noted above, a number of other jurisdictions already have graduated response laws that can culminate in disconnection of the account holder's Internet access 61. However, those laws have been met with substantial and well-founded criticism. Intense lobbying efforts by right holders to include a graduated response strategy in the Anti-Counterfeiting Trade Agreement failed after vociferous opposition 62 (although a general provision 'condition[ing] ISP eligibility for safe harbor from claims for third party infringement on 'an online service provider's adopting and reasonably implementing a policy to address unauthorised storage or transmission of materials protected by copyright' did make it in). 63

A paper by Nicolas Suzor and Brian Fitzgerald has persuasively made the case that graduated response schemes that provide for disconnection often fail to comply with key tenets of the rule of law, particularly with regard to proportionality and due process. 64 And in May 2011, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued a report finding that 'cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law' amounts to a violation of Article 19 of the International Covenant on Civil and Political Rights ('the Covenant'), which provides that '[e]veryone shall have the right to freedom of expression'. 65

Though Article 19 provides for that right to be restricted, such restrictions 'shall only be such as are provided by law' and must be necessary 'for respect of the rights or reputations of others' or for reasons of national security, public order, or public health or morals. 66 The Special Rapporteur found that disconnection of Internet access as a consequence of the violation of intellectual property rights contravened the Article because it was a 'disproportionate' restriction on the right to freedom of expression. 67 The Report went on to
strongly recommend that States that had implemented such provisions should amend or repeal them, and that others should refrain from adoption.68

Although the Report has not been formally adopted by the UN, its strong suggestion that Internet disconnection is an inappropriate penalty for copyright infringement casts doubt on the legitimacy of such regimes. Regimes that have incorporated graduated response via 'private ordering' mechanisms have also hit rough water. The European Data Protection Commissioner recently ordered Irish ISP Eircom to cease enforcing the 'three strikes' regime that it introduced as part of a settlement with right holders in 2009, apparently over privacy concerns regarding the use of IP addresses to identify alleged infringers.69

Instead of responding to any lack of deterrence by introducing the highly problematic sanction of disconnection, New Zealand (and other countries considering taking a similar route) should learn from the lessons of its current scheme. It is certainly possible to design systems that have less 'leakage' in the form of copyright infringement, by, for example, mandating use of one or more IP addresses for each person once IPv6 becomes prevalent, by including all copyright infringement regardless of tool used to commit it, and by capturing even organisations whose IP addresses are not allocated by their ISPs. However, each of those changes would give rise to new loopholes which will inevitably be exploited as end users seek ways of obtaining desired content. Resources that could have been used to pay creators will continue to be used instead to avoid the operation of the law, via http tunnelling, proxies, darknets, Virtual Private Networks and dozens of other methods that haven't yet been thought of.

Even if it were possible to eliminate all infringement, it's by no means certain that this is the most desirable result. As Professor Alain Strowel has observed, 'a solution that would eliminate all piracy, if at all possible, would seem dangerous or at least dubious for both individual liberties and technological innovation.'70 This is particularly so in a market like New Zealand, where right holders have apparently adopted a strategy of limited availability and high prices. The willingness of users to pay for expensive Internet bandwidth and access to anti-regulatory tools such as seedboxes and UseNet in order to obtain access shows that there is money to be spent on content – it's just not going to right holders.

One user wrote: '[p]rovide a service that is superior to what the pirates are providing, and people will flock to your service. [Infringement doesn't occur] because people don't want to spend money, but because your service is terrible'.71 Full compliance with the law by end users would seem unlikely to do anything to change this. Indeed, it would seem likely to lead to continued stagnation and little incentive for right holders to improve the availability of content. Instead of simply bowing to pressure to introduce more onerous penalties, legislatures around the world should acknowledge to the root of the problem. If graduated response laws are to exist at all, they should be in a form that encourages the timely and reasonably priced availability of content.

REFERENCES


Kang, Cecilia. 2011. 'USTR: Acta won't include three-strikes; draft available in days' Washington Post <http://voices.washingtonpost.com/posttech/2010/04/ustr_acta_wont_include_three-s.html> at 16 December 2011.


Suzor, Nicolas; Fitzgerald, Brian. 2011. 'The legitimacy of graduated response schemes in copyright law' University of New South Wales Law Journal 34(1) 1.


ENDNOTES

1 For an overview of the regimes in place in France and South Korea, see (de Beer and Clemmer 2009). An English translation of the Taiwanese legislation is available at Taiwan, Province of China World Intellectual Property Organization <http://www.wipo.int/wipolex/en/text.jsp?file_id=187795##None> article 90quinquies, at 19 October 2011. At the time of writing, the UK system had not yet come into operation.
and currently being challenged by two large ISPs. Discussion of its current status is available at (Sweney and Halliday 2011).

2 Copyright Act 1994 (NZ) s 122R(2).

3 New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083 (Dr Wayne Mapp).

4 New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083 (Dr Wayne Mapp).


8 Copyright Act 1994 (NZ) s 122A(1).


10 Copyright Act 1994 (NZ) s 122C(1).

11 Copyright Act 1994 (NZ) s 122D(1).

12 Copyright Act 1994 (NZ) s 122D(3), 122F(4).

13 Copyright Act 1994 (NZ) s 122E(3), 122F(4).

14 Copyright Act 1994 (NZ) s 122F(1).

15 Copyright Act 1994 (NZ) s 122F(3).

16 Copyright Act 1994 (NZ) s 122D(1)(b).

17 Copyright Act 1994 (NZ) s 122U.

18 Copyright (Infringing File Sharing) Regulations 2011 (NZ), reg 7.

19 Copyright Act 1994 (NZ) s 92B(2A).

20 Copyright Act 1994 (NZ) s 122G(1)-(2).

21 Copyright Act 1994 (NZ) s 122H(1).

22 Copyright Act 1994 (NZ) s 122G(4)-(5).

23 New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083 (Dr Wayne Mapp).

24 Copyright Act 1994 (NZ) s 122O(5).

25 See Copyright Act 1994 (NZ) s 122J(1). The application must be made before the expiry of the quarantine period (35 days from the date of the notice) but after the 14-day period in which the account holder could challenge the notice (or, if a complying challenge is made, after the last day on which the challenge could be rejected).

26 Copyright Act 1994 (NZ) s 122O(5).

27 Copyright Act 1994 (NZ) s 122O(1).

28 Copyright Act 1994 (NZ) s 122O(2).


30 Copyright (Infringing File Sharing) Regulations 2011 (NZ), reg 12(3).
Copyright Act 1994 (NZ) s 122O(4).

Copyright (Infringing File Sharing) Amendment Act 2011 (NZ) s 2; Copyright Act 1994
(NZ) s 122S.

Siobhan Keogh, First copyright infringement notices arrive (2011) New Zealand PC
World <http://pcworld.co.nz/pcworld/pcw.nsf/news/first-copyright-infringement-notices-
arrive> at 1 December 2011.

Timothy B Lee, New Zealand traffic down as 'three strikes' copyright law takes effect
copyright-law-takes-effect.ars> at 15 November 2011.

New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083
(Or Wayne Mapp).

See Copyright Act 1994 (NZ) s 122U; Copyright (Infringing File Sharing) Regulations
2011 (NZ), reg 7.

See eg ISPs can charge $25 to process copyright infringement notices (2011) Computerworld
infringement-notices> at 19 December 2011.

See Copyright Act 1994 (NZ) s 122U, which provides that “An IPAP may charge a rights
owner for performing the functions required of IPAP under sections 122A to 122T.”
Where an account holder is within an on-notice period, those sections expressly provide
that the IPAP is not required to issue a notice. See Copyright Act 1994 (NZ) s 122C(4).

See eg Gregory White, IPv4 VS IPv6 (2001) informIT
2011.

See Press Release: Available Pool of Unallocated IPv4 Internet Addresses Now
Completely Emptied (2011) The Internet Corporation for Assigned Names and Numbers

Gregory White, IPv4 VS IPv6 (2001) informIT
2011.

MED confirms talks about centralised copyright notice system (2011) Tech Liberty NZ

See Copyright Act 1994 (NZ) s 122A.

See eg NZ Legislation shifts file-sharing from bittorrent to tunnels (2012) 1_through_8
<http://1through8.net/blog/2012/2/8/nz-legislation-shifts-file-sharing-from-bittorrent-to-
tunnel.html> at 21 March 2012.


<http://documents.envisional.com/docs/Envisional-Internet_Useage-Jan2011.pdf> at 12 December 2011. Note that this report was commissioned by NBC Universal, a large-scale
right holder.

Internet traffic reportedly fell some 2-3% in the immediate wake of the Megaupload
shutdown. However, traffic levels very quickly recovered, with this study showing that it
was simply redistributed to other providers of infringing content: Kevin Fogarty,
MegaUpload takedown didn’t slow pirate downloads, just moved them offshore (2012) ITWorld
<http://www.itworld.com/security/247998/megaupload-takedown-didnt-slow-pirate-downloads-just-moved-them-offshore> at 21 March 2012. The medium and long-
term effects of the legal action against Megaupload on the availability of infringing
content via filelockers remain unclear.
Forums › New Zealand Broadband › Keen to hear from anyone that receives a copyright infringement notice (2011) geekzone

Netflix rules out New Zealand launch - Broadband too slow, can't get content rights (2011) reddit New Zealand

Sharky, Speed Up Your Torrent Downloads, Get a Seedbox (2008) TorrentFreak

Policy environment for Internet number resource distribution in the Asia Pacific (2011) APNIC


Ernesto, Busted: BitTorrent Pirates at Sony, Universal and Fox (2011) TorrentFreak


New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083 (Dr Wayne Mapp).

New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083 (Gareth Hughes).

Claire Rogers, Online purchases 'a rip-off' (2011) Stuff

Natalie Apostolou, Netflix rules out Kiwi launch (2011) The Register

New Zealand, Parliamentary Debates, House of Representatives, 12 April 2011, 18083 (Gareth Hughes).


See above n 1.

See eg Cecilia Kang, USTR: Acta won't include three-strikes; draft available in days (2010) Washington Post
<http://voices.washingtonpost.com/posttech/2010/04/ustr_acta_wont_include_three-s.html> at 16 December 2011.


Nicolas Suzor and Brian Fitzgerald, 'The legitimacy of graduated response schemes in copyright law' (2011) 34(1) University of New South Wales Law Journal 1, see particularly discussion at 6-25.

Frank LaRue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2011) United Nations General Assembly Human Rights Council


Reported at ‘Massive blow’ to music industry as Eircom anti-piracy measures rejected (2011) The Journal at 19 December 2011 (full ruling not publicly available)


Netflix rules out New Zealand launch - Broadband too slow, can’t get content rights (2011) reddit New Zealand at 13 December 2011.

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

INTRODUCTION

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

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

Thus, two basic legal models have evolved which can tackle the problem of unlawful P2P distribution; safe harbour copyright remedial limitations and graduated response regimes in public law. At a time when Australia is grappling with what to do about that problem, it is timely to consider in some detail the provenance and the contours of the two ‘original’ models – the US safe harbour and the French graduated response regime. That consideration enables deeper thought about the open questions at hand in Australia: what might occur in Australia in the aftermath of the High Court’s denial of ISP copyright liability in Roadshow Films v iiNet?
This essay attempts that exercise, with a focus upon some of the key drivers that helped to shape the US safe harbour and the French HADOPI laws and explains the application of both regimes to the problem of unlawful P2P distribution. In so doing some concluding observations can be made about the ramifications of the High Court’s decision upon efforts to resolve the problem in Australia, and the type of posture that may be required from the Australian government for progress to be made here.

THE AMERICAN SAFE HARBOUR

THE ORIGIN OF THE US SAFE HARBOR REGIME

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

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

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

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

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

A – facilitating transitory digital network communications;
B – the provision of system caching;
C – storing material on systems or networks at the direction of users;
D – the provision of online location tools.
Each category has its own array of conditions that the service provider needs to satisfy to be eligible for the immunity. However, one condition that applies for all categories is that the service provider ‘has adopted and reasonably implemented, and informs subscribers and account holders of the service provider’s system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers’.4

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

(i) whether it is plausible that direct liability alone against actual infringers would be effective;
(ii) would the creation of indirect liability deter the infringing conduct at a lower cost than direct liability alone;
(iii) would the creation of indirect liability assist the party incurring the liability in making an efficient decision to avoid that liability; and
(iv) would the creation of indirect liability interfere unreasonably with legitimate activity (Arrow et al 2005).

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

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

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

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

(i) secondary liability from category A activities – facilitating transitory digital network communications; or
(ii) direct liability from category C activities – storing material on systems or networks at the direction of users.

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

**Liability for P2P transmissions: category A activities**

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

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

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

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

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

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

**Inducement liability** requires, in the ISP-P2P setting, that the ISP both supplies the facility that may be used to commit direct infringement and does so with the intention of promoting that infringement. Such an intention could be evidenced by assessing the totality of the conduct (including omissions to act), statements and any financial benefit accruing to the alleged inducer. In *Grokster*, the defendants had specifically targeted users of another P2P network (Napster) that had been effectively shut down by prior rights holder legal action, failed to attempt to develop filtering tools and sold space for advertising that would be directed at their P2P users.2 Notably, the creation of copyright inducement liability was a response to the Supreme Court’s acceptance of the inapplicability of either contributory or vicarious liability to the P2P software publishers. Would such liability be apt for in the ISP-P2P setting? It seems highly unlikely, as it is improbable that any mainstream ISP would ever engage in conduct that is tantamount to actively promoting P2P infringement.
The consequence of this analysis is that an ISP in the US, when it acts as a category A conduit in relation to P2P infringements occurring over its customers’ connections, has no obvious secondary liability for those infringements. Importantly, this conclusion stands even if rights holders acted (as did the rights holders in the Roadshow Films v iiNet litigation) to furnish the ISP with weekly information about those P2P infringements. To the extent liability is conceivable in that setting under the current state of US law, contributory (rather than vicarious or inducement) liability seems the most plausible form of liability. Such a notice stratagem would likely give rise to complex questions in the US about the scope of contributory liability in such a setting. As Elkin-Koren (2006, 37) observes, since ISPs supply services capable of significant non-infringing uses contributory liability would require establishing ‘reasonable knowledge of specific infringing files’ at the time during which the ISP defendant materially contributed to the infringement.

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

**Liability for ‘making available’ via P2P: category C activities**

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

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

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

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

In *Re Charter Communications* the Eighth Circuit by majority agreed, observing that ‘as a court we are bound to interpret the terms of the statute and not to contort the statute so as to cover the situation presented by this case’ (393 F 3d 771, 777 (2005)). As a consequence of these cases, rights holders have reverted in P2P cases to the long-established litigation procedure of seeking, in actions against John Doe, the issue of subpoenas requiring John Doe’s identity.
Doc’s ISP to divulge the defendant’s actual identity (Brenner 2012). And significantly, an implication of the decisions is that a subscriber’s making available of files on a P2P network does not involve the relevant ISP in any Category C activity that could give rise to liability in the ISP.

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

THE 6 JULY 2011 MEMORANDUM OF UNDERSTANDING

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

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

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

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

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

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

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

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

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

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

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

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

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

THE FRENCH GRADUATED RESPONSE

THE ORIGIN OF THE HADOPI REGIME

In 2007 President Sarkozy commissioned a report by a group of experts and industry leaders, headed by Denis Olivennes, on the ‘Development and Protection of Culture on New Networks’. The resulting Olivennes Report had such an impact that the French President, prior to its publication, personally oversaw what has become known as the Olivennes Agreement.15 The Olivennes Agreement, arrived at on 23 November 2007 between the French government, ISPs and rights holder groups, was underpinned by the key recommendations of the Olivennes Report. Many of those recommendations were directed at accelerating the availability of content through lawful online avenues and the removal of technological protection measures upon music catalogues. However the final recommendation was that a warning and sanction mechanism should be established – with sanctions including the
suspension of a subscriber’s ISP account – in which the mechanism would apply to all providers of internet access and might require the establishment of an independent authority (Olivennes Report 2007, 25).

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

- The maximum criminal penalties for online copyright infringement were a €300,000 fine and three years imprisonment. However these were maximum penalties that French courts resisted applying for non-commercial P2P infringement, as they were disproportionate given the commonality of such infringement. Further, it noted that a legislative attempt to create in 2006 a small-fine regime for online infringers – €38 for downloads and €150 for uploads – had been ruled unconstitutional on the basis that online infringers should not be treated more leniently than other infringers. (Olivennes Report 2007, 7)

- Technical filtering of unauthorised material on P2P networks by cooperation between ISPs and rights holders was not yet a technically feasible approach. (Olivennes Report 2007, 27-31)

- The then operation in the US of safe harbour mandated repeat infringer account termination policies instituted by ISPs under their contractual terms of service with subscribers. The Report noted that both punitive account terminations, and the necessity of correlating reported IP addresses to subscriber identities, were considered virtually impossible for an ISP to justify doing under French law solely on the basis of a contractual power. That was because, under French human rights protections, penal measures and matters affecting online privacy required the intervention of a judge or public authority. (Olivennes Report 2007, 17)

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

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

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

> Our country possesses one of the strongest content industries in the world, and this agreement provides an opportunity for the preservation and development of the cultural identity and influence of France and Europe. Our country also benefits from having one of the most developed broadband Internet access industries in the world, which is a considerable competitive advantage in the virtual economy. These strengths should not cancel each other out, but rather should complement each other in the best interests of the consumer who will therefore have both powerful distribution networks and richly diversified content.
Notably, the sentiment expressed here is consistent with a philosophy expressed at the conferences revising the Berne Convention – a good example being comment made almost 100 years earlier at the Berlin revision conference when a free exception to copyright for the mechanical reproduction of musical works was abolished. At that time it was stated:

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

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

**THE FEATURES OF THE HADOPI REGIME**

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

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

**THE POLITICS AND EFFICACY OF HADOPI**

This regime was initially enacted in May 2009 in a somewhat different form; after the third notice within a year HADOPI could itself order up to a one-year suspension of Internet access for breach of the duty to supervise. A June 2009 constitutional ruling, however, found that aspects of the regime were invalid; effectively only a judge (not the HADOPI) could order suspension of Internet access and that, in any event, a 12-month suspension for breach of the duty to supervise was a disproportionate penalty (Jančić 2010, 452-454). More fundamentally the same ruling gave two important validations of the approach underpinning the HADOPI
First, it found that the duty to supervise was a validly enacted obligation. Second, it
found that the regime struck a correct balance with privacy interests. The necessary revisions
– reducing the suspension term to one month and vesting power in a judge – were made by
the French Parliament in September 2009. Further constitutional review in October 2009 left
the revised laws largely undisturbed, and these remain current.

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

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

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

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

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

The most interesting, and potentially surprising, part of this conclusion is that
the study occurs before anyone received a third notice (i.e. before any cases have
been referred to the criminal court), and that the increase in sales is observed
even before the law’s final passage. While this may seem irrational, it is
consistent with the idea that increasing the salience of the law, the illegality of piracy, and the potential penalties is sufficient to change user behaviour. (Danaher et al 2012, 19)

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

CONCLUSION

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

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

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

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

At a public seminar in May 2012 on the High Court Roadshow Films v iiNet decision and its ramifications, speakers included both Chief Executives of the main negotiating bodies – the
Australian Federation Against Copyright Theft and the Communication Alliance. There, one aspect of the negotiations was exposed for all to see: who pays? The Communications Alliance set out the following as a hypothetical trial of ISPs passing on rights-holder notices to their subscribers: 50,000 notices at a cost of $40 per notice; $250k contribution to education and appeal mechanism; total cost to rights holders of $2.25m. Implicit in this proposal is a view that because an ISP has no liability in the ISP-P2P setting – or to use the phrase adopted by Gummow and Hayne JJ in Roadshow Films v iiNet, the ISP owes no ‘duty of care’ to rights holders – then any cooperation is being done as a matter of favour, and that an ISP’s cost of so doing should be fully indemnified by rights holders.

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

REFERENCES

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


---

**ACKNOWLEDGEMENTS**

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

---

**ENDNOTES**


2. The provisions of Part V Division 2AA relating to any such code require (by regulation) that ‘it must be developed through an open voluntary process by a broad consensus of copyright owners and carriage service providers’, and be registered by the Australian Communications and Media Authority (ACMA) under processes specified in the Telecommunications Act 1997: *Copyright Regulations 1969* (Cth) reg 20B.
3. Australia-United States Free Trade Agreement 2004, article 17.11(29).

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


7. Compare *Ellison v Robertson*, 357 F 3d 1072, 1077 (2004) where it was held that had ‘a reasonable trier of fact could find that [the ISP defendant] had reason to know of potentially infringing activity’.


11. Copyright Act 1976 (US), §512(h).

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


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


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


In *iiNet*, the High Court held that current Australian copyright law is powerless to prevent large-scale peer-to-peer (P2P) infringements. A similar conclusion was previously reached by the Irish High Court in the *UPC* decision. This article compares and contrasts the two decisions, finding that the judges in both cases came to a number of similar conclusions. The article also explains how dealing with large-scale P2P infringements requires a combination of appropriate regulation, partnerships between the telecommunications and content industries and education. It concludes that, as in Ireland, legislative reform is needed to deal with the problem of P2P file-sharing.

**INTRODUCTION**

The High Court decision in *Roadshow Films Pty Ltd v iiNet Ltd* ((2012) 286 ALR 466) (*iiNet*) was not the first judicial outcome in which a court ruled that it was powerless to prevent peer-to-peer (P2P) infringements of copyright by imposing obligations on ISPs and that the respective Copyright Acts were not readily suited to enforce the rights of copyright owners in respect of well-known widespread P2P infringements. The *EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd* ([2010] IEHC 377) decision (*UPC*), handed down by Charleton J of the Irish High Court in October 2010, was remarkably similar in many ways to the *iiNet* case, and provides an interesting counter-point to the Australian High Court decision. This article compares and contrasts the two cases, in relation to both the evidence of large-scale infringements and the inadequacies of the current law to deal with the problem. The article then explains how dealing with large-scale infringements requires a coordinated strategy, incorporating regulation, partnerships between the telecommunications and content industries, and ongoing consumer education.

**ACCEPTANCE OF EVIDENCE ON P2P INFRINGEMENTS**

Both *iiNet* and *UPC* involved widespread P2P infringements occurring across an ISP’s network, based on infringing files found by users accessing a notorious international website, The Pirate Bay. In *UPC*, Charleton J recognised that the Irish music industry and other creative industries were being ‘devastated by piracy’ and, in the case of the ISP in question:

...a substantial portion of its 150,000 customers, or the children in their teenage and twenties years of these customers, are using the internet service provided by UPC to steal copyright material which is the property of the recording companies” ([2010] IEHC 377, [8]).

Ironically Charleton J even compared the widespread infringements in Ireland to those in Australia ([2010] IEHC 377, [16]).
From evidence presented to the court, Charleton J concluded that ‘the large majority of the current use of peer-to-peer technology was for the purpose of illegally downloading copyright material’ ([2010] IEHC 377, [39]). He was furthermore convinced that UPC was fully aware of the infringements occurring across its network and that the ISP had even ‘considered whether it is making a profit from it’ ([2010] IEHC 377, [18]).

Both the majority (French CJ, Crennan and Kiefel JJ) and minority (Gummow and Hayne JJ) judgments in the iiNet case recognised that by mid-2008 more than half the usage of iiNet’s traffic by volume was BitTorrent file sharing and that ‘it was common knowledge that the BitTorrent system was used for infringing activities’ ((2012) 286 ALR 466, 476). In this, the High Court merely reiterated the evidence provided by iiNet’s CEO under cross-examination.

In both the UPC and the iiNet case, the applicants used the same vendor (DtecNet) to provide the requisite evidence and in both cases the accuracy of the DtecNet data was recognised by the Court. For example, in UPC, Charleton J found the DtecNet evidence ‘to be accurate’ and that ‘there was no question put which undermined the reliable nature of that system’ ([2010] IEHC 377, [81]).

In iiNet, although the High Court, like the majority in the Full Federal Court, was critical of the level of information provided to iiNet prior to the ‘filing of experts’ reports in the proceedings’ ((2012) 286 ALR 466, 485), which subsequently explained the methodology used by DtecNet to obtain the comprehensive evidence data, the accuracy of the evidence of infringement was not disputed. In any event, it remains questionable whether the provision of the expert reports prior to filing the lawsuit would have had the effect anticipated by the Court, as iiNet had made it known to AFACT (in earlier correspondence) that it, in fact, understood how AFACT came to its allegations ((2011) 275 ALR 1, 72) and, moreover, confirmed that it would not be taking any action in relation to the notices and that there was no additional information that would change its position ((2011) 275 ALR 1, 23-24; 71-73; 128).

Importantly, the minority judgment in iiNet also observed that, based on the quality of the evidence presented by AFACT, ‘injunctive relief on a quia timet basis would be available’ ((2012) 286 ALR 466, 488). In the UPC case, on the other hand, Charleton J determined that he was not in a position to grant injunctive relief to the recording companies against internet piracy ‘even though that relief is merited on the facts’ because Irish copyright law was not yet fully compliant with its obligations under European law ([2010] IEHC 377, [138]). On this basis, Charleton J concluded that, ‘(l)egislative intervention was required…to protect constitutional rights to copyright and foster the national resource of creativity’ ([2010] IEHC 377, [131]).

**INADEQUACY OF THE CURRENT LAW**

In iiNet, both the majority and minority judgments found that the legislation, and particularly s101(1A) of the Copyright Act, did not impose a positive obligation on ISPs to prevent P2P infringements by subscribers, effectively rendering the protections under section 112E and the safe harbour regime unnecessary. It is to be recalled that the Full Court found that neither s 112E nor the safe harbour provisions were available to iiNet: findings that were not challenged in the High Court.

From this, the majority in iiNet concluded that, ‘…the concept and 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’ ((2012) 286 ALR 466, 486). It is important to read the conclusions of the Court on this point carefully. First, the majority acknowledged that it is not cost-effective or practical to bring actions against individuals ((2012) 286 ALR 466, 480-1). Secondly, in determining whether or not iiNet had taken reasonable steps under section 101(1A)(c), the majority pointed out that the absence of an industry code of practice, which is already referenced in that paragraph, was an important consideration ((2012) 286 ALR 466, 484).
The High Court’s decision should therefore be interpreted as unambiguously concluding that, in the absence of a relevant code of practice for ISPs, the scheme established by the Digital Agenda Act and supplemented by the safe harbours had failed, at least in relation to P2P infringements. Australian Courts were thus powerless to order iiNet to take any action, despite widespread infringement occurring on iiNet’s network of which iiNet was aware ((2012) 286 ALR 466, 488), despite iiNet’s capacity to identify and communicate with account holders (at 475; 482), despite iiNet’s technical ability and contractual right to prevent such infringement (at 487) and despite the fact that iiNet had no ‘safe harbour’ policy in place under Div 2AA of the Act (at 500). In the face of the large-scale infringements acknowledged by the Court, this seems to point to a failure of the current legislative regime – and especially the Digital Agenda Reforms and the safe harbour regime – to deal with a substantial problem that was not adequately anticipated.

WHERE TO NEXT?

Following the decision of the High Court in iiNet, we are left with a legislative regime that, in its current form, is unable to deal with large-scale P2P infringements. So, where to next?

There is no ‘one’ silver bullet. Preventing online content theft requires a coordinated strategy that involves regulation, content and telecommunication industry partnerships and ongoing education campaigns, that clearly identify the positive outcomes for consumers that come from valuing intellectual property rights.

INDUSTRY PARTNERSHIPS

Interestingly enough, content and telecommunications companies are no longer on opposite sides of the ‘net’. As convergence becomes a reality, telecommunication companies are getting into the game of content distribution. We are fast adopting the same game plan – to monetise content.

The commercial partnership between the technology sector and the content industry has already resulted in highly sophisticated business models that ensure that multiple business objectives are met while delivering films and TV shows to consumers. To suggest that the content industry simply reduces its already competitive prices and makes all content immediately available across all delivery platforms over-simplifies what is a sophisticated business sector, which is all too familiar with keeping their audience happy with quality entertainment.

The telecommunications and technology sectors have been working hand in hand with the content industry for years to deliver attractive means for Australian audiences to enjoy content when they want it and where they want it: Foxtel, Telstra T-Box, Apple TV, ABC iView, Crackly, smh.tv, Fetch TV, fixplay, iTunes, Mubi, Quickflix and YouTube. Australian movie and TV rentals all combine new technology with tailored content offerings to meet an ever increasing and recognised demand.

Hollywood movies are now increasingly screened in Australia cinemas ‘before’ they are released in the United States. Last year, of the 10 most popular films in Australia (by MPDAA box office receipts) 70% were released in Australia before the United States. (MPDAA 2012)

Such wider availability of movie and TV content is being recognised by Australian consumers. Independent research conducted on behalf of the Intellectual Property Awareness Foundation found that 78% of Australians agreed that there are now an increasing number of online options for people to legally obtain and watch TV series and movies (IPAF2012).

But why would the movie and TV industry go through the trouble and expense of investing so heavily in quality content and making that content available across differing delivery platforms if that same content could be siphoned off and distributed illegally? The ability of the film and TV industry to continue to deliver high quality entertainment to consumers in
flexible ways and at variable price points is dependent upon our ability to protect our content. Commerce only succeeds in a free market economy, not a free-for-all economy. The content and telecommunications industry needs to work together to find smart and practical ways to protect creative content. In doing so we’ll not only protect Australian jobs and legal content but also ensure that the internet works for everyone.

The telecommunication industry has started to recognise this and in some jurisdictions is protecting the content which has become an integral part of their business model. On May 31 the United Kingdom ISP, SKY, in following other UK ISPs and complying with a court order to block ‘The Pirate Bay’, issued the following statement:

*We have invested billions of pounds in high-quality entertainment for our customers because we know how much our customers value it. It’s therefore important that companies like ours do what they can, alongside the government and the rest of the media and technology industries, to help protect their copyright. Such protection makes sure that consumers continue to benefit from TV programmes, movies and music both now and in the future. These means taking effective action against online piracy and copyright infringement* (SKY 2012).

**THE COOPERATIVE US MODEL**

In the United States, constructive discussion between the movie and music industry and the five major ISPs, following consultation with consumer groups, resulted in an effective and proportionate graduated response framework being voluntarily agreed upon and importantly co-funded. In April this year the Centre for Copyright Information (CCI), the body responsible for managing the voluntary US copyright alert system was announced (CCI 2012). The CCI’s Advisory Board includes representatives from open Internet advocacy groups (including Public Knowledge) as well as consumer groups.

The purpose of this co-funded US copyright alert system is not to punish but to educate subscribers about copyright and the many sources of legal content available, as well as to help them guard against the risks of illegal file sharing. The copyright notice system consists of 4-6 copyright alerts, issued at the discretion of each ISP. If, after these educational and acknowledgment alerts, the subscriber’s account still appears to be engaged in illegal file sharing, the ISP may institute ‘Mitigation Measures’. These Mitigation Measures (imposed solely at the discretion of the ISP) may include, for example: temporary reductions of Internet speeds, or redirection to a landing page until the subscriber contacts the ISP or reviews and responds to educational information about copyright. It must be noted that ISPs are not required to impose any Mitigation Measure which would disable or be reasonably likely to disable the subscriber’s voice telephone service (including the ability to call emergency services), e-mail account, or any security or health service. A dispute resolution process is also inherent in the framework. Before a Mitigation Measure is imposed, a subscriber may request for an independent review, which will be undertaken by a qualified and independent entity.

Australian research suggests that such a copyright alert framework would be effective here with most users (more than 70%) saying that they would stop illegal file sharing once alerted that it is occurring, that it is illegal and in breach of the ISPs terms and conditions, and that there are consequences associated with continuing to engage in it (IPAF 2012, 40). This clearly begs the question of why some Australian ISPs have seemingly rejected what their US counterparts, consumer groups and open Internet advocacy groups accept is a fair and equitable approach?
EDUCATION AND AWARENESS

In addition to content and telecommunication industry partnerships, a longer-term solution to deterring online content theft is education and awareness. It’s not about placating rights holders but, more importantly, ensuring communities value intellectual property in the digital age.

There is now a generational shift from a generation that values ownership of content to a generation that values access to content – but with this shift has also started to come an expectation of getting something for nothing. In his book, Free Ride, Robert Levine writes: ‘By making it essentially optional to pay for content, piracy has set the price of digital goods at zero’ (Levine 2011, 3). The expectation of getting something for nothing is an unfortunate by-product of the Internet era and has created a legacy that has begun to devalue quality entertainment products.

When generally law-abiding citizens access content illegally online, it’s not simply a question of availability. That may be a common excuse or, more to the point, a ‘convenient excuse’. The primary reason given by illegal downloaders for accessing content illegally is because they can get it without having to pay for it (IPAF 2012, 44).

The film industry recognises that we have a role to play in making consumers aware of the wide variety of places where they can get legal content without any of the online risk involved in engaging with ‘pirate’ sites – the same websites that place consumers at a very real risk for identity theft, fraud and damaging privacy violation. Confirming this, McAfee research concluded that entering ‘free’ into Google along with any other term (whether it be movie, music or video) will increase by threefold the likelihood of being redirected to a malicious website that will infect your PC or mobile device and attempt to acquire your personal information (Greve 2010, 13). Malware designers and hackers know where Internet users like to go and what key words they like to use. Symantec, for example, recently issued a media advisory on the teenage phenomenon, Hunger Games (Symantec 2012). It found that searches related to ‘free’ copies of the movie were turning up malicious results with poisonous links designed to infect the users’ computers, smartphones and tablets.

The film industry needs to ensure that our consumers are aware of the role of copyright and the contribution that their choice and responsible use can make to the future of content. Some say that reinforcing the value proposition for intellectual property is too much of a challenge. However the alternative, where creativity is no longer respected and digital content has zero value, is not to the advantage of anyone. A long-term sustainable content industry is in the interests of rights holders, telecommunication and technology companies and most of all to consumers who enjoy quality entertainment.

REGULATION

Which leaves us with the third silver bullet – regulation.

Sixteen months after Charleton J found in the UPC case that Irish copyright law was not compliant with its obligations under European law and that legislative intervention was required, the Irish Parliament signed into law the European Union (Copyright and Related Rights) Regulations, which allow for member states to ‘ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe copyright’.

Sixteen months from judgment to legislative fix.

CONCLUSION: THE NEED FOR REFORM

And, so, what are the ultimate lessons to be learnt from the High Court decision in iiNet? Firstly, the statutory framework has now been fully tested through every available level of court in the country. Secondly, the High Court has recognised that the existing framework is
Inadequate to address the issue of P2P infringement (and may never have been specifically designed to do so). Thirdly, the High Court has unanimously identified the need for legislative change. And finally the policy justification for legislative action is overwhelming.

In the Digital Economy: Future Directions report, the government has already recognised that ‘content is the key driver of digital economy growth’ (DBCDE 2009, 36) and, in turn, ‘the digital economy is essential to Australia’s productivity, global competitiveness and improves social well-being’ (DBCDE 2009, 1). With the roll out of the NBN the government cannot ignore the conclusions reached by the High Court and delay on this critical issue.

As observed by Gummow and Hayne JJ, this issue ‘is best resolved by legislative processes rather than by any extreme exercise in statutory interpretation by judicial decisions’ ((2012) 286 ALR 466, 495). While regimes are being put in place in other parts of the world to effectively deal with copyright infringements, now that the law has been tested and found wanting, it is important Australia not fall behind.

REFERENCES


CASES

EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd ([2010] IEHC 377)

Roadshow Films Pty Ltd v iiNet Ltd ((2012) 286 ALR 466)
ENDNOTES

1. 50% of iiNet’s traffic was BitTorrent: ((2012) 286 ALR 466, 476; 488).
INTERNET USERS AND COPYRIGHT
SHOULD WE HAVE AN INDUSTRY CODE?

Holly Raiche
University of New South Wales

After three judgments between 2010-2, Roadshow has provided much needed clarity on what Internet Service Providers (ISPs) should – or should not – do when informed of alleged infringing activity by their customers. The judgments have also made useful suggestions on what an industry code for ISPs would look like. What is missing is a clearer understanding of the third parties in these debates – the public – the users. How do they use the Internet? What do they know of copyright? And if a code for ISPs is developed, how should it protect public rights to fair access to Internet content?

COPYRIGHT – A QUESTION OF BALANCE

Copyright legislation strikes a balance of competing interests and competing policy considerations. Relevantly, it is concerned with rewarding authors of original literary works with commercial benefits having regard to the fact that literary works in turn benefit the reading public.

In both its title and opening recitals the Statute of Anne of 1709 (sic) echoed explicitly the emphasis on the practical or utilitarian importance that certain seventeenth century philosophers attached to knowledge and its encouragement in the scheme of human progress. The "social contract" envisaged by the Statute of Anne, and still underlying the present Act, was that an author could obtain a monopoly, limited in time, in return for making a work available to the reading public.¹

The original technical advance that, ultimately, let to the passage of the Statute of Anne was the printing press. As new technologies such as the ‘jukebox’², the photocopier³, or DVDs⁴ are developed, the balance between a creator’s rights and public access to information – the “social contract” – must be continually redrawn. The task is becoming increasingly important – and challenging - in the world of the Internet and the access it provides to content.

The challenge for copyright law in this new environment is to demonstrate that it can continue to effectively provide a just and acceptable balance between the valid interests of intellectual property rights owners and the public interest in fair and reasonable access to a wide range of information. (Copyright Convergence Group 1994, 7)

The focus of this article is the public interest side of that balance; in an Internet world, how should rights holders be able to protect their legitimate rights in a way that honours the public’s fair access to Internet content.

USE OF THE INTERNET

Australians are using the Internet for an increasingly wide variety of purposes. Top of the list is emails, closely followed by banking, checking information (such as sports, weather, maps), and making travel arrangements. (ACMA 2008, 5; Figure 2) There are differences in the way different age groups use the Internet. Top of the list for all age groups is still email, but for
younger users (age 16 to 24), streaming video and audio and downloading podcasts rate more highly than for other age groups (ACMA 2008, 18; Table 3). When focusing specifically on young people’s Internet usage over a three-day period, the highest usage was for homework, followed by messaging/chatting, followed by social websites and blogs. Usage for emails, and gaming came next, followed by watching/listening to video/audio clips. (ACMA 2008, 12; Table 3)

What this suggests in the copyright context is that while the Internet meets a range of communications needs for the public, access to copyright material (legally or otherwise) still makes up a smaller part of people’s Internet use than access to other information and services.

IMPACT OF PIRACY

Rights holders nevertheless point to the large and detrimental impact Internet piracy has and will have on the creators and publishers of original works.

The Australian Content Industry Group commissioned Sphere Analysis to undertake such a study. The conclusions were that, in 2010, over 4.7 million Australian Internet users accessed online content illegally, that the value of lost retail sales to content industries was $900 million, over 8,000 jobs in those industries were lost as a consequence and the annual impact of Internet piracy to the Commonwealth Government revenue was $190 million. (Sphere 2011, 3 and 5-8) By 2016, the figures would be much worse. Up to 8 million Internet users would access online content illegally, the value lost would be up to $5.2 billion, with a further 40,000 jobs lost and a loss to the Commonwealth of $1.1 billion. (Sphere 2011, 3 and 9-11)

The Australian Federation Against Copyright Theft (AFACT) also commissioned a study on the economic consequences of movie piracy in Australia. Again, the consequences of infringing downloading of movies were found to be dire. The equivalent of 6,100 full time jobs was lost in the 12 months leading up to the third quarter of 2010, with loss of sales of $1,370 million, and tax losses up to $193 million. (Ipsos Media 2011, 3)

The UK Hargreaves Report, however, questions evidence for online piracy in the UK.

*Given its importance, you would think that we would have a very clear picture of the scale and dynamics of online piracy, but this is not so. There is no doubt that a great deal of piracy is taking place, but reliable data is surprisingly thin on the ground. There is no shortage of claims about levels of infringement, but in the Review’s four months of evidence gathering, we have failed to find a single UK survey that is demonstrably statistically robust. For many surveys, methodology is not available for peer review.*

Measurement of any area of unlawful activity presents statistical challenges: these are not new problems in the world of criminology, where policy analysts are used to drawing different lessons from surveys of victims of crime, general social surveys about crime and policy recorded levels of crime. However, for online copyright infringement, there are further complications:

- the offence leaves no physical trace
- surveys question respondents who have an imperfect understanding of what is within the law in the first place and may be motivated either to deny taking part in any unlawful activity or to exaggerate doing so;
- free downloads are not necessarily illegal and paid for downloads are not necessarily legitimate;
- what is legal in one country may not be in another and the internet allows businesses and consumers to trade across boundaries;
- not all P2P file sharing is illegal and not all illegal activity is conducted via P2P (in fact P2P file sharers appear to be moving to other means of accessing music including live streaming);
studies that have attempted to measure piracy by measuring Internet traffic are problematic because other factors affect traffic levels including changes in volume of spam and increases in broadband speed, which permit much greater volumes of activity and especially higher density video files. (Hargreaves 2011, 69; para 8.10)

The same complications on measuring online infringement would apply equally in Australia. If, therefore, there is a conclusion on the incidence of online piracy and its impact on content owners and the economy more generally, it is only that there is piracy and it has impacts. But with the questionable level of both, there must be caution in any regulatory response.

The other reason for caution in any regulatory response is the increasing difficulty in understanding what amounts to infringement. Clearly, there is a section of the public that uses the Internet to download content in ways that they know violate the content owner’s rights. But, as the Hargreaves report notes, from the average Internet user perspective, it is not easy to understand what is or is not legal in the copyright context.

A second and also significant problem is that we have in recent years witnessed a growing mismatch between what is allowed under copyright exceptions and the reasonable expectations and behaviour of most people. Digital technology has enabled use and reuse of material by private individuals in ways that they do not feel are wrong – such as sharing music tracks with immediate family members, or transferring a track from a CD to play in the car. It is difficult for anyone to understand why it is legal to lend a book to a friend, but not a digital music file. The picture is confused by the way some online content is now sold with permissions to format shift (iTunes tracks) or to ‘lend’ files (Amazon ebooks) at no extra cost. This puts the law into confusion and disrepute. (Hargreaves 2011, 43 para 5.10)

Confusion on the law in an online environment makes its enforcement problematic at two levels: ensuring that the copying amounts to infringement, and then enforcing it.

In an online environment, the options for content owners enforcing their rights include actions against the providers of the connectivity between the user and content, against Internet intermediaries such as web hosts or search engines or against individual infringers.

Given the global reach of the Internet and the possibility of large numbers of people accessing potentially copyright material, there is little value in pursuing individual infringers. There is more value in pursuing the providers of software that enables copying or Internet intermediaries such as Google.

Increasingly, however, content owners try to involve ISPs in the enforcement of copyright. Specifically, the argument runs, that while the ISPs are not said to have directly infringed copyright, they have, through their action (or inaction) ‘authorised’ the copyright infringement by their customers.

The tests for whether a person has ‘authorised’ the infringement under the Copyright Act 1968 include the following:

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

(b) the nature of any relationship existing between the person and the person who did the act concerned;

(c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.

The High Court’s recent decision held that the ISP iiNet (and, by inference, ISPs generally) did not have the necessary power to prevent a customer from any infringing activity and could only stop any infringing activity indirectly, through the termination of a customer’s account.

That is, arguably, the first two limbs of the ‘authorisation’ test were not met. However, both the majority and minority judgments address the third limb of the test – an industry code, or lack thereof. Quoting from the majority judgment (emphasis added):

INTERNET USERS AND COPYRIGHT: SHOULD WE HAVE AN INDUSTRY CODE? 573
The nature of the internet, the BitTorrent system, and the absence of any industry code of practice adhered to by all ISPs are all factors which are relevant to the statutory task of assessing whether iiNet took reasonable steps to prevent or avoid the primary infringements, given its indirect power to do so.\(^{13}\)

**AN INDUSTRY CODE?**

In the copyright context, industry codes have been developed to codify an ISP’s responsibility when informed of their customers’ alleged infringing activities.\(^ {14}\) In the Australian context, a relevant industry code would set out any ‘reasonable steps’ an ISP should take ‘to prevent or avoid the infringing act, including whether the person complied with any relevant industry codes of practice’ under the Copyright Act.\(^ {15}\)

The Act goes on to define an industry Code to mean:

- an industry code that:
  - (i) meets any prescribed requirements; and
  - (ii) is registered under Part 6 of the Telecommunications Act 1997; or

- an industry code developed in accordance with the regulations.\(^ {16}\)

The relevant regulations are as follows:

For subparagraph (a) (i) of the definition of industry code in section 116AB of the Act, the following requirements are prescribed in relation to an industry code to which condition 2 of item 1 of the table in subsection 116AH (1) of the Act applies:

- (a) the industry code must be developed through an open voluntary process by a broad consensus of copyright owners and carriage service providers;
- (b) the industry code must include a provision to the effect that standard technical measures are technical measures that:
  - (i) are used to protect and identify copyright material; and
  - (ii) are accepted under the industry code or developed in accordance with a process set out in the industry code; and
  - (iii) are available on non-discriminatory terms; and do not impose substantial costs on carriage service providers or substantial burdens on their systems or networks.

In determining the remedies (and the limitations on remedies) available to the courts against carriage service providers (noting ISPs are a category of carriage service provider) for the transmission of infringing material, the relevant conditions that must be met include:

1. The carriage service provider must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers. (italics added)

2. If there is a relevant industry code in force, the carriage service provider must comply with the relevant provisions of that code relating to accommodating and not interfering with standard technical measures used to protect and identify copyright material.\(^ {17}\)

Emmet J, in the Full Court decision on iiNet\(^ {18}\) summarised the elements that should be included under an industry code before iiNet (or other ISPs) suspend or terminate a customer’s account under s. 101(1A)(c) as follows:

1) iiNet has been informed in writing of particulars of specific primary acts of infringement of copyright of the Copyright Owners, by use of particular IP Addresses of iiNet customers.
2) iiNet has been requested in writing to take specific steps along the following lines in relation to such primary acts of infringement:
   (a) iiNet should inform its customer of the particulars of the allegations of primary infringement involving the use of that customer’s iiNet account.
   (b) iiNet should invite the customer to indicate whether the service has been used for acts of infringement as alleged.
   (c) iiNet should request the customer either to refute the allegations or to give appropriate assurances that there will be no repetition of the acts of infringement.
   (d) iiNet should warn the customer that, if no satisfactory response is received within a reasonable time, perhaps 7 days, the iiNet service will be suspended until such time as a reasonable response is received.
   (e) iiNet should warn the customer that if there are continued acts of infringement by use of the service, the service will be terminated.
   (f) iiNet should terminate the service in the event of further infringements.

3) iiNet has been provided with unequivocal and cogent evidence of the alleged primary acts of infringement by use of the iiNet service in question. Mere assertion by an entity such as AFACS, with whatever particulars of the assertion that may be provided, would not, of itself, constitute unequivocal and cogent evidence of the doing of acts of infringement. Information as to the way in which the material supporting the allegations was derived, that was adequate to enable iiNet to verify the accuracy of the allegations, may suffice. Verification on oath as to the precise steps that were adopted in order to obtain or discern the relevant information may suffice but may not be necessary.

4) The Copyright Owners have undertaken:
   (a) to reimburse iiNet for the reasonable cost of verifying the particulars of the primary acts of infringement alleged and of establishing and maintaining a regime to monitor the use of the iiNet service to determine whether further acts of infringements occur, and
   (b) to indemnify iiNet in respect of any liability reasonably incurred by iiNet as a consequence of mistakenly suspending or terminating a service on the basis of allegations made by the Copyright Owner.

At the time of the High Court decision, no industry code that would meet the requirements of the Copyright Act (and Regulations) or Emmet J’s tests was in place. However, since the initial action was brought against iiNet there have been at least two Australian proposals for an industry code.

**PROPOSED CODES**

iiNet itself proposed a scheme that envisaged the creation of an independent body. It would receive information from the content owners about alleged infringement, pass that information to the relevant ISP for identification of the customer and, having received customer information, notify the relevant customer of the alleged infringement. The Independent body would have an oversight role in technical processes to determine both the accuracy of identifying alleged infringements by an IP address, and the matching of an IP address to a specific customer. It would also have a role in appeals by the customer. At no stage would either the content owner or the ISP contact the customer directly.
The telecommunications industry body, Communications Alliance, also developed a scheme to address online copyright infringement. (Communications Alliance 2011) The elements of their ‘Notice and Discovery’ Scheme are as follows:

- Rights holders participating in the scheme will provide details of the detection technology and processes they will use to generate infringement notices to the ISPs, with the technology independently audited and agreed upon with ISPs.

- Using the approved technology, rights holders will provide the relevant ISP with notice of the alleged infringing activity within 14 days of detection. Such notice will include:
  - The copyright work involved
  - The rights holder’s entitlement to the work
  - The IP address involved
  - The date and time of the alleged infringement

- Within 14 days of receipt of rights holder notice, the ISP must,
  - Send an ‘education’ notice to its account holder (the notice to include the copyright work involved, details of alleged infringing activity, the account holder’s rights of appeal and any further action to be taken by the ISP in the case of further infringing activity by the account holder); and
  - The ‘grace period’ allowed for account holder response to the notice; or
  - Advise rights holder of the ISP’s inability to match IP address to account holder.

- If, after expiration of ‘grace period’ and within the following 12 months, the rights holder provides a second infringement notice to the ISP involving the same account holder, the ISP is to send a ‘warning’ notice to the account holder including:
  - Mention of the previously sent ‘education’ notice
  - Notice of further alleged infringing activity
  - Other information (as per the education notice) including that failure to act may result in account holder details given to rights holder, who may take further action.
• Up to three warning notices can be sent to the alleged infringing account holder. After three notices are sent, the rights holder may apply (through an approved legal process) for account holder details. (Communications Alliance 2011, 5-8)

Both schemes have elements of Emmet J’s requirements. There are requirements on content owners for accurate, verifiable notifications of alleged infringements. There are requirements on ISPs to pass on notification of alleged infringing activity to the ISP customer, generally through a series of letters (with or without ISP letterhead on the notifications). There are avenues of appeal for the ISP customer. Particularly with the iiNet proposal, there is strong privacy protection as the customer’s details are not given to content owners. Generally, there is also recognition of the need for customer education on copyright.

Both proposals, however, shy away from Emmet J’s proposed sanction of ISPs terminating a customer’s service, even as a last resort. In the Communications Alliance proposal, any such action is left to the copyright owner’s enforcement action through the courts.

Coming from the Internet user perspective, the global Internet Society released a major paper on this issue. Its ‘working principles’ to address copyright infringement include the following elements:

• The need for an enforcement approach which is effective, efficient, replicable across jurisdictions and proportionate
• The need for awareness raising and education for Internet users
• Ensuring that the methods used for detection of infringing activity and of the alleged infringer are accurate and that stringent data protection rules and security are followed (noting that technical measures to combat online copyright infringement can be circumvented and will not prevent copyright infringement from occurring)
• The provision of stepped enforcement procedures by ISPs with an educative element (warnings followed by a sanction)
• Ensuring that enforcement procedures are is linguistically, socially, culturally and economically appropriate and do not unreasonably interfere with the business or activities of ISPs or other parties, do not diminish innovation and development of the Internet and are applied to proven, not suspected, infringement.
• Ensuring that sanctions are proportionate fair, appropriate and are applied with due process by an independent suitably qualified third party. (Internet Society 2011, 10-11, para 33). For a discussion of codes in overseas jurisdictions, see 26-37)

The Internet Society makes three important points in its principles:

• Although unstated, there is an implied recognition of the need for reward for creative endeavour and a way to ensure that intellectual property rights are respected
• Education and legal, affordable alternatives to infringing activities must be part of the answer
• There are still significant issues with sanctions, including technical limitations of detection processes, natural justice issues for the customer as well as respect for privacy rights.

Both the iiNet judgment at first instance and the High Court judgment recognised the growing importance of the Internet in people’s lives. As discussed above, downloading content (legally or otherwise) is still only a small part of how people use the Internet. The Internet is how people communicate (through VoIP services, emails, messaging or social networks), how they bank, do research, travel, etc. Quoting Cowdroy J from the judgment at first instance:

There are multiple uses for the Internet and there are multiple means to consume significant amounts of quota for non-infringing purposes. Even where there is evidence before the Court of accounts where infringing activity is occurring, the evidence does not suggest that a significant amount of quota was being used for the
purpose of infringing the applicants’ copyright. (Roadshow 2011, para 450. See also French CJ, Crennan and Kiefel JJ in the High Court judgment: Roadshow 2012, para 64)

After the High Court judgment in iiNET, arguably ISPs do not need the protection of a Code in order to be found not to have ‘authorised’ infringing activity of their account holders. However, the judgment of Emmet J specifically mentioned an industry code as part of the authorisation test and his judgment was not contradicted by the High Court.

For content owners, the most important advantage of a code would be the recognition that other industry sectors have a role to play in the fundamental principle of reward for creative endeavour. It would also provide the codification of what content owners can – and cannot – expect from ISPs in response to notices of alleged infringement. From an ISP perspective, a code would clarify their responsibilities (or not) in response to alleged infringing activities by their account holders – without the expense of litigation.

If a Code is developed, Emmet J’s judgment, the legislation and regulations, plus existing code proposals (discussed above) already point to its essential elements.

The regulations include the requirement that such a code is ‘developed through an open voluntary process by a broad consensus of copyright owners and carriage service providers.’ Clearly the other important group at that table must be Internet users.

The regulations also cover the importance of industry acceptance of technical measures used to protect and identify copyright material. Importantly for ISPs, the regulations also require that such measures ‘do not impose substantial costs on carriage service providers or substantial burdens on their systems or networks’.

From a user perspective, there are other essential elements to a Code.

- The Code must not equate account holder with infringer. The Internet connection may be a wireless router and used by many individuals – not just the alleged infringer. Even with a wireline connection, one computer may have many users.
- Privacy of account holder details must be respected. Only in the last instance, under judicial order (if ever) should account holder details be provided to content owners
- An account holder must have access to an affordable, accessible and speedy appeals mechanism
- Sanctions must be graduated, and must begin with a series of notification letters of infringing activities, with full details of the alleged infringement, appeals mechanisms available and further action that the ISP may take if infringing activity continues.
- Termination by the ISP of access to the Internet service must be a sanction of last resort. While the Act does include the possibility of ‘termination in appropriate circumstances’, there are other actions that should precede termination, including suspension, traffic shaping, blocking, etc. (Internet Society 2011, 22ff)

As discussed above, and mentioned in two of the three iiNet decisions, the public uses the Internet for a range of communications tasks; downloading content is just one of them and a lesser one at that. With the rolling out of the National Broadband Network, there will be one pipe into people’s homes that will carry most of their communications, including their access to medical advice and emergency services. Those lifeline services must never be cut.

CONCLUSION

Both in Australia and internationally, the response to online piracy has been a mixture of legislation and/or industry codes involving the detection of alleged infringing activity, identification and notification to the alleged infringer and possible sanctions for continued infringement. As many commentators have argued, however, the better long term response is not to rely on ISPs as enforcement agents. The better response will recognise that the Internet
is an integral part of people’s lives. People increasingly want to access their information and entertainment online, and increasingly, are prepared to pay to do so.

REFERENCES

ACMA. 2008. Telecommunications Today Report No 6 Internet Activity and Content, September

Communications Alliance. 2011. Australian Internet Service Provider (ISP) Proposal: A Scheme to Address Online Copyright Infringement, November

Copyright Convergence Group. 1994. Highways to Change: Copyright in the New Communications Environment, August


Ipsos MediaCT and Oxford Economics. 2011. Economic Consequences of Movie Piracy in Australia, January

Sphere Analysis. 2011. The Impact of Internet Piracy on the Australian Economy, February


CASES


IceTV Proprietary Ltd v Nine Network Australia Proprietary Ltd [2009] HCA 14


Roadshow Films Pty Limited v iiNet Limited [2011] FCAFC 23 (24 February 2011) (Full Court judgment)

Roadshow Films Pty Limited v iiNet Limited [2012] HCA 16 (20 April 2012) (High Court Judgment)

University of New South Wales v Moorhouse [1975] HCA 26,

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242

Viacom International Ltd v YouTube Inc, 2nd Circuit, Court of Appeal Docket No 10-3270-cv, 5 April 2012.

ENDNOTES

1 IceTV Proprietary Ltd v Nine Network Australia Proprietary Ltd [2009] HCA 14, at paragraphs 23-25.


5 The term piracy is used in this article to mean the unauthorised copying of works in contravention of (infringement of) the Copyright Act 1968.

6 The term ‘rights holder’ refers to the individual or organisation who, under the Copyright Act 1968, is authorised to use and/or publish works protected by that Act.

7 ISPs are a subset of carriage service providers, defined in s. 87 of the Telecommunications Act 1997.

8 Intermediaries include web hosts, search engine, ecommerce platforms etc. For a full list of the types of Internet intermediaries, see Weatherall 2011: 7-8. See also Attorney-General’s Department 2011: 3-4, in which the Department proposes expanding the safe harbour scheme so that it applies to a broader category of service provider, rather than just carriage service provider.

9 See, for example, Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005].

10 see Viacom International Ltd v YouTube Inc, 2012.

11 Copyright Act 1968 s 101(1A) The issues surrounding ‘authorisation’ are discussed elsewhere in this journal.


13 Ibid, paragraph 71. See also paragraph 139.

14 See discussion on ISP codes internationally later in the article.

15 Copyright Act s 101(1A)(c)

16 Copyright Act 1968 s. 116AB

17 Copyright Act 1968, c. 116AH(1)

18 Roadshow (2011) paragraph 210 ff.

19 The iiNet paper including this diagram was available on the iiNet website as at October 2011. <iiinet.net.au>. Interestingly, the proposal and diagram are no longer available on the iiNet website. See also <http://www.theaustralian.com.au/australian-it/piracy-dispute-panel-proposed/story-e6frgakx-1226048723392> on a similar scheme proposed by the Internet Society of Australia and the law firm Maddocks.

Optus' TV Now service sought to take advantage of the "home taping" or "time shifting" exception to copyright infringement provided by s 111 of the Copyright Act 1968 (Cth). It enabled its mobile phone subscribers to record free to air television programs from their mobile phones, with the ability to play them back at a later time. Once a subscriber selected a program for recording, it was recorded by an automated process on Optus' servers. A Full Court of the Federal Court has overturned the trial judge's finding that this service was legal. This article considers the Full Court's reasoning and the questions it raises for the concept of "making" under the Copyright Act.

INTRODUCTION

(1). Find a show in the Guide
(2). Press “Record”
(3). Watch your recorded show (later).

As you are snuggling back into your couch tonight and your better half insists that you are both going to watch Delta in The Voice, the three steps above fairly accurately describe your actions as you hastily try to set your DVR/PVR/VCR to record tonight’s footy game. First, you scroll through the electronic program guide (EPG) to find the channel it is on and the time it is scheduled for broadcasting. Next, you click on the button to (store the instruction to) record the broadcast. After the credits have finally rolled on scenes of the wildly clapping audience and other emotional highlights, you get to bring up the Playback menu and sit down to some real entertainment. Does it make a difference if you are not some middle-aged curmudgeon and instead you are down at the Bar having a drink, so you pull out your mobile phone and use Optus’ TV Now service?

Rares J, at first instance, held it did not. In a decision which potentially has ramifications far beyond the narrow question under consideration, the Full Court of the Federal Court has ruled that it does. Andrew Demetriou (the CEO of the Australian Football League) seeing a reported $153million from Telstra for the “mobile” rights under threat reportedly labelled Optus’ intention to seek special leave to appeal from that decision to the High Court, “stupid”, “disgusting” and “disappointing”. High drama indeed (as these things go).

SOME BACKGROUND

In 1984, the US Supreme Court ruled that taping broadcast television at home on a VCR to watch the program at a more convenient time did not infringe copyright. In Australia, section 111 of the Copyright Act 1968 already provided a specific defence for making copies at home for private and domestic purposes. In the typically cribbed and carping way we do these things, however, it provided immunity only against claims based on the copyright in the broadcast itself. The defence did not extend to copyright in the underlying works such as scripts, screenplays and cinematograph films. So, it was a defence only for broadcasts of
football games and other, unscripted events. “Home taping” a scripted program like Neighbours or The Big Bang Theory infringed copyright.

So far as I am aware, the copyright owners never sued anyone in Australia for such infringements but, nonetheless, this state of affairs was plainly unsatisfactory.7

In 2006, Parliament finally decided to act and redress these and other anomalies. The Copyright Amendment Bill 2006 in its initial incarnation would simply have removed the anomaly. In the course of its passage through Parliament, however, an important change was made: the words which required the copy to be made “in domestic premises” were deleted. The Minister explained this change to Parliament:8

This relates to time shifting. … This amendment substitutes a new section 111(1), which removes the requirement that a recording of a broadcast under section 111 must be made in domestic premises. This amendment provides greater flexibility in the conditions that apply to time-shift recording. The development of digital technologies is likely to result in increasing use of personal consumer devices and other means which enable individuals to record television and radio broadcasts on or off domestic premises. The revised wording of section 111 by this amendment enables an individual to record broadcasts as well as view and listen to the recording outside their homes as well as inside for private and domestic use.

Accordingly, s 111 of the Copyright Act now provides that it is not an infringement of any copyright:

if a person makes a cinematograph film or sound recording of a broadcast solely for private and domestic use by watching or listening to the material broadcast at a time more convenient than the time when the broadcast is made.

Section 111(3), however, removes that protection if the film or recording is dealt with in various ways, such as offering for sale or selling copies.

HOW OPTUS TV NOW WORKED

Readers of this journal will no doubt find much of interest in the technical details of how Optus’ system worked. For present purposes, however, it suffices to note the following. The service was available only to individual subscribers or employees of small to medium business customers of Optus. Qualifying subscribers received 45 minutes of storage as part of their existing mobile plan; this could be extended to 5 hours on payment of an additional $7.00 per month or 20 hours for $10.00 per month. Through the terms and conditions, each subscriber agreed to use any recordings only for private and domestic purposes.

Having agreed to the terms and conditions, the subscriber could access an electronic program guide provided by Optus and could nominate to record one or more programs as indicated above. The program guide showed only programs to be broadcast in the subscriber’s home town so, for example, a subscriber from Melbourne who happened to be in Sydney could not record programs showing on the Sydney networks.

The programs were not recorded, however, on the subscriber’s device. Instead, when Optus’ systems detected that a subscriber had selected a program for recording, the broadcast was picked up by antennas Optus had set up, recorded and then stored on Optus’ servers.

Optus recorded each program in four formats: a format for PCs, a format for Mac computers, a format for IOS devices and a format for Android devices. The subscriber did not have to nominate which format the program was recorded in and it did not matter whether he or she had only a PC or a Mac. The program was recorded in all four formats. However, a separate (set of) recording(s) was apparently made for each subscriber.

Once the recordings were made, they were stored on Optus’s server for 30 days and then deleted automatically. Within that 30 day period, the subscriber could watch the program as few or as many times as he or she liked. When the subscriber logged into Optus’ system to watch the program, it automatically detected what device they were using and played back the
recording in the applicable format. If the subscriber was using a iOS device, playback could start 2 minutes after recording began.

**WHAT THE TRIAL JUDGE FOUND**

On the initial question: who made the recording, Rares J found it was made by the subscriber:

63 … the user of the TV Now service makes each of the films in the four formats when he or she clicks on the “record” button on the TV Now electronic program guide. This is because the user is solely responsible for the creation of those films. He or she decides whether or not to make the films and only he or she has the means of being able to view them. If the user does not click “record”, no films will be brought into existence that he or she can play back later. The service that TV Now offers the user is substantively no different from a VCR or DVR. Of course, TV Now may offer the user a greater range of playback environments than the means provided by a VCR or DVR, although this can depend on the technologies available to the user.

and:

66 … the only person who could cause the Optus datacentre to bring into existence or create the films in the four formats was the user who clicked the instruction “record” on his or her compatible device. I agree with the reasoning of the Second Circuit Court of Appeals in Cartoon Network 536 F 3d at 131 that there is no real or sufficient distinction between the characterisation of a user of a service, like TV Now, to record a film of a broadcast and a person who uses a VCR (or DVR) to do so ….

His Honour then went on to find that the making of the recording was protected by s 111. On the basis of s 22(6) of the Copyright Act, his Honour also found that the subscriber, not Optus, communicated the transmission of the recording when the subscriber played it back. Accordingly, it was not communicated to the public in infringement of the exclusive communication right.

**WHY THE FULL COURT ALLOWED THE APPEAL**

The Full Court rejected the trial judge’s foundation conclusion: that the copies of the broadcasts were made by the subscriber. Instead, the Full Court ruled that the copies were made by Optus or, in the Full Court’s preferred view, by both Optus and the subscriber. In either case, Optus was not protected by s 111 and so infringed. It may be readily doubted that Parliament had such a service in mind when s 111 was amended to take its present form, but the Full Court did not base its conclusion explicitly on such a doubt.

**WHO MADE THE COPY (RECORDING)**

According to the Full Court, the trial judge’s conclusion that the copies (recordings) from the broadcasts were made by the subscriber was wrong primarily because it did not pay sufficient regard to the pervasive nature of Optus’ involvement. The fact that its involvement was entirely automated, ‘non-volitional’ in American parlance, did not save it. Accordingly, the Full Court said:

67 Accepting as we do the appropriateness of the OED definition for the purposes of s 86, s 87 and s 101, we consider that Optus’ role in the making of a copy – ie in capturing the broadcast and then in embodying its images and sounds in the hard disk – is so pervasive that, even though entirely automated, it cannot be disregarded when the “person” who does the act of copying is to be identified. The system performs the very functions for which it was created by Optus. Even if one were to require volitional conduct proximate to the copying, Optus’ creating and keeping in
constant readiness the TV Now system would satisfy that requirement. It should also be emphasised that the recording is made by reason of Optus’ system remaining “up” and available to implement the subscriber’s request at the time when its recording controllers poll the user database and receive a response indicating that a recording has been requested. What Optus actually does has –

a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner … trespassed on the exclusive domain of the copyright owners: CoStar Group Inc v LoopNet Inc [2004] USCA4 133; 373 F3d 544 at 550 (4th Circ. 2004).

The Full Court had earlier identified a range of factors contributing to the pervasive involvement of Optus:

50 The first matter to be noted is Optus’ TV Now Service itself. Optus designed it; gave it its functionality; owned the intellectual property in it …; and marketed the service it provided to its customers. The system itself was configured so as to be able to receive, copy, store and permit the viewing of on compatible mobile and PC devices, the free-to-air broadcasts of the 15 TV channels in each of the five mainland State capitals. And it was fully automated. Its function in short was to receive, copy, store and stream to a subscriber’s device, programmes required by a subscriber to the TV Now service.

51 … The subscriber does not “store” television shows. Optus stores copies. …

52 … one additional matter requires notice. Optus at all times retained possession, ownership and control of the physical copies made on the hard disc of its NAS computer until they were deleted by Optus after the expiry of 30 days from recording or by the subscriber before then. Viewing of the programmes copied was achieved by way of streaming the appropriate compatible version of playback data to the user’s device. No data, no copies of the programme, were thereby stored in that device in any permanent form in that process.

Notwithstanding the “pervasive” involvement of Optus, the Full Court was clearly troubled that no copy of any broadcast was made unless a subscriber chose to record it. Optus did not choose any program to be recorded and had no say in whether or not any broadcast was recorded. Their Honours could not overlook the fact that nothing was recorded without a decision made by the subscriber:

76 If one focussed not only upon the automated service which is held out as able to produce, and which actually produces, the copies but also on the causative agency that is responsible for the copies being made at all, the need for a more complex characterisation is suggested. The subscriber, by selecting the programme to be copied and by confirming that it is to be copied, can properly be said to be the person who instigates the copying. Yet it is Optus which effects it. Without the concerted actions of both there would be no copy made of a football match for the subscriber. Without the subscriber’s involvement, nothing would be created; without Optus’ involvement nothing would be copied. They have needed to act in concert to produce – they each have contributed to – a commonly desired outcome. The subscriber’s contributing acts were envisaged by the contractual terms and conditions. How they were to be done were indicated by the prompts given on the Optus TV Now TV guide page. The common design – the production of the selected programme for transmission to the subscriber – informed the solicitation and the taking of a subscription by the subscriber; it was immanent in the service to be provided. (emphasis supplied)

The Full Court considered it was not necessarily appropriate to identify only one person as the “maker”; the copy could be made jointly. As a result, the Full Court “preferred” the view that, while Optus at least was a maker of the copy, both Optus and the subscriber made the recording.
WHY S 111 DID NOT APPLY

Having concluded that Optus or (preferably) Optus and the subscriber made the copy, the Full Court then found that Optus’ involvement in making the recorded copy was not protected by s 111: put simply, the recorded copy was not made for Optus’ private and domestic purposes:10

89 There is nothing in the language, or the provenance, of s 111 to suggest that it was intended to cover commercial copying on behalf of individuals. Moreover, the natural meaning of the section is that the person who makes the copy is the person whose purpose is to use it as prescribed by s 111(1). Optus may well be said to have copied programmes so that others can use the recorded programme for the purpose envisaged by s 111. Optus, though, makes no use itself of the copies as it frankly concedes. It merely stores them for 30 days. And its purpose in providing its service — and, hence in making copies of programmes for subscribers — is to derive such market advantage in the digital TV industry as its commercial exploitation can provide. Optus cannot invoke the s 111 exception. (original emphasis)

Optus was not able to avail itself of the s 111 defence even though the subscriber who “instigated” the making of the copy would be entitled to the benefit of the defence.11

Section 111(1) does not explicitly state that the person who made the copy must be the same person who uses the recording to watch or listen to it at a more convenient time but, in many respects, the Full Court’s interpretation can be seen as a logical consequence of their Honours’ conclusion that Optus was the, or a, maker of the copy. As I shall discuss in the next section, however, it is neither a necessary conclusion and, with respect, leads to a very significant constraint.

Having reached these conclusions, it was unnecessary for the Full Court to decide the other issues dealt with by the trial judge, including his Honour’s conclusion that the subscriber, not Optus, made the communication when the recording was “played back” and it was not a communication to the public.12 While one could credibly argue that his Honour’s conclusions on these two issues were consistent with the legislative regime, questions will inevitably hang over his Honour’s conclusions on these questions too as the Full Court’s approach to who made the copy is so divergent from his Honour’s approach on that question.

SOME QUESTIONS

Following the Full Court’s ruling, Optus suspended the Optus TV Now service.13 According to press reports, however, Optus has applied for special leave to appeal the Full Court’s decision to the High Court of Australia.14 Even if that application fails, however, the Full Court’s ruling poses a number of considerable challenges.

Perhaps the most startling point is the Full Court’s conclusion that Optus was liable for infringements even though the subscriber for whom the copies were made was not. This is not to say that copyright law never imposes liability on one person where it would not impose liability if the same conduct were engaged in by someone else. It is however troubling, to say the least, where liability would not fall on the “instigator” of the conduct.

THE FULL COURT’S DEFINITION OF “MAKE”

Turning to the meaning of “make”, the Full Court rejected as contrived Optus proposed definition of “to make” derived from the Macquarie Dictionary as “to produce by any action or causative agency”, “to cause to be or become” and “to cause, induce or compel (to do something)”.15 Instead, the Full Court considered that the “essence” of “to make” in the context of ss 86(a), 87(a) and (b) is:16

the idea of making (ie creating or producing) a physical thing (ie the embodiment of the copyright subject matter). We agree with the AFL’s submission to this effect.
The OED definition with its emphasis on producing a “material thing” is an apt one ….

Despite rejecting Optus’ proposed definition as contrived, the Full Court nonetheless immediately acknowledged that there must also be a “causative agency” in “making”: “The issue is not simply how something is made. It is by whom is it made.”

In adopting its definition of “make”, the Full Court relied on the concept of “making a cinematograph film” or a copy of a film. But, with respect, it is not clear that really helps. Section 22(4) of the Copyright Act instructs us that “making a cinematograph film” is a reference to “the doing of the things necessary for the production of the first copy of the film”. It also defines the “maker of a cinematograph film” as “the person by whom the arrangements necessary for the making of the film were undertaken”.

It could be argued that the primary role of s 22(4) lies in identifying the owner of copyright in a cinematograph film as copyright subject matter. Other parts of s 22, however, are not so limited. Insofar as s 22(4) could provide assistance, the maker of the film is typically thought of as the producer.

In many respects, it is not inapt to describe Optus as the person who has made many of the arrangements necessary for the making of the recording. However, it is at least arguable that Optus’ role is not that of a producer. The producer may not be the person who actually records the sounds and images and edits them into the “first copy”. Those acts will typically be done by directors, directors of photography, editors and the like. Nonetheless, it seems arguable that the producer has a more direct role in the film project than Optus had in the making of the recording: the producer at least determines what project will be made and does not just hire the camera equipment, sound stage, other infrastructure and personnel involved to make the film.17

Similarly, the Full Court’s approach sits at odds with the definition of the maker of a communication provided by section 22(6): the person responsible for determining the content of the communication, not the person whose network is used to transmit the communication.18

According to the Full Court, the automated or “non-volitional” nature of Optus’ involvement was no reason to find it was not the maker. However, our law has long distinguished between the role of a mere amanuensis and an author in the making of a work.19 That distinction is drawn in the context of the maker of original work which requires an authorial contribution. The authorial contribution, however, goes to the requirement of originality rather than the making.

These considerations suggest that the identity of the causative agent should be determinative.

**SHOULD THE SUBSCRIBER HAVE BEEN AN AUTHORISER?**

The Full Court’s use of “instigates” and “concerted action” might be thought to be the language of authorisation. If rather than pressing the Record “button” the subscriber had gone into an Optus store and handed over a USB stick with a request that the sales assistant make a copy and the sales assistant (or some other Optus employee) then arranged for a copy to be made, there could be little doubt that the recording was made by Optus20 and the subscriber authorised the making of the recording.

At least three points emerge from this. First, the Full Court’s characterisation of the subscriber’s role as a “maker” rather than an “authoriser” highlights the significance of the subscriber’s role. In many cases of authorisation, it is often possible to say that there would have been no infringement but for the authoriser procuring, inducing or purporting to grant authority to do the infringing act. Typically, however, there still remains a need for the infringer to go on and deliberately perform the infringing act.22 Thus, the authoriser’s role in the infringement is somewhat indirect: it is at a step removed from the actual infringement. The Full Court’s preferred characterisation implicitly suggests, therefore, that the subscriber’s role was rather more direct than that of an authoriser.
Secondly, the question emerges whether the automated nature of the process makes a difference. Thirdly, characterising the subscriber’s role through the more traditional concept of authorisation has at least the virtue of analytical clarity. Nonetheless, it still leads to some difficult issues.

**The designedly automated nature of Optus TV Now**

As already noted, the Full Court concluded that the entirely automated nature of the processes on Optus’ side did not exonerate it from the charge of making the recording. This is in stark contrast to the conclusions reached by the Second Circuit Court of Appeal in the United States in the *Cartoon Network* case and VK Rajah JA in *Record TV Pte Ltd v MediaCorp TV Singapore Pte Ltd*. On the other hand, the Full Court drew comfort from a conclusion in a Japanese decision.

There were a number of strands in the Full Court’s rejection of *Cartoon Network*. First, and unexceptionably, the legal regimes and common law rules are not on all fours. Moreover, the Full Court characterised this aspect of *Cartoon Network* as directed to distinguishing between two different forms of liability: liability as a primary infringer for making a copy and liability as a secondary infringer for contributory liability. But, with respect, the liability that the copyright owner sought to impose on Cablevision, and which was rejected, in *Cartoon Network* was direct liability for making the allegedly infringing copy.

Relying on some decisions at District Court level (i.e., subordinate to or less authoritative than the Second Circuit) and criticism by Prof. Ginsburg, the Full Court appears also to have considered that *Cartoon Network* was of questionable authority even in the United States of America. It is with respect true that the Second Circuit’s opinion is not binding on the other Circuit Courts, nor is it the final arbiter; that role falls to the Supreme Court of the United States of America. As the Full Court notes, District Judge Feess sitting in the Central District of California in the Ninth Circuit declined to follow *Cartoon Network* in the absence of a specific direction from the Ninth Circuit Court of Appeals.

Thirdly, the Full Court considered that analogies were not particularly helpful in this field. Rather, it focused on “the system itself is configured designedly so as to respond to a third party command to make [the] copy”. It has been observed that the courts are astute to thwart attempts to evade liability though the clever design of technological systems.

An example is the *MP3s4free.net* case. Cooper operated a website which linked to infringing copies of recorded music. Browsers who clicked on a link were taken to a site from which an infringing copy of the recording was downloaded to the browser’s device; either automatically or upon further choices being made. Cooper set it up so that anyone could log into his website and place a link to an infringing copy on it; he did not need to insert or place the link himself. Nor did he ever need to give them permission before their links appeared on his website. But that is a very different situation to Optus TV Now. In Optus TV Now, the Full Court considered that the “users”, the subscribers, were perfectly entitled to the defence provided by s 111: they were not infringers and the copies (insofar as made by them) were not infringing copies.

**Authorisation and agency**

A situation where the copier was liable when the customer may not have been are the news clipping cases. Neville Jeffress (Media Monitors) provided a service to customers where, in return for payment, it monitored (amongst other things) press reports about the customer or nominated fields of interest and provided photocopies of the reports to the customer. The customer could then circulate them amongst its employees and the like.

Hill J rejected Media Monitors attempt to rely on the fair dealing defences for research or study, criticism or review or reporting of news on several grounds. One of the grounds for that rejection was that Media Monitors did not have a relevant fair dealing purpose. Whatever the purpose of its customers, its purpose was “purely commercial” “to supply a photocopy of material already published for a fee”. The nature and scale of its copying was also not a fair dealing.
In the Panel case, however, the Full Court recognised that Network Ten could rely on the fair dealing defences for materials made on its behalf by Working Dog (the production company), assuming the other requirements were made out. That is, the differently constituted Full Court in the Panel case recognised that the fair dealing defence could be exercised through an agent.

There does not seem to be any reason in principle why a subscriber to Optus TV Now could not exercise its acknowledged rights through an agent - Optus. Surely, it could not be suggested, for example, that if I were to program the DVR at home to record the next episode of The Voice for my daughter then s 111 would not operate and I would be infringing? It is also noteworthy that the circumstances are very different to the news clipping cases. In Media Monitors, Media Monitors was copying articles rather indiscriminately and the customers were circulating them wholesale amongst their employees. An Optus TV Now subscriber, however, nominated a specific program; without that specific “instigation”, nothing was recorded and only the subscriber and his or her close personal circle could watch the recording (otherwise the benefit of s 111 would be lost).

**HOW DOES OPTUS TV NOW APPLY IN OTHER SITUATIONS?**

At the end of their decision, the Full Court emphasised that their conclusion was based on the particular “service provider-subscriber relationship” and “to the nature and operation of the particular technology” in question. Their Honours concluded “different relationships and differing technologies may well yield different conclusions to the ‘who makes the copy’ question.”

That is, of course, inherent in our system of law-making. It is equally true, however, that their Honours’ reasoning will be scrutinised to see whether those different relationships and differing technologies fall on one side of the line or the other.

**The formalism**

If a customer were to go into an Internet cafe and use the computer and software set up by the cafe operator to download, say, an unauthorised and infringing video-clip to an USB stick the customer had brought with them, it is not hard to distinguish that situation from Optus’ TV Now as the copy ends up, if it is not (initially) made, on the customer’s USB stick. But how is the situation where the customer just views the infringing video on the computer in the Internet cafe relevantly different either from the situation where he or she copies the file on to the USB stick or from the Optus TV Now situation? Perhaps, in both situations, the answer on the Full Court’s reasoning would be that both the customer and the Internet cafe operator “made” the copy?

In the last couple of years, USB sticks have been increasingly displaced by online storage, or syncing systems like Dropbox, Sugarsync, Box.net, Crashplan, Carbonite and more recently iCloud and Google Drive. These enable the customer to have stored on remote servers copies of material on their personal computers. Most people, uninformed by the arcana of copyright law, probably would think that they “make” the copies of their documents and other files that are stored on the service provider’s server. It is difficult, however, to distinguish the design and provision of the service provider’s infrastructure from the design and provision of the Optus TV Now infrastructure. Perhaps, the narrow targetting of Optus’ service, to recording only transmissions which have (at a minimum) “broadcast” copyright in them is a distinguishing feature from such services which typically permit the user to store any kind of material.

In many of those types of cases, the copyright owner may not even know that there is any infringing activity going on and will have little economic incentive to pursue individual instances. What about services such as Flikr, YouTube and the like? Often, the “posting” of material on these types of sites is public, in that anyone can view them and, often, the material posted attracts large audiences. In such cases, the user consciously uploads the (assumed) infringing material to the provider’s server rather than just “clicks” Record, although the acts of selection and button clicking are often no different in terms of difficulty and commitment.
One might think that service providers in this category could rely on the protections provided by the DMCA-type safe harbours. The existence of such safe harbours may be predicated on the assumption that these types of services do in fact “make” the copies. In Australia at least, however, they provide protection only to “carriage service providers”. It may be doubted that these types of storage providers qualify as “carriage service providers” since they do not provide the network connectivity. If the Full Court’s reasoning applies to these services, therefore, the review into who should be able to rely on these defences assumes even greater significance.

ENDNOTES

1 The precise steps and button may vary of course depending on the brand of the machine and the program guide source. For example, you may need to click to confirm or you may want to add a few minutes on to the duration of the recording on the off chance that there is a bit of schedule creep.

2 Singtel Optus Pty Ltd v National Rugby League Investments Pty Ltd (No 2) [2012] FCA 34; 94 IPR 1. The analogy would have been even stronger if Optus had structured its arrangements formally as the rental of a TV antenna and a DVR, rather than provision of a service: Judge Nathan sitting in the Southern District of New York refused a preliminary injunction against such a service: American Broadcasting Companies Inc. v Aereo Inc. (SDNY 12-cv-01543, 11 July 2012).

3 National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd [2012] FCAFC 59 (27 April 2012) (Finn, Emmett and Bennett JJ).


6 Sony Corp of America v Universal City Studios Inc. (1984) 464 US 417; 2 IPR 225. In formal terms, the majority held only that Sony was not liable for contributory infringement as its Betamax machines had substantial, non-infringing uses.

7 Lord Templeman described a situation where millions of citizens were breaking the law through ignorance or contempt as ‘lamentable’: CBS Songs Ltd v Amstrad Consumer Electronics Ltd [1988] AC 1013 at 1060; 11 IPR 1 at 17.

8 Extracted in Singtel Optus (No 2) at [57] (emphasis supplied by Rares J).

9 See also at [59] and [75] and, for rejection of Optus’ argument based on the wholly automated nature of its system, [64].

10 [2012] FCAFC 59 at [89] and [93].

11 [2012] FCAFC 59 at [92]. The conclusion in favour of the subscriber’s reliance on the defence is only obiter dictum and, as the Full Court acknowledged, assumes that the subscriber in question had the relevant private and domestic character - a point the copyright owners disputed at trial.


15 [2012] FCAFC 59 at [58] and [48]

16 [2012] FCAFC 59 at [58].

17 The degree of artistic involvement may be greater or lesser according to how much artistic autonomy is accorded the director and other players.

18 Of course, s 22(6) had to be introduced to overcome the decision in Telstra Corporation Ltd v Australasian Performing Right Association Ltd (1997 191 CLR 140 (the Music on Hold case) and s 22(5) still provides that the maker of a broadcast is the person who provided the service.

19 Donoghue v Allied Newspapers Ltd [1938] Ch 106.

20 (Ignoring for present purposes that the sales assistant may well work in a franchised or licensed outlet rather than being directly employed by Optus.) Of course, in even this imaginary, alternative “steampunk” version of reality, a more likely form of procuring the copy would be for the request to be sent by fax/email/text or IM.

21 For simplicity, I shall just refer to the statutory concept adopted in Copyright Act 1968 (Cth) ss 13(2), 36(1) and 101(1) which will typically cover common law cases of joint tortfeasorship or common design: Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16 (20 April 2012) at [57] per French CJ, Crennan and Kiefel JJ and [100] per Gummow and Hayne JJ.

22 To use a term which, if not “neutral”, was not in issue between the parties.

23 Putting to one side cases of quia timet relief: Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16 (20 April 2012) at [94] per Gummow and Hayne JJ and [8] per French CJ, Crennan and Kiefel JJ.

24 In Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16 (20 April 2012), Gummow and Hayne JJ appear to recognise that purporting to grant a right to do something which infringes constitutes authorisation. French CJ, Crennan and Kiefel JJ are less clear: at [69], their Honours appear to require the authoriser to have power to control whether or not the infringement is done. Power to prevent the infringement, however, is only one of the three non-exhaustive factors listed in Copyright Act 1968 ss 36(1A) and 101(1A): see Roadshow Films [2012] HCA 16 at [68] and [135]; Lindgren, Lahore and Rothnie, Copyright and Designs, LexisNexis Australia (looseleaf), at [34,484].

25 Cartoon Network LP, LLLP v CSC Holdings Inc. 536 F 3d 121 (2nd Cir 2008).


27 [2012] FCAFC 59 at [60].

28 [2012] FCAFC 59 at [61] - [63].

29 [2012] FCAFC 59 at [64], see also [68].

30 Giblin


32 For example, De Garis v Neville Jeffress Pidler Pty Ltd (1990) 37 FCR 99; 18 IPR 292.

33 18 IPR at 298.

34 18 IPR at 302.

35 TCN Channel Nine Pty Ltd v Network Ten Pty Ltd (2002) 118 FCR 417 at [100] - [101] (Hely J)

36 [2012] FCAFC 59 at [100].

37 Copyright Act ss 111A(2) and 111B(3) would appear to preclude reliance on the “temporary copy” defences.
Copyright Act 1968 ss 116AA – 116AJ.

The High Court has rejected the inference of authorisation, however, from the enactment of s 112E: Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16 at [26] and [113].

Telecommunications Act 1997 (Cth) s 87.

The Stop Online Piracy Act, or SOPA, was a highly controversial proposal put to US Congress to enable the enforcement of copyright and trade mark law against foreign ‘rogue’ websites. SOPA would have enlisted a range of new intermediaries in the online enforcement ‘war’, in particular, domain name servers, credit card providers and online advertising service providers. This article outlines the proposals that were included in SOPA and critically analyses the simplistic ‘least cost avoider’ reasoning that justifies enlistment of these intermediaries on the basis that there is an online enforcement problem that they could assist in reducing. Although SOPA itself is politically dead, ideas embodied in it are likely to recur in some form in the future. It is therefore worth critically examining what was proposed.

INTRODUCTION

On 18 January 2012, thousands of websites, including Wikipedia, went dark. At the same time literally millions of letters, phone calls, and emails were directed at Members of the US Congress. The cause was the latest front in the online copyright enforcement wars, the Stop Online Piracy Act – SOPA – a piece of proposed legislation introduced into Congress to address ‘foreign rogue websites’.

There had been opposition to SOPA, and White House officials had expressed concern about aspects of the bill on 14 January. It had, nevertheless, seemed that SOPA was on a fast-track, and would sail through committee and rapidly become US law. It had bipartisan support, and similar bills had received favourable committee reports (US Senate Judiciary Committee 2010, 2011). After January 18, support evaporated. Within days, both SOPA and a similar Senate bill had been withdrawn. SOPA was politically dead.

SOPA, its introduction, consideration and ultimate demise, make for fascinating politics. January 2012 was a remarkable – and unprecedented – moment in Internet activism and in particular over intellectual property (IP) law. The implications of these unprecedented events are still playing out (Benkler 2011, 2012; Weatherall 2012). But SOPA is also interesting as representing a new stage in the battle to involve Internet intermediaries in policing IP infringement. In Australia the limits of secondary liability in copyright have been the subject of debate in the context of the Roadshow v iiNet litigation.

SOPA would have enlisted a broader set of players in copyright enforcement – namely non-authoritative domain name servers and financial intermediaries – with scant regard for common law doctrines of secondary liability. The reasoning behind SOPA is simple: there is a problem (online IP infringement based overseas) and these parties are in a position to do something about it. As this article shows, however, this calculus, although superficially attractive, is too simple. It leaves out of consideration a range of costs and issues that ought to form part of any decision to legislate.

This article describes the proposals in SOPA, situates them in the context of existing and developing laws on intermediary liability in copyright, and evaluates the ‘least cost avoider’
argument that is sometimes used by proponents. Although _SOPA_ itself may be dead, this analysis is important because some of the ideas represented in its provisions are likely to return in future IP enforcement proposals.

**WHAT _SOPA_ PROPOSED**

_SOPA_ was intended to address sites online that the US government and IP owner representatives have labelled ‘foreign rogue websites’: those which enable or engage in copyright infringement and/or trade mark counterfeiting with impunity because they are based beyond the jurisdiction of US courts (Judiciary Committee 2010: 3-4; 2011: 3-4). The Pirate Bay, for example, as a popular BitTorrent site, based in Sweden, that is used to find movies available for download, would be an archetypal rogue site. Taking action against foreign infringing sites has been on the US policy agenda since at least 2010 (Executive Office of the President of the United States 2010). Although US authorities have ways to impede the operation of such sites, such as seizing US-registered domain names and seeking the extradition and criminal prosecution of persons involved, rightholders urged that better mechanisms were needed to protect the US’ entertainment industries.

_SOPA_ was actually the third similar legislative proposal introduced into Congress during 2010-11. The first, introduced into the US Senate in September 2010, was the _Combating Online Infringements and Counterfeits Act_, or _COICA_ (S.3804, 111th Congress (2010)), superseded in May 2011 by the _Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act_, or _PIPA_ (S.968, 112th Congress (2011)). _SOPA_ was introduced into the House of Representatives in October 2011. All three bills proposed similar mechanisms to address rogue sites. This paper focuses on _SOPA_ as the most recent, and most extensive, proposal.

_SOPA_ targeted rogue sites via three key mechanisms. A first process, in §102, would empower the US Attorney-General to seek from a US Court an injunction against a site (in _rem_, i.e., against the website rather than the individual if the individual cannot be found or brought before the court) and then serve that injunction on a series of US-based Internet intermediaries requiring them to cease dealing with the site. US non-authoritative domain name servers would have to prevent the domain name from resolving, making the site harder to find; to similar effect, search engines would have to eliminate links to the site; payment providers (such as credit card companies) would be required to refuse to process US-related transactions; and companies providing Internet advertising would be required to cease serving advertisements to the site, depriving it of revenue. This would be initiated against a ‘foreign infringing site’, defined in §102(a) as one that was ‘US-directed’ and used by US Internet users, where the site owner/operator was ‘committing or facilitating the commission’ of criminal copyright violations or trade mark counterfeiting, so that the site would have been subject to seizure if based in the US. Proponents claimed that the legislation targeted only the ‘worst of the worst’, although the criminal threshold is not a high one: under US law, criminal liability arises wherever a single copy is made for commercial advantage or private financial gain (17 USC §506). In sum then, as Benkler put it, _SOPA_ would have enabled a ‘multi-system denial of service attack’ on an alleged rogue site (Benkler 2011: 54).

A second process (entitled the ‘market-based system’ and set out in §103) would allow private parties harmed by a rogue site’s activities (including, but not confined to, an affected IP owner) to contact payment providers and Internet advertising service providers, requiring them to cease doing business with the accused site within five days. The idea was to cripple or eliminate rogue sites by taking away these financial and advertising services that tend to give them the ‘appearance of legitimacy’ (Judiciary Committee 2011: 4). More importantly, the goal was to deprive such sites of services that enabled their monetisation (Judiciary Committee 2011: 7). The system would operate as a form of ‘notice and terminate’. Court involvement would be required only if the intermediary failed to comply, or if the accused site provided a counter-notification, in which case the harmed party would have been able to seek an injunction against the accused site (§103(c)) and serve it on payment providers and Internet advertising service providers requiring them to take ‘technically feasible and reasonable
measures’ within five days to cut off transactions relating to the site (§103(d)). Failure to comply at this point could lead to proceedings requiring the intermediary to ‘show cause’ why they should not be subject to an injunction and appropriate ‘monetary sanction’ (§103(d)(4)). This second process, as one enabling private actions, was to have been available against only a subset of more seriously infringing websites ‘dedicated to the theft of US property’. This term, defined in §103(a)(1), referred to US-directed sites, used by American users, which were ‘primarily designed or operated for’ offering goods or services in a manner that ‘engages in, facilitates, or enables’ copyright infringement, breach of anti-circumvention laws, sale or promotion of counterfeit trade mark goods, or where the operator of the site ‘turned a blind eye’, deliberately avoiding confirming a high probability of the site being used to carry out such acts.

Third, SOPA would have provided an immunity from action under US law (§104) for any of these Internet intermediaries – domain name servers and registrars, search engines, payment service providers, and advertising service providers – for action taken under the legislation, or otherwise voluntarily blocking access or ending financial affiliation with a site taken in the ‘reasonable belief’ that it was one targeted by the legislation. This would remove some qualms an intermediary might otherwise have about taking action against a customer who might, if services were terminated, sue for breach of contract.

SOPA also foreshadowed even broader measures to deprive rogue sites of funds, requiring the Intellectual Property Enforcement Coordinator to produce a report identifying and discussing ‘notorious foreign infringers’, and whether such infringers should be denied access to US capital markets (§107).

SOPA contained some limited protections for the accused. Actions by the Attorney-General were to be commenced in the first instance against the owner/operator of a site in personam, thus requiring attempts to notify the site owner of impending action: only if ‘due diligence’ failed to reveal this person would an in rem action against the site be allowed (§102(b)(1) and (2)). The owner or operator (among others) of a site could at any time issue a motion to modify, suspend, or vacate any order made under the legislation (§102(d)) on a range of grounds. Under the market-based notice-and-terminate system, an accused site could issue a counter-notification, in which case court proceedings would be necessary before action by an intermediary would be required (§103(a)(5)) – although:

(a) a counter-notification would only be valid if the owner/operator was prepared to consent to the jurisdiction of US courts and

(b) even in the absence of court action, intermediaries would be immune from suit if they chose to take action (§104), reducing an intermediary’s incentives to resist.

There were also penalties for ‘knowing misrepresentation’ that a site was dedicated to the theft of US property (§103(b)(6)).

Following criticism, SOPA’s key author and sponsor, Republican Lamar Smith, tabled amendments in December 2011. The amendments were intended more firmly to exclude domestic sites, to soften the obligation to prevent resolution of domain names; to give intermediaries more leeway in determining appropriate technical measures; confine the scope of orders to those portions of a site found to be ‘infringing’ or ‘dedicated to the theft of US property’ (revised §104); and tighten the immunity from suit to require that any ‘reasonable belief’ that a site was one of those targeted must be based on ‘credible evidence’ (revised §105).

In addition, the amended Act proposed a study of the Act’s impact (revised §106) with a view to determining not only whether the measures were effective to reduce infringement (as envisaged in the original bill) but also to identify any unintended consequences. It also contained a series of opening recitals (§2) to address more general concerns, asserting that the Act should not be construed to require the use of particular technology, monitor networks, or impact on the security or integrity of the domain name system or any other system operated by an Internet intermediary. Critics remained unconvinced.
THE CONTROVERSIES

SOPA provoked outrage on numerous grounds. The unilateral extraterritorial application of US law, which could cut off financial resources for sites legitimate in the countries in which they were based; the failure of the laws to confine their remedies to the ‘worst of the worst’; and the potential for drastic remedies to be applied *ex parte* were all the subject of sustained criticism. SOPA’s broader significance in the debate over Internet governance is explored elsewhere (Benkler 2011, 2012; Gross, M. 2012; Weatherall 2012). The focus here is on SOPA’s proposed expansion of the intermediaries involved in IP enforcement online to two new groups: domain name servers, and financial intermediaries.

In extending liability to these groups, SOPA represented a departure from existing laws, embodied in the US in the *Digital Millennium Copyright Act 1998* and in Australia in Part V Div 2AA of the *Copyright Act 1968* (Cth), which provide a ‘safe harbour’, that is, relief from liability for any monetary remedies, to certain online intermediaries in return for them taking steps aimed at reducing copyright infringement online and removing infringing material. These laws cover ISPs providing Internet access to subscribers, online hosts and search engines, as well as those who engage in caching. For these entities, at least at the time the relevant laws were drafted, liability was a real possibility and in some cases may continue so. Existing law then is premised on intermediaries’ preferring to protect themselves from potential liability for their users’ copyright infringement and therefore complying with the relevant conditions.

SOPA would not have relieved intermediaries of potential liability for copyright damages. It proposed to create standalone obligations, where the main penalties for non-compliance were to be subject to an injunction and, in some cases, an appropriate ‘monetary sanction’. The documentation that has accompanied SOPA, COICA or PIPA does not suggest that the intermediaries targeted are to blame or are being held ‘responsible’ in some way for the IP infringements. A much more simple calculus seems to be at work: there is a problem (widespread foreign IP infringement), and these intermediaries, while not (necessarily) liable under traditional IP doctrines of secondary liability, are in a position to do something about it.

In taking this approach, the proponents of SOPA seem to apply a simplified version of the ‘least cost avoider’ theory often cited as a justification for imposing liability on third parties in copyright (Brennan 2010; Lindsay 2010) and beyond (Lichtman and Posner 2006; Calabresi 1961). According to this theory, liability for another’s wrongdoing may be imposed on (innocent) third parties where direct liability applied to wrongdoers will be predictably ineffective, and the third party actors are capable of controlling the bad actors or mitigating the damage they cause. In other words, the obligation to enforce laws can be imposed on a third party who is in a position to do so most efficiently.

One problem with an overly simplistic application of least cost avoider theory sometimes seen in policy documents, although generally not in serious economic analysis such as that in Lichtman and Posner (2006) and Lindsay (2010) is that it represents a very partial analysis of the impact of liability. If we focus solely on whether the third party is a low cost enforcer, we can tend to ignore other important considerations: such as

1. whether it is necessary to impose liability through law, or whether the private parties are in a position to reach an optimal allocation of responsibility;
2. what are the *benefits* gained by turning the relevant intermediaries into enforcers, and do they justify the costs involved;
3. what broader costs may be imposed on *other* parties and for society and
4. what longer term implications might arise from the imposition of liability.
Perhaps the most controversial provisions of SOPA were those requiring service providers\textsuperscript{14} to take measures to prevent the domain name of a foreign infringing site from resolving to the corresponding Internet Protocol Address (§102(c)(2)(A)), and instead to direct the user to text prescribed by the Attorney-General (§102(c)(2)(A)(iv)). According to critics, these provisions represented ‘an unprecedented, legally sanctioned assault on the Internet’s critical technical infrastructure’ (Lemley et al 2011: 1). Proponents argued that this was one way efficiently to enforce IP rules. But as the debate and eventual abandonment of these provisions showed, proponents failed to grapple with

(a) the broader costs of such an approach or

(b) its questionable benefits.

The DNS is, by design, universal: whenever, and wherever, a person types in a given domain name, that user’s browser should be able to query any domain name server to identify the IP address of the relevant server and receive the same response. Under SOPA, this would no longer be true: users in the US at least who typed in an affected address would be routed to an entirely different place: most likely, to a stern warning page.

Commentators questioned the effectiveness of such measures, suggesting that DNS redirection would be trivial to avoid (Crocker et al 2011; similarly see Ofcom 2011).\textsuperscript{15} Most criticism, however, focused on the broader costs of these measures. Some tools that users could adopt to avoid DNS filtering (for example, adopting a DNS service from a site overseas, or downloading a software ‘plug-in’ to achieve that goal) could place the user’s security (whether knowingly or not) at risk: an overseas DNS server might correctly resolve the IP address of the Pirate Bay, but not, perhaps, the Bank of America, putting consumers at some risk of fraud or identity theft (Crocker et al 2011).\textsuperscript{16} US legislators, while acknowledging this risk, argued that a substantial proportion of users did not intend to commit IP-related crime, and would therefore not circumvent the filtering (Judiciary Committee 2011: 10).

Critics further suggested that SOPA would interfere with moves to introduce security extensions to the DNS known as DNSSEC (Crocker et al 2011). DNSSEC is designed to prevent ‘man-in-the-middle’ attacks on DNS queries. It does so by ensuring that if a user requests the server for a particular entity (for example, their bank), the response comes from the legitimate server for that bank. SOPA would have required replacing authenticated responses with pointers to other resources (i.e. the government warning), and as such, were inconsistent with DNSSEC (2011: 6). The UK’s telecommunications regulator, Ofcom, has also noted this incompatibility (Ofcom 2011: 5).

At a more general level, commentators argued that adopting DNS blocking of sites disapproved by the US Government would offer the cover of legitimacy to similar moves already being undertaken by other governments to block websites they do not approve. This could both encourage Internet censorship, and contribute to the ‘balkanisation’ of the Internet and the further undermining of the universality of the DNS (Crocker et al 2011; Lemley et al 2011) (although it is perhaps worth noting that given US authorities have already been involved in the seizure of websites via other legal mechanisms, the additional impact of SOPA in this regard might be doubted).

Judging from the criticism and the response from policymakers, the DNS proposals are less likely than other aspects of SOPA to reappear in future proposals. Concerns about the integrity and universality of the Internet’s technical infrastructure struck a chord with US policymakers (as did the popular characterisation of the proposals as ‘censorship’). In the first public statement on SOPA released by the office of the US President, the White House’s highest-ranking officials in the area of the Internet and IP enforcement, Victoria Espinel (IP Enforcement Coordinator), Aneesh Chopra (Federal Chief Technology Officer), and Howard Schmidt (Cyber-Security Coordinator), stated (White House 2012) that although policing copyright infringement was important:
Proposed laws must not tamper with the technical architecture of the Internet through manipulation of the Domain Name System (DNS), a foundation of Internet security. Our analysis of the DNS filtering provisions in some proposed legislation suggests that they pose a real risk to cybersecurity and yet leave contraband goods and services accessible online. We must avoid legislation that drives users to dangerous, unreliable DNS servers and puts next-generation security policies, such as the deployment of DNSSEC, at risk.

The DNS-related provisions were significantly watered down (albeit not removed entirely) by the amendments to SOPA in December 2011, and in January 2012 SOPA author and sponsor Smith stated that he would remove the provisions entirely (US House Judiciary Committee 2012a). Senator Leahy, the sponsor of the corresponding House bill PIPA, suggested that similar provisions in that Act would also be reconsidered, perhaps by requiring a study of their impact before implementation (Gross G 2012).

SOPA’s proposal for DNS manipulation is not without precedent, nor is it entirely inconsistent with policy moves elsewhere. A number of countries already prohibit access to certain sites online using similar techniques: most notoriously China and Iran, but a number of other countries to greater or lesser degrees; the possibility has also been suggested in Australia, where Labor Party policy favours Internet censorship at an ISP level. Such moves to formalise DNS filtering on a significant scale, are however more controversial coming from the US which has in recent times adopted a strong stance in favour of Internet ‘freedom’ (Clinton 2010, 2011), and which has invested significant resources into developments such as DNSSEC.

On the other hand, there is a distinction between the streamlined blocking regime contemplated by SOPA and the more targeted blocking seen in some jurisdictions facilitated through the court system. In the United Kingdom, courts have specifically ordered ISPs to block access to a number of sites found in court proceedings to be infringing copyright; Indian courts have also issued several website-blocking orders to support copyright enforcement in 2012 (Celestine 2012). The breadth of sites targeted, the move to make sites’ banishment from the Internet as complete as possible, and the absence of any opportunity or requirement in the legislation to consider the proportionality of such a remedy as applied to a given site distinguish SOPA from these court-based processes.

CUTTING OFF THE MONEY

More likely to recur in future proposals for IP enforcement online are those parts of SOPA that enlist financial intermediaries and online advertising providers. These proposals generated less controversy, and have precedents in US laws relating to online gambling and online pharmacies, both of which involve financial intermediaries such as credit card providers in cutting off illegal transactions (MacCarthy 2010a). These proposals also drew support from even vehement opponents of SOPA, such as Google, itself an online advertising provider and provider of payment services. In evidence before the House Judiciary Committee in November 2011, Google stated its belief that ‘an approach that focuses on advertising and payment services ... is the most promising path toward an effective solution’ (Oyama 2011).

This is perhaps not surprising: even under conventional IP doctrine, credit card companies in particular are a much more borderline case for secondary liability than domain name servers, and some IP plaintiffs have sought to bring proceedings against them. The lead case on this issue at present is the 9th Circuit decision in Perfect 10, Inc. v Visa International Service Association. In this case, the plaintiff, an Internet publisher of photos of ‘natural models’, had identified websites, many based overseas, reproducing the plaintiff’s photographs without permission or payment. Rather than directly suing the websites, the plaintiff brought an action against credit card companies and affiliated banks and data processing services, alleging that, by continuing to process transactions for these sites after being notified of the plaintiff’s claims, they were liable for vicarious and contributory copyright infringement and for secondary liability under trade mark law.
By majority, the 9th Circuit upheld a summary judgment in the defendants’ favour given by the District Court, holding that the activities of the credit card companies lacked a ‘direct connection to the infringement’. No infringing material passed over the defendants’ networks; nor did the defendants assist in the location, reproduction or distribution of infringing materials.\textsuperscript{20} Although the processing of credit card transactions did assist in making infringement \textit{profitable}, increasing incentives to infringe, the connection to the actual infringement was insufficiently direct. The majority drew a contrast with the position of a search engine, which leads users directly to infringing images and hence plays a more ‘essential’ or ‘material’ role in infringement.\textsuperscript{21} Nor was the credit card company analogous to entities like swap meets or file-sharing sites like Napster, which provide the ‘site and facilities’ for infringement. Nor, under a vicarious liability analysis, did the credit card companies have the ‘right and ability to control’ the infringements: as the majority expressed it, ‘the mere ability to withdraw a financial “carrot” does not create the “stick” of “right and ability to control” that vicarious infringement requires.’\textsuperscript{22} The majority was also explicit that it was making a policy choice: refusing liability for credit card companies which were a ‘primary engine of electronic commerce’ was consistent with Congress’ policies in favour of facilitating electronic commerce.\textsuperscript{23}

But how is one to judge whether a given connection to infringement is sufficiently ‘direct’? Comparing the majority’s opinion to Judge Kozinski’s strident dissent, it seems that directness is in the eye of the beholder. Judge Kozinski disputed the majority’s assertion that credit cards played only a limited role:

\begin{quote}
 Defendants here are alleged to provide an essential service to infringers, a service that enables infringement on a massive scale. Defendants know about the infringements; they profit from them; they are intimately and causally involved in a vast number of infringing transactions that could not be consummated if they refused to process the payments; they have ready means to stop the infringements.\textsuperscript{24}
\end{quote}

His Honour pointed out that ‘sale’ of infringing material is itself an infringement, and that credit card providers were involved in every single sale from the infringing sites,\textsuperscript{25} and argued that search engines were no more important to infringement than credit card providers. Interestingly, however, even Kozinski J balks at imposing liability on an online advertising provider. Since users can download material whether or not advertisements are present on a site, it could not be clear that, for example, refusing to serve ads to infringing sites would cause infringers to cease their erring ways.

Similar issues – and some similar reasoning – are evident in the recent Australian case of \textit{Roadshow v iiNet},\textsuperscript{26} in which the Australian High Court was required to consider whether a general purpose Internet Service Provider (ISP) should be liable for copyright infringement committed by customers who were using BitTorrent to download movies, at least once the ISP was notified that the IP address used by those customers had been detected in infringement. Like the credit card company, an ISP could be said to be a party benefiting commercially from infringing activity (Brennan and Weatherall 2009). But like the court in \textit{Perfect 10 v Visa International}, the judges of the High Court decision found against liability, emphasising the limited and indirect nature of iiNet’s connection to and ability to prevent infringement. According to the High Court, iiNet could only indirectly prevent infringement by terminating its contractual relationship with the infringing customers.\textsuperscript{27} It seems likely, based on the reasoning in iiNet, that an Australian court would reach a conclusion similar to the court in \textit{Perfect 10}: that any power a credit card company might have over IP infringements is indirect at best and insufficient for liability under court-developed principles of copyright.

Thus although financial intermediaries’ liability for copyright under traditional doctrines of secondary liability is a closer call than for domain name servers, it is still not a clear case. The argument supporting \textit{SOPA} however was that financial intermediaries and advertising service providers are a least cost avoider when it comes to online infringement: they have information
which can be used to trace wrongdoers and their accounts; they can detect and stop transactions involving those accounts; and they can act across multiple legal jurisdictions.

However, again, this reasoning is too simplistic. There are several reasons why we would need to at least question whether liability needs to be imposed by law, although these reasons are different from those applying to domain name servers. First, it may be that the market has the potential to respond appropriately. At least some credit card providers and advertising providers have already, in the absence of any legal obligation, taken steps to recognise IP rights, introducing systems whereby IP owners can complain about infringing merchants and have services to those merchants terminated (MacCarthy 2010b). If a legislative scheme were to be adopted, we would want to be convinced it was in some way superior to this voluntary system, and would remain superior even if circumstances or technology change.

Further, if the wronged party can deal directly with the intermediary and thereby reach a ‘deal’ to mitigate the harm caused by the wrongdoers, then legislation may be unnecessary and perhaps harmful if it sets in stone an inflexible or insufficiently nuanced set of practices. It is arguable a deal could be reached between IP owners and financial intermediaries: there are a finite number of significant and readily-identifiable payment providers and online advertising providers with whom rightsholders would need to deal to have a significant impact on the financing of infringing activity. Perhaps the impact would not succeed in totally wiping out funding for infringing sites, but perfect enforcement in this realm is probably too lofty a goal.

One would also expect that if mitigation efforts by intermediaries would reduce real, quantifiable economic harm, then IP owners should be prepared to pay intermediaries to take mitigating steps, at least up to the point where payment does not produce any further equivalent reduction in harm (MacCarthy 2010a). If no deal (or no satisfactory deal) has been reached, this could be due to information asymmetries or transaction costs, but it could also suggest that the costs of the desired mitigating steps exceed rightsholders’ willingness to pay, meaning that intermediaries are in fact not the least cost avoider, or that the costs of enforcement exceed the benefits to rightsholders.

These considerations beg a further question: what are the real benefits likely to be generated if financial intermediaries or advertising providers engage in enforcement? It is a mistake to assume (as US legislators appear to) that if identified steps by an intermediary will provide more enforcement than direct action against wrongdoers, it must be worthwhile for those steps to be taken. The calculus is particularly stark with copyright. We do not enforce copyright for its own sake; rather, we enforce it to achieve the goals of copyright, namely, provide incentives to creators.

This suggests that we would need to be convinced that enforcement by financial intermediaries and advertising providers would in fact lead to increased profits on the part of copyright owners, sufficient to outweigh the costs of any systems. If figures produced by the copyright industry of harm caused by piracy were true, the benefits might well outweigh any costs. It is far from clear, however, that those figures bear any relation to the actual harm suffered or the harm that would be prevented by mitigating steps such as are envisaged in SOPA. The situation in trade mark law is perhaps different. We enforce trade mark law chiefly so that consumers will not be confused as to the origin of goods or services or tricked into purchasing ‘fakes’. It is more difficult to quantify this ‘benefit’ as compared to the attempt to quantify the benefit of additional profits to a copyright owner. To the extent, too, that sites sell harmful counterfeit goods (such as fake medicines) the benefits of enforcement may well be much higher.

We also need to consider the costs for other parties and the other, longer-term implications. One would expect that any costs incurred by intermediaries would be passed on to all customers: will this have an impact on whether customers take up the service, and if so, will that stop some marginal players from entering ecommerce? Or will intermediaries tend to ‘overreact’ and too readily cut off services to accused websites (particularly given SOPA’s proposed broad immunity for such action), thus increasing barriers to innovation and to entry into the global online market? As for longer-term implications, the most significant question
is whether the imposition of liability by the US will encourage other countries to impose liability on financial intermediaries in other contexts. Is there a danger, in other words, of financial intermediaries and advertising providers accumulating obligations imposed by an increasing number of countries, each of which could be individually justified but which, taken cumulatively, impose prohibitive compliance burdens? Alternatively, is there some danger that international partners like the United Kingdom will become resentful of the unilateral imposition of US law in this way? It may be worth noting that the EU Parliament did in fact pass a resolution criticising the SOPA proposal (Whittaker 2011). The legislative background of SOPA, PIPA and COICA fails to address any of these issues.

CONCLUSION

As one might expect, the political battle over SOPA has tended to be dominated by polarised positions. To critics, the legislation represented a massive incursion into civil liberties, the shape of Internet technology and Internet freedom more generally. To proponents, it was a practical solution to a crisis in IP enforcement online and an efficient means of ensuring parties in a position to contribute to IP enforcement did so.

As this article has attempted to show, however, the real issues are somewhat more nuanced. Website blocking is not unheard of and nor is it always unjustified, as court discussions in the United Kingdom suggest. Action by credit card companies and other financial intermediaries in support of IP rights is already occurring in a voluntary way without excessive controversy and, once again, it is hard to argue that such action could never be justified – as the different judgments in the Perfect 10 case suggest.

In the end, the real problem with SOPA lay in its breadth and its lack of nuance. In seeking to provide efficient, streamlined mechanisms for enforcement and provide immunities to remove barriers (such as the fear of an action for breach of contract) to smooth cooperation between rightsholders and intermediaries, SOPA created a sweeping set of rules that allowed for ‘execution’ of a website on accusation, and without any real consideration of whether it was a proportional remedy in the particular case, or appropriate from the perspective of international comity. There was no spirit of compromise or balance in SOPA. By extending our analysis beyond a simplistic concept of the least cost avoider, considering broader costs and benefits, and more narrowly tailoring imposition of SOPA’s ultimate penalty to a smaller set of more justified cases, a far better solution could be reached.

REFERENCES


Celestine, A. 2012. ‘Why the Internet of the near future will be radically different’, Economic Times, 20 February 2012.


ENDNOTES

1 For a history, see Weatherall (2012). Notably, the US is not the only jurisdiction that has taken action against overseas infringing sites. In the UK, the High Court in *Twentieth Century Fox Film Corp. v British Telecommunications Plc* [2011] EWHC 1981 ordered British Telecommunications (BT) to block subscribers’ access to Newzbin, a site already found in earlier litigation to be infringing copyright on a mass scale: *Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] FSR 21. See also *Dramatico Entertainment Limited et al v British Sky Broadcasting Ltd et al* [2012] EWHC 1152 and *Dramatico Entertainment Limited et al v British Sky Broadcasting Ltd et al* [2012] EWHC 268 (concerning the similar blocking of the Pirate Bay website).

2 This term was defined in §101 of *SOPA* as introduced to mean Internet sites used to conduct business with US residents or otherwise demonstrating minimum contacts sufficient in other areas of US law to enable the exercise of personal jurisdiction of US courts over the owner or operator of the site.

3 The relevant criminal violations were 18 USC §2318 (Trafficking in counterfeit labels, illicit labels, or counterfeit documentation or packaging); 17 USC §506(a) (incorporated via 18 USC §2319) (wilful infringement of copyright (a) for commercial advantage or private financial gain, (b) by reproduction or distribution of copyrighted works with a total retail value of more than $1,000 over a 180 day period, or (c) by distribution of a work being prepared for commercial distribution); 18 USC §2319A (Unauthorised fixation of and trafficking in sound recordings and music videos of live musical performances); 18 USC §2319B (Unauthorised recording of Motion pictures in a Motion picture exhibition facility), 18 USC §2320 (Trafficking in counterfeit goods or services), or 18 USC Chapter 90 (which provides criminal offences relating to trade secrets).

4 The *Prioritizing Resources and Organization for Intellectual Property Act* of 2008, 110th Congress, HR 4279 (*PRO-IP Act*) gave power to courts to require forfeiture of property used or intended to be used to commit or facilitate the commission of an IP criminal offence. This provision has been used to justify the seizure of domain names of US-based sites. See generally Mellyn (2011).

5 Benkler used this phrase in describing the attack on Wikileaks that followed its publication of a trove of US diplomatic cables. Benkler’s phrase is equally apt to describe the kind of attack envisaged in *SOPA*.
This immunity would not, of course, extend to actions brought in foreign courts. This is not a hypothetical issue: when Visa decided to cease providing payment services to Russian site AllOfMP3, it was sued in a Russian court and ordered to continue processing transactions. In the event, Visa chose to process only Russian-based transactions: MacCarthy (2010a: 1092ff).

Although note that there seems to have been little discussion at least in public of the feasibility of implementing the measures in SOPA against only part of a site. Ofcom, in their 2011 report on website blocking, queried the granularity of the techniques reviewed, and proposed that one option would be for site owners to be asked to remove infringing content, with site blocking ‘reserved primarily for sites that fail to cooperate in a timely way with “notice and takedown” procedures’: (Ofcom 2011: 7).

Provision for studies was also to be found in the original draft of SOPA, but in the original draft, the studies seemed to be confined to issues of importance to rightsholders – namely, the effectiveness of the new mechanisms and ‘any need to amend the provisions ... to adapt to emerging technologies’: §106(b).

See in US Law 17 USC §512; in Australian law the affected activities are identified in Copyright Act 1968 (Cth) ss 116AC-116AF. The conditions required to be met are set out in s 116AH.

Note that subsequent to this legislation, courts have developed secondary liability in ways that denied liability for Internet intermediaries in at least some cases covered by the safe harbours: Reese, 2009. The High Court decision in Roadshow Films Pty Ltd v iiNet Ltd (No. 2) [2012] HCA 16 may have the effect of precluding liability for most Internet Service Providers under Australian law, but other intermediaries would still be at risk.

One exception, perhaps, is the sustained attack on Google in particular which appears to have occurred in the House Judiciary Committee. The hearing may be viewed at http://judiciary.house.gov/hearings/hear_11162011.html. An additional document produced by the Committee following the January 18, 2012 protests, also conveys considerable criticism of Google in particular, arguing that it had ‘generated enormous profits from illegal websites’, and that ‘Google’s conduct demonstrates there is a need for the government to step up enforcement of intellectual property rights online and provide increased protections to American consumers’ (US House Judiciary Committee 2012b). Interestingly, this ‘myths vs facts’ document misstates the ‘facts’ about SOPA, failing to mention at all the second mechanism set out in §103.

Interestingly, the High Court makes reference to similar reasoning in Roadshow v iiNet: Roadshow Films Pty Ltd v iiNet Ltd (No. 2) [2012] HCA 16, per French CJ, Crennan and Kiefel JJ at [55]; per Gummow and Hayne JJ at [110].

Another problem is that the theory assumes that the substantive law is appropriate, which assumption may not be correct. If the substantive law is calibrated to grant too much power to rightholders, this may be tolerable in a world of imperfect enforcement but less tolerable the more effective enforcement becomes.

Service provider in this context would include essentially any ‘provider of online services or network access, or the operator of facilities therefor’ (as defined in 17 USC §512(k)(1)) that operates a non-authoritative domain name system server – that is, a cache file comprised of domain name server lookups. As noted by Lemley et al (2011: 34) this is a ‘category that includes hundreds of thousands of small and medium-sized businesses, colleges, universities, nonprofit organizations’ as well as ISPs.

Notably, since SOPA was directed at non-authoritative domain name servers, it would not involve removal from the root.

As Dan Kaminsky argued, ‘[t]here has long been a bright line in computer security technology—do not subvert the will of the user, for the user is in the position to opt out of
all protections. By sanctioning the use of DNS filtering to combat copyright and trademark infringement, this bill will directly cause users to opt out of using their ISP’s name servers. This will lead to more hacks against American assets...’(Kaminsky 2011).

17 Data on Internet filtering may be obtained from the OpenNet Initiative, a collaboration between three groups – the Citizen Lab at the University of Toronto's Munk school of global affairs, Harvard University's Berkman centre for internet & society and the SecDev Group in Ottawa – that investigates internet filtering around the world: http://opennet.net.

18 See above Note 1.

19 Perfect 10, Inc v Visa International Service Association 494 F 3d 788 (9th Cir. 2007).

20 Perfect 10, Inc v Visa International Service Association 494 F 3d 788, 796-797 (9th Cir. 2007).

21 Perfect 10, Inc v Visa International Service Association 494 F 3d 788, 797-98 n8 (9th Cir. 2007).

22 Perfect 10, Inc v Visa International Service Association 494 F 3d 788, 803 (9th Cir. 2007).

23 Perfect 10, Inc v Visa International Service Association 494 F 3d 788, 794 (9th Cir. 2007).

24 Perfect 10, Inc v Visa International Service Association 494 F 3d 788, 816 (9th Cir. 2007).

25 Perfect 10, Inc v Visa International Service Association 494 F 3d 788, 815 (9th Cir. 2007).


27 Roadshow Films Pty Ltd v iiNet Ltd (No. 2) [2012] HCA 16, per French CJ, Crennan and Kiefel JJ at [65], [78]; per Gummow and Hayne JJ at [137]-[139]; [143]. The first of these judgments uses the language of ‘directness’ explicitly; Gummow and Hayne JJ rely on similar reasoning without using this language. It may be worth noting too that the first instance judgment also sought to create a test based on the directness of the connection between alleged authoriser and infringement, arguing that authorisation could only lie if the alleged authoriser provided the ‘means of infringement’: Roadshow Films Pty Ltd v iiNet Ltd (No 3) (2010) 263 ALR 215.

This article identifies some of the motivations behind, and the activities of, WikiLeaks. It then analyses the broader implications of the actions taken to withdraw funding support from WikiLeaks through the so-called ‘Banking Blockade’. This article then considers the impact of the Banking Blockade which effectively dried up donations to WikiLeaks in 2010. It assesses what this means for the future of the Internet itself as an increasingly privatised domain, where the power of contract can overcome protections offered by the general law.

INTRODUCTION

‘The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops.’ John Perry Barlow, Twitter, 3 December 2010.

In February 2012, WikiLeaks proved that it was down but certainly not out, with the publication of the ‘Global Intelligence Files’ or ‘Stratfor documents’, its fourth substantial leak in two years. WikiLeaks commenced publishing in December 2006, and released a range of documents such as Scientology texts, email logs of US Vice-Presidential candidate Sarah Palin and the Guantanamo Bay handbooks, to name but a few. This article however will focus on the leaks that appear to have had the most significant political impact, the Afghan war files, the Iraq war files, the US Embassy cables and the Stratfor files.

The Stratfor documents, comprising some five million emails from the Texas based company that operates as a ‘global intelligence publisher’ which has a large number of US Government and private sector clients, reflect the operations of a private intelligence agency with close ties to the US military (WikiLeaks 2012). One of the most publicised aspects of those documents revealed what most had long suspected to be the case: that the US Government had prepared a grand jury indictment against WikiLeaks founder and front man, Julian Assange. Whilst this confirmed the fact that the US does intend to take direct legal steps against Assange, few were surprised by this development. Moves have long been in train to ensure that the necessary groundwork for such an indictment have been put in place.

Assange has been under house arrest in the UK since December 2010 pending resolution of his legal battle against extradition to Sweden to face questioning regarding sexual assault allegations being investigated against him there. The legal challenges to the European Arrest Warrant and the ramifications of the extradition proceedings are not addressed in this article; however it is important to note that Assange has been fighting extradition to Sweden on the basis that it may open the door for his deportation to the US to face espionage charges there (Rundle 2012). Assange lost his appeal to the UK Supreme Court against extradition on the basis of a European Arrest Warrant in May 2012 (Assange v The Swedish Prosecution Authority [2012] UKSC 22) and his further request to re-open the case was denied by the Supreme Court on 14 June 2012 (Bowcott 2012). Subject to a possible appeal to the European Court of Human Rights, Assange faces extradition to Sweden at the beginning of July 2012.
What will happen to Assange once he is on Swedish soil is unknown. Nevertheless, it is not the detention of WikiLeaks’ founder, central protagonist, driving force and spokesman that has crippled the activities of WikiLeaks over 2011 and 2012. Rather it was the withdrawal of services by Visa, Mastercard, PayPal and others, effectively starving WikiLeaks of funds. The power of the US Government became secondary to the power of contract and private control of key aspects of e-commerce and the US Constitutional guarantees of free speech became irrelevant in the context of the actions of the private sector.

This article considers the nature and function of WikiLeaks as a publisher of information. It then examines the response of US lawmakers and the media to the key leaks. These responses are analysed in the context of considering the role played by contract in regulating participation in the public sphere. It is important that in considering the actions against Julian Assange and WikiLeaks that we also consider the implications of these actions more broadly for the freedom of Internet communication.

The mainstream media, itself having reached a point of identity crisis, has largely attempted to distance itself from WikiLeaks, unwilling to share any protections that it may have gained with a ‘mere whistleblower’ site. This characterisation too has implications for citizen participation in the broader democracy promised but not yet delivered by the Internet age (Benkler 2011). The publication by WikiLeaks of its archive of US diplomatic cables in unredacted form in September 2011 caused its former media partners (who had published various forms of the cables commencing in late 2010) to publicly condemn the publication and to denounce the publication as the sole action of Assange (Ball 2011). This effectively severed any further collaboration between WikiLeaks and these mainstream outlets, leaving WikiLeaks in the cold as it sought to fight off the Banking Blockade.

What does the concerted effort to shut WikiLeaks down and to silence Assange tell us about the effectiveness of the Internet as a fully functioning networked public sphere? In particular, why has contract and the exercise of private regulation been so successful in silencing WikiLeaks when the public law has not? The vital role of contract in justifying the withdrawal of essential services from WikiLeaks provides an exemplar of the importance of private rule making in the increasingly privatised public sphere and demonstrates yet again, that serious threats to freedom of expression can come from corporations as easily as from government. Whilst the Internet is characterised as a public domain for free discussion and dissemination of ideas and Web 2.0 platforms in particular can provide an opportunity for participation and exchange of ideas, these platforms are largely privately owned. For example, Facebook alone had 845 million monthly active users as of December 2011, all of whom had to agree to the Facebook terms of service in order to connect and stay connected (Facebook 2012).

**WIKILEAKS: A SHORT BIOGRAPHY**

WikiLeaks is a new model of online news dissemination. Its structure, operations and motivations are little understood, despite the worldwide furore caused by the publication by WikiLeaks of a series of documents in the period 2010-2012. However, the fallout from those publications has resulted in the arrest of US Army Private First Class Bradley Manning, the detention of Julian Assange, the withdrawal of service provision from WikiLeaks by numerous providers, including Amazon, MasterCard, VISA and PayPal, and extensive denial of service attacks both against and in support of WikiLeaks. It has also highlighted the growing influence of hacktivist collectives, such as Anonymous, whose actions in support of WikiLeaks have drawn attention to the power of the Internet as a protest platform.

Julian Assange registered the domain name WikiLeaks.org in October 2006 (Assange 2011, 130). Originally envisaged by Assange as a place where anyone could post material anonymously, which could then be read, commented upon and dissected by others, it quickly moved away from this model of publication. First, in order to encourage disclosure of material from whistleblowers WikiLeaks had to assure absolute anonymity of sources. In order to achieve this Assange developed the ‘Rubberhose’ program in combination with an
anonymous dropbox system. Second, the ‘wiki’ model depended upon people becoming involved, reading, commenting upon and editing comments and verifying the veracity of the documents. This simply did not happen, much to Assange’s early disappointment. Wading through a large volume of documents in order to discover a useful political point or to uncover a secret is not appealing to the majority of people accustomed to having the news packaged for them. Therefore WikiLeaks quickly had to adapt and take on the role of editor itself or to share this role with mainstream media. This explains, in part, Assange’s own personal transformation of his position and role from being a mere conduit for publication to seeing himself as a journalist and editor. It also explains the need for WikiLeaks to experiment with a variety of associations with mainstream news organisations (Leigh and Harding 2011). In addition, the large backlog of information that was to build up pending publication caused tensions within WikiLeaks. Daniel Domscheit-Berg, once a key member of the WikiLeaks team, left WikiLeaks to establish his own leak site after disagreements with Assange over the effort that came to be devoted to publishing material relating to the activities of the US Government and the delays this caused to the release of other information that had been collected by WikiLeaks (Domscheit-Berg 2011). As noted above, disagreements over treatment of disclosed material was also to lead to the breakdown of WikiLeaks’ partnerships with mainstream media publishers (Ball 2011).

The release of documents by WikiLeaks commenced in December 2006, with the publication of a letter relating to the Islamic Government of Somalia. This was followed in 2007 with the publication of the Guantanamo Bay manual, which covered the treatment and management of detainees, detailing matters of psychological torture and interrogation techniques (Assange 2011, 141-143).

In January 2008, WikiLeaks published hundreds of documents relating to massive tax evasion facilitated through the Swiss bank Julius Bär (Domscheit-Berg 2011, 17). This publication provoked legal action from the Bank, including a temporary injunction granted against WikiLeaks in a California court, as well as generating a huge amount of publicity for the nascent whistleblower site. The bank subsequently dropped further legal action when the injunction was lifted. 2008 also saw the publication of Scientology handbooks, American fraternity handbooks, Vice-Presidential candidate Sarah Palin’s emails, and the membership list of the British National Party. 2009 saw the publication of a number of reports and messages, including the pager messages from 9/11. Following a period offline in late 2009, when it was shut down by an injunction against Dynadot, who directed the WikiLeaks.org domain to the European servers of WikiLeaks, 2010 was to witness a series of major publications, including the video: Collateral Murder. Unlike the rest of WikiLeaks releases to date, Collateral Murder represented the first attempt by WikiLeaks to produce a major independent journalistic piece. The 17-minute video is an edited version of 39 minutes of footage filmed from the cockpit of a US Army Apache helicopter in Iraq. It shows a group of armed Iraqis, talking with two Reuters employees. The helicopter opens fire on the group, killing several people, including the Reuters employees. An Iraqi man taking his children to school is also shot and killed when he stops to render assistance. The emotional and inflammatory nature of the video attracted a great deal of press and public attention and represented a new development for WikiLeaks as a content provider.

The Afghanistan war logs were released in July 2010, with the Iraq war logs following in October 2010 and the US Embassy Diplomatic cables in November. The Afghan war logs comprised the US Military’s own logs of combat between 2004 and 2009, detailing matters such as requisitions for equipment. The Iraqi logs detailed field reports from the Iraq conflict, including details of civilian casualties and reports of torture by the Iraqi military and police (Benkler 2011, 325).

The source of all the leaks relating to US military activities is believed to be US Army Private First Class Bradley Manning. Manning, is currently in detention and being tried before a military court with respect to 22 counts including aiding the enemy; wrongfully causing intelligence to be published on the internet knowing that it is accessible to the enemy; theft of public property or records; transmitting defense information; and fraud and related activity in connection with computers, relating to the disclosure of information to WikiLeaks (Pilkington
At the time of the leaks Manning, then 21 years old, was stationed in Iraq. He is alleged to have copied the classified files to a CD and smuggled them out of the room. Manning was arrested in May 2010 following disclosures made to former hacker, Adrian Lamo, regarding the leaks. The Court Martial has been told that Manning was working in an atmosphere of lax security, with passwords being left beside computers on Post-it notes and computers containing confidential material being used for gaming and personal reasons. It is also claimed that Manning was motivated by conscience to make the document disclosure, with evidence being tendered that a computer used by Manning hosted the claim: ‘This is possibly one of the more significant documents of our time. Removing the fog of war and revealing the true nature of 21st century asymmetrical warfare.’ (Pilkington et al 2012).

In July 2010, fearing retribution from the US Government, following the publication of the Afghanistan war logs, an ‘insurance’ file was posted to WikiLeaks and a torrent site, allegedly to be decrypted in the event of anything happening to Assange. This file contains a large number of documents whose content is unknown, but presumably is highly damaging to US interests (Benkler 2011, 329).

As noted above, WikiLeaks published the Stratfor documents in February 2012.

ASSANGE’S MOTIVATIONS

According to Assange’s own description WikiLeaks was created from an intersection between a passion for freedom and transparency and an extensive understanding of computer networks. Assange had grown up as a hacker, a story colourfully portrayed in the book, Underground, on which Assange is listed as a researcher, and also later revealed as the hacker Mendax featured in the book (Dreyfus 1997). Inevitably these excursions as a young hacker had led to brushes with the law, but also the development of a sense of the global power of the Internet. This hacker culture clearly underpins the early incarnations of WikiLeaks.

Assange understands power as a network and a conspiracy. His mission in founding WikiLeaks was at least in part aimed at breaking up the strength of the conspiracy:

Authoritarian power knows how to strengthen itself through conspiracy, but it came to seem natural to me, logical indeed, that resistance would grow in direct proportion to how much people understood the conspiracy. I am not talking about conspiracy in the sense of secret, one-off cover ups, the ramblings of tinfoil-hat-wearing weirdos. I’m talking about systemic conspiracy, the habitual modus operandi for governments who prefer to do everything in secret. Information would set us free. And computer science, as a form of maths, would be our aid in revealing political relationships (Assange 2011, 123)

In an essay originally published in 2006 on the Cryptome.org site (another independent leaks site operated by John Young, with whom Assange had an early association) Assange outlined his thoughts on conspiracies and the role that leaks can play in undermining the efficient operation of secretive and unjust organisations. First, Assange identifies the conspiracies as connected graphs:

First take some nails (‘conspirators’) and hammer them into a board at random. Then take twine (‘communication’) and loop it from nail to nail without breaking. Call the twine connecting two nails a link. Unbroken twine means it is possible to travel from any nail to any other nail via twine and intermediary nails. Mathematicians say the [sic] this type of graph is connected.

Information flows from conspirator to conspirator. Not every conspirator trusts or knows every other conspirator even though all are connected. Some are on the fringe of the conspiracy, others are central and communicate with many conspirators and others still may know only two conspirators but be a bridge between important sections or groupings of the conspiracy (Assange 2006a, 2).
Assange then asserts that the power of the conspiracy can be reduced by disrupting information flow and by disrupting and throttling links: ‘A conspiracy sufficiently engaged in this manner is no longer able to comprehend its environment and plan robust action.’ (Assange, 2006b, 5). Just such an action is explored by Galloway and Thacker in The Exploit:

Protocological struggles do not center around changing existent technologies but instead involve discovering holes in existent technologies and projecting potential change through those holes. Hackers call these holes “exploits” (Galloway and Thacker 2007, 8).

When this power of exploiting network vulnerabilities is combined with political purposes, hacking becomes ‘hacktivism’ (Ludlow 2010). It is therefore notable that in these essays Assange also explicitly refers to regime change and the need to replace bad governance. This recognition of bad governance is placed in the context of an encouragement to act against it, asserting that those who witness an unjust act and do not act, become a party to that injustice (Assange 2006b; Assange 2011, 140). Thus the actions of WikiLeaks may be better understood in the context of the great battle for Internet freedom, the core preoccupation of hacktivism. As Manne has observed:

At the core of the cypherpunk philosophy was the belief that the great question of politics in the age of the internet was whether the state would strangle individual freedom and privacy through its capacity for electronic surveillance or whether autonomous individuals would eventually undermine and even destroy the state through their deployment of electronic weapons newly at hand. (Manne 2011).

Of course, both WikiLeaks and Assange have evolved since 2006. The Cryptome publications of 2006 do not necessarily reflect Assange’s motivations in 2012, however they are useful in understanding the broad context of the activities and philosophies underpinning WikiLeaks and should therefore be considered. In particular, the strong emphasis on openness and transparency is a fundamental meme of Internet pioneers. As Krotoski has observed WikiLeaks utilises the open and transparent nature of the internet itself in the structure of the publication system (Krotoski 2011). Therefore, criticisms of its actions may more appropriately be directed at a system that resulted in such massive disclosure of its supposed secrets (Goldsmith 2010).

THE NETWORKED PUBLIC SPHERE

In his influential work on peer production, The Wealth of Networks, Yochai Benkler identified the shift from a mass-mediated public sphere to an Internet-enabled ‘networked public sphere’. In Chapter 7 of that work Benkler identifies the growth in citizen-enabled media, the ability of people to become publishers and active participants, rather than passive recipients, of news and public debate. Social production tools such as email, social media, blogs and wikis equip individuals with the power to reach an audience of a scale formerly reserved for the mass media. This empowerment of citizen publishers, according to Benkler, has the effect of democratisation, through participation in debate and agenda setting (Benkler 2006, 272). Of course, WikiLeaks is the exemplar of such forms of publication, uncontrolled by government and to a large extent uncontrolled by mass media. WikiLeaks has had mixed success in partnering with large news organisations (Leigh and Harding 2011) and Assange is now recreating himself as a television talk show host (whilst under house arrest).

These ideas have since been embraced and amplified by others such as Zizi Papacharissi, who in her work A Private Sphere, has argued that citizen consumers feel disenfranchised by politics and mass media (Papacharissi 2010, 15). The Internet provides citizens with the technology and capability to create new spaces in which to develop their own private spheres (Papacharissi 2010, 23). Whereas Benkler presents an optimistic view of the digitally empowered ‘prosumer’ (Benkler 2011, 375), Papcharissi warns that the Internet alone does not inherently improve democracy or civic participation (103 -105). It is threatened by
increasing moves towards a walled garden approach to the Internet, favoured both by government and private platform providers.

**THE US RESPONSE**

The Obama administration has found itself in a contradictory stance on Internet activism. In January 2010, Secretary of State Hillary Clinton, gave an address on the importance of internet freedom, referring to a speech in which President Obama ‘spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship’ (Clinton 2010). Heralding the power of the First Amendment, Secretary Clinton noted the importance of freedom of expression on the Internet and stressed the role of the US as global champion of an open Internet, empowering citizens and making governments accountable.

Following the release of the ‘Collateral Murder’ video, the US Justice Department commenced a criminal investigation into WikiLeaks. It demanded that Twitter disclose the tweets and subscription data of Assange and others who had been involved in the production of the video (Sifry 2011, 127).

In March 2010, WikiLeaks released a report prepared in 2008 for the US Army Counterintelligence Center (WikiLeaks 2010). That report, the purpose of which was to ‘assess the counterintelligence threat posed to the US Army by the WikiLeaks.org Web Site’ concluded that WikiLeaks ‘represents a potential force protection, counterintelligence, operational security (OPSEC), and information security (INFOSEC) threat to the US Army’. The Report however appeared to lack a true understanding of how WikiLeaks operated, citing directly from the tongue in cheek assertion on the WikiLeaks site that the stated intent of WikiLeaks is ‘to expose unethical practices, illegal behavior, and wrongdoing within corrupt corporations and oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa, and the Middle East…The developers believe that the disclosure of sensitive or classified information involving a foreign government or corporation will eventually result in the increased accountability of a democratic, oppressive, or corrupt government to its citizens.’

The Report than goes on to suggest that the real dangers arise from the fact that WikiLeaks is essentially an unmoderated site that allows anyone to post and respond to information: ‘the [WikiLeaks] site could be used to post fabricated information; to post misinformation, disinformation, and propaganda; or to conduct perception management and influence operations designed to convey a negative message to those who view or retrieve information from the Web site.’ It notes the uncertain legal status of WikiLeaks and includes an acknowledgement that efforts to discredit WikiLeaks include claims that it is a front for the CIA. The Report also notes that several countries, such as China, Israel, North Korea, Russia, Thailand and Zimbabwe have blocked access to WikiLeaks ‘type’ websites, and have claimed the right to investigate and prosecute such sites and to remove and block access to content on such sites. Most tellingly, in light of subsequent developments the Report states:

*WikiLeaks.org uses trust as a center of gravity by assuring insiders, leakers, and whistleblowers who pass information to WikiLeaks.org personnel or who post information to the Web site that they will remain anonymous. The identification, exposure, or termination of employment of or legal actions against current or former insiders, leakers, or whistleblowers could damage or destroy this center of gravity and deter other from using Wikileaks.org to make such information public. (WikiLeaks 2010)*

In this Report, WikiLeaks appears to be a far more organised entity than the single person organisation that it essentially was at that time (Lovink and Riemens 2010).
THE BANKING BLOCKADE AND WITHDRAWAL OF SERVICE FROM WIKILEAKS

The Cablegate documents (a vast cache of cables from various US Embassies back to Washington) were released globally via various news organisations, including the New York Times, Der Speigel, El Pais and The Guardian, on 29 November 2010. In the days following this release several US senators and media commentators made calls for the arrest or assassination of Julian Assange. The incoming chair of House Homeland Security Committee, Senator Peter King, had pre-empted the release by publicly questioning the Obama administration regarding whether WikiLeaks could be designated as a foreign Terrorist organisation (McCullagh 2010a). Republican Presidential hopeful Newt Gingrich called for Assange to be classified as an enemy combatant (Fox News 2010). Republican Senator Mitch McConnell claimed that Assange was a ‘high-tech terrorist’ stating that: ‘He has done enormous damage to our country’ (McCullagh 2010b). In particular, Republican Senator Joseph Lieberman raised the question as to why companies such Amazon as were supporting WikiLeaks by facilitating donations and hosting their services. Amazon stopped hosting WikiLeaks on 1 December 2010 claiming that WikiLeaks was in breach of its terms of service in a number of ways, particularly with respect to its rights to own or control hosted content (AWS n.d.). Ironically, WikiLeaks had been prompted to move to the Amazon Cloud hosting service due to the large scale DDoS attacks it had been experiencing from pro-government activists following the publication of the Embassy cables (Benkler 2011, 338-339). A spokesperson for Senator Lieberman immediately announced: ‘Sen. Lieberman hopes that the Amazon case will send the message to other companies that might host WikiLeaks that it would be irresponsible to host the site’ (Slajda 2010). Every DNS followed suit on 2 December 2010, making it impossible to access the WikiLeaks website by redirecting its domain name. PayPal severed its payment facility for WikiLeaks donations on 3 December 2010, stating: ‘PayPal has permanently restricted the account used by WikiLeaks due to a violation of the PayPal Acceptable Use Policy, which states that our payment service cannot be used for any activities that encourage, promote, facilitate or instruct others to engage in illegal activity. We’ve notified the account holder of this action.’(WikiLeaks 2011, PayPal 2010a) This position was reviewed and reinforced in a statement from PayPal’s General Counsel on 7 December 2010 (PayPal 2010b).

On 7 December 2010 VISA and Mastercard stopped processing payments to WikiLeaks. Mastercard’s spokesperson told Cnet: ‘MasterCard rules prohibit customers from directly or indirectly engaging in or facilitating any action that is illegal’ (McCullagh 2010b). VISA Europe justified its suspension of service on the grounds that it was investigating whether WikiLeaks contravened any VISA operating rules (BBC 2010). The Bank of America discontinued service to WikiLeaks on 18 December 2010 stating that it was acting upon ‘reasonable belief that WikiLeaks may be engaged in activities that are, amongst other things, inconsistent with our internal policies for processing payments (AFP 2010). Apple removed the WikiLeaks app (not actually provided by WikiLeaks) from its App Store on 20 December 2010 on the grounds that the App violated the developer guidelines. Western Union placed WikiLeaks to its Interdiction List on 21 December 2010 (WikiLeaks 2011, 6-8). WikiLeaks became effectively cut off from its key funding sources and was characterised as an outlaw institution.

All of these actions were based on the service providers’ claim that WikiLeaks had violated their terms of service, such as indicated by PayPal example above. This is despite the fact that the US Government publicly stated, following a Treasury Department investigation instigated by complaints aired by Senator Peter King, that there are no grounds for WikiLeaks to be blacklisted (Norman 2011, Rubenfeld 2011). WikiLeaks asserted that the withdrawal of service from WikiLeaks is based upon a letter sent to Julian Assange’s lawyers from the US State Department on 27 November 2010. That carefully worded letter suggested that WikiLeaks was in possession of secret information which had been provided in breach of US laws. The letter, signed by Harold Koh, Legal Adviser of the Department of State, stated:
‘if any of the materials you intend to publish were provided by any government officials, or any intermediary without proper authorization, they were provided in violation of U.S. law and without regard for the grave consequences of this action. As long as WikiLeaks holds such material, the violation of the law is ongoing.’

The letter then concluded with wording which appears designed to provide a foundation for later legal action:

*We will not engage in a negotiation regarding the further release or dissemination of illegally obtained U.S. Government classified materials. If you are genuinely interested in seeking to stop the damage from your actions, you should: 1) ensure WikiLeaks ceases publishing any and all such materials; 2) ensure WikiLeaks returns any and all classified U.S. Government material in its possession; and 3) remove and destroy all records of this material from WikiLeaks’ databases. (Reuters 2010; Koh 2010)*

This State Department letter had in fact been prompted by a letter from WikiLeaks, anticipating the publication of the cables and seeking assistance with appropriate redaction. PayPal later confirmed that the State Department letter was influential in its conclusion that WikiLeaks was illegal: ‘We have an acceptable use policy and their job is make sure that our customers are protected, making sure that we comply with regulations around the world and making sure that we protect our brand.’(Tsotsis 2010)

WikiLeaks has stated that the Banking Blockade has effectively starved it of income (95% of its revenue, costing it ‘tens of millions of pounds’) and this lead in 2011 to WikiLeaks suspending its publishing operations (WikiLeaks 2011; Rundle 2011).

Like much of WikiLeaks’ contentious activities, these developments were surrounded by a number of other controversies, including allegations that the Bank of America had engaged a legal firm to sabotage WikiLeaks and its known supporters: the attempts to revoke the charitable status of Wau Holland Foundation (an organisation receiving donations on behalf of WikiLeaks) and its suspension by Paypal, and the DDoS attacks initiated by Anonymous in support of WikiLeaks against MasterCard and VISA. WikiLeaks has also indicated that it will bring anti-trust actions against MasterCard and VISA and has attempted to engage the European Commission in these actions.

The massive number of users of online services such as Facebook, World of Warcraft, Twitter, are the fodder of daily news. The fact that each user of such platforms has first to agree to a one-sided End-User Licence Agreement is less well understood. Google and Apple have however, more recently, come under fire for their privacy terms and users may be becoming more savvy about what they are consenting to when they click ‘I Agree’. More generally, such terms are presented on a take it or leave it basis and users have no choice than to accept the terms if they wish to use the service.

WikiLeaks found itself in such a situation when it moved its data to Amazon’s Cloud service, not anticipating that it would be hamstrung by the Terms of Service and disputing of course that it had been found guilty of any illegal activity. In any event, whether its activities are illegal does not matter, because as a private enterprise, Amazon is under no obligation to host WikiLeaks. Nor in fact is PayPal, Mastercard or Visa.

What this serves to illustrate is that we are increasingly becoming subject to the private regulatory regimes of contract, with no opportunity to bargain, dissent or renegotiate. Rebecca MacKinnon correctly observes: ‘the political discourse in the United States and in many other democracies now depends increasingly on privately owned and operated digital intermediaries’(MacKinnon 2012, 86). Rundle notes (citing Assange) that the ban imposed by Visa, Mastercard and PayPal restricted not only the operations of WikiLeaks but individual rights regarding contributions to and support of WikiLeaks work (ie anyone who wanted to ‘vote with their wallet’) (Rundle 2011). The extent of control over online transactions exercised by these three corporations (97%) creates a de facto monopoly, meaning that these corporations wield extensive power over global online purchasing decisions and hence significant political power (Rundle 2011). Rundle observes:
Thus the net/web is both, as is endlessly celebrated, a device for openness zero cost global communication and organisation, flattened hierarchies, etc- but also the greatest tool for the centralisation of power that the world has yet seen. WikiLeaks’ mission, is, in part, to make that centralisation visible and contest it – so inevitably the manner of attacking relied crucially on using the monopoly power of financial transaction, which is heavily linked into the US state. (Rundle 2011)

CONCLUSION

In April 2012 a coalition of US based WikiLeaks supporters, including Daniel Ellsberg, and Internet activist and spokesman for the Electronic Frontiers Foundation, John Perry Barlow, announced that they were planning a US based foundation which could be used to channel funds to WikiLeaks and others who had been affected by actions like the Banking Blockade (Ball 2012). It is believed that a US based foundation would have greater success in defending WikiLeaks’s activities on the basis of the US First Amendment.

To some extent, the WikiLeaks story has served its purpose by focusing public attention on a number of important questions, such as the independence and autonomy of media (an issue also sharply in focus in the UK following the News of the World scandal), and importantly the power of private organisations in restricting access to Internet services. As Barlow has observed: ‘We now have organisations with the ability to stifle free expression with no bill of rights that applies to them- just terms of service’ (Ball 2012). How we choose to respond to this challenge remains to be seen.

REFERENCES


ENDNOTES

1. Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom, Yale University Press, 2006, 10. The role of the public sphere in fostering democracy is derived from the work of Jurgen Habermas, The Structural Transformation of the Public Sphere, 1962, trans Thomas Burger, MIT Press, 1989. See further, Mark Poster, ‘CyberDemocracy: Internet and the Public Sphere’, 1995, in which Poster asserts that whilst the internet should be regarded as a public space, the nature of machine mediated discussion so transforms the nature of that discussion that Habermas’ concept of the public sphere as ‘a homogenous space of embodied subjects in symmetrical relations, pursuing consensus through the critique of arguments and the presentation of validity claims’ should be abandoned. Nevertheless, this article formed the foundation stone of a more extended analysis of the digital public sphere. Available at http://www.humanities.uci.edu/mposter/writings/democ.html.


6. WikiLeaks, 2010, citing a number of other confidential sources.
This article examines the role of Internet Service Providers (ISPs) in combating botnets. The first section addresses recent Australian initiatives where ISPs are called on to take a proactive security role. The first initiative is the Australian Internet Security Initiative established by ACMA. The second, and most recent, initiative is the Australian Internet Industry Association (IIA) Code of Practice consultation paper on ‘For Industry Self-Regulation in the Area of E-Security’. The E-Security initiative involves ISP monitoring and detecting compromised computers connected to their networks, notifying customers when their computers are infected and, hence, are part of a botnet, providing links to information to disinfect a computer, and quarantining the infected computer until it is ‘fit for connection’.

The article examines ISP legal liability issues and addresses the February 2010 amendments to the Telecommunications Interception Act which exempt ISPs from the obligations of the previously established interception and warrant framework when performing detection and monitoring (including interception of communications) for reasons related to network protection and security.

INTRODUCTION

Botnets have captured the attention of the computer security experts and governments and are considered by many to be one of the most significant threats to the integrity of the Internet. A botnet is a collection of remotely controlled and compromised computers known as “zombies” controlled by a “botmaster / botherder” that run software known as ‘bots’ on the zombie computer. In a metaphorical sense, a botnet parallels a mode of distribution. Botnets may involve anywhere from a few hundred bots to several thousand to one documented case involving 13 million bots. Zombies receive their instructions from the bot master in the form of a bot (malicious software). The bot must retrieve its instructions from what is known as the “command and control” (C&C) of the botnet. This often occurs in the Internet Relay Chat server or a set of designated domain names allowing a botmaster or a bot herder to control the bots remotely to perform activities which tend to be of a malicious nature. Other botnets leverage peer-to-peer networks and computer game consoles for their command and control locations.

Why do botnets matter? Botnets are said to be involved in most forms of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click-fraud, to keylogging technology and traffic sniffing which captures passwords and credit card information, and to mass identity theft. In the words of leading botnet researcher Jeremy Linden of Arbor Networks, “Almost every
major crime problem on the Net can be traced to them.” Internet security guru Vincent Cerf has equated botnets to a pandemic, warning that a quarter of all personal computers have already become zombies. Botnets are perceived by many experts as a pandemic, yet most users and businesses are unaware of the term or the threat that botnets pose to the Internet.

More compelling is the description of botnets, zombies and related crimes from someone within the inner workings of the commercial child pornography industry. The article, “My Life in Child Pornography” was posted to the wikileaks site and is considered by many security experts and cybercrime researchers to be accurate and authoritative. The anonymously written document was translated from German to English. A relevant excerpt is copied below:

“But how, specifically, child pornography is sold? ... Today, the answer is SPAM.... In order to send spam Trojan-infected (zombie) computers are used. But zombie computers have yet another use: it will be used in a targeted fashion to steal identities. They even use the computer of the user whose identity is stolen to conduct credible transactions such as purchase of domains, etc. But that is not everything: the installed Trojans are sometimes used as a SOCKS proxy to upload CP. The Russians have even worked out a schema to use infected computer as a network combing these infected computers (each computer would be part of a huge, redundant cluster) as a kind of huge, distributed and remote servers can be (a kind of Freenet Project, however, by using infected computers as the nodes). I want to make one thing clear: if you have an email address, there is a possibility that there is child pornography on your computer because you have received CP advertising. And if your computer is not 100% safe against Trojans, viruses and rootkits, there is the possibility that your computer is part of the vast child pornography network.”

For those readers having difficulty with the technology, allow me to put it into layman’s terms. Once a computer is a zombie, it can be used in every illegal function of the child pornography distribution chain. This includes SPAM botnets, links found within SPAM messages which trigger the downloading of malicious software (malware). The malware infects your computer and takes it over without your ever knowing that it has done so. Your banking details are stolen. Other items related to your identity are stolen (Eg. Your email address is highjacked, usernames and passwords). The stolen identity (email and credit card details) are then used to register and purchase domain names, to launder money, to store child pornography, and to distribute child pornography. All of this done typically in a manner so that the user has no idea that their computer is a zombie, not to mention that child pornography and other nefarious materials are being stored and later distributed using your computer.

Governments and organisations are beginning to recognise the importance of tackling botnets. The problem of botnets is described by the European Network and Information Security Agency as:

“Botnets represent a steadily increasing problem threatening governments, industries, companies and individual users with devastating consequences that must be avoided. Urgent preventive measures must be given the highest priority if this criminal activity is to be defeated. Otherwise the effect on the basic worldwide network infrastructures could be disastrous.”

Governments are focusing much attention on cyber security and cyber crime with botnets driving many initiatives. The United States, the United Kingdom and Australian governments have all announced major cyber security strategies in 2009 with botnets featured predominantly.
COMBATING BOTNETS

The following diagram explains a botnet. In Step 1, the botnet herder needs to acquire zombie computers to form part of his/her botnet. This may be done in a variety of ways but it is often done with a malicious software that self-replicates, known as a “worm”. The computer becomes infected and a zombie subject to the commands of the botnet herder. In Step 2, the botnet master then makes content available to the bots, which causes them to perform actions. The botnet herder then uses software known as a ‘bot’ to command the zombie to perform certain actions. The botnet herder may issue commands or he/she may hire out the botnet to third parties for nefarious purpose such as to send illegal spam, or to launch a distributed denial of service attack.

There are approximately four methods of tackling botnets which I will refer to as:

1) ISP and/or domain name service (DNS) registrar disconnection of C & C when located on web pages,

2) Infiltration and disruption of the C&C in IRC, P2P, or Wifi Modem channels (typically by security organisations),

3) Prosecution of the botnet herder(s), and

4) Zombie/Bot remediation (typically by the ISP). ISPs play a role in all but one of these methods; infiltration and disruption of the C&C where the botnet is receiving its commands in the IRC or P2P channels is typically not performed by ISPs. Each of these methods requires some elaboration as to the architectural structure of the botnet and the role of the ISP.
ISP AND/OR DNS REGISTRAR DISCONNECTION OF C & C LOCATIONS

The first method involves contacting the DNS provider or ISP to inform them that they have clients who are using their services to run botnets. The DNS provider in most instances will be an ISP. New and amended entries into the domain name registries are managed by ISPs and by corporations offering such services such as NetRegistry. The database that maps domain-names to IP addresses is performed by those ISPs who operate domain-name servers. Where a botnet is programmed to receive its instructions (C & C) from a website, a request may be made for disconnection of service or the ISP may blacklist the range of unique Internet Protocol Addresses the botnet is using to run its C & C. The DNS registrar may also be contacted with a request to remove the domain name from its register. This can be an effective route but requires the person to know the webpages the botnet is connecting to receive its instructions (C & C), the DNS/IP address of the IRC server, port and nickname of the bot, and most importantly, it requires desire on the ISP to take action.

There is no legal obligation for ISPs and DNS registrars to take any action to disconnect the webpage or remove the domain name. That said, many DNS providers and ISPs do not tolerate abuse of their service and will take measures to stop the botnet by blacklisting the IP addresses where the C & C receives its instruction or termination of their connection contracts. This approach, however, is not always possible for a number of reasons. The service provider may have legal obligations that restrict its ability to disconnect or blacklist. The diversification of IP addresses and webpages across multiple ISPs and DNS registrars and often jurisdictions may make this approach unfeasible. For example, where a botnet has multiple channels where it receives its instructions, several hundred ISPs may need to be contacted across different jurisdictions. Any action taken would require disconnection by ISPs at the same time. Otherwise the botnet merely selects another channel to receive its instructions (C & C). Botnet could be set to receive instructions (C & C) through multiple channels: webpages, search engine keywords, IRC, and P2P. Where the C & C is located in a P2P channel, ISPs do not play a role. The instructions could be embedded in an innocent party’s webpage such as CNN. The ISP will not disconnect an innocent party though they may be in a good position to contact and inform the innocent third party that they are being used as part of a botnet.

INFILTRATION AND DISRUPTION OF THE C & C IN IRC OR P2P CHANNELS (TYPICALLY BY SECURITY ORGANISATIONS)

The second method has security researchers running interference with the C & C of the botnet. This might include infiltrating the C & C and initiating commands of their own, thereby disrupting the botnet. In some instances, the individuals may elect to launch a DDoS attack on webpages where the C & C receives its instructions. Again, this disrupts the botnet. This type of approach, however, requires perpetual observation and constant attention by the individual or organisation disrupting the botnet. It does not permanently shut down the botnet. It is neither desirable nor practical and, in the case of a DDoS attack, it is outright illegal as it would constitute unauthorised access, modification or impairment to data held in a computer under section 476 of the Criminal Code 1995 (Cth). Self-defence would likewise not apply in this situation, as botnet activists are not defending their own property. Moreover, where C & C is embedded into innocent third party websites, the extent of tolerated interference significantly diminishes.

PROSECUTION OF BOTNET HERDER

This method looks at prosecution of a botnet herder. In order to prosecute a botnet herder, you must first make an identification of the botnet herder. This is an extremely difficult task. Several factors must be present in order to identify a botnet herder:

- The IP address of the IRC server must be known along with the port, and nicknames of the bot
• The IP address may be traced to the ISP or DNS registrar
• The ISP or DNS registrar would have to provide subscriber information (either voluntarily or through a production order to disclose subscriber information and data traffic logs)
• The subscriber information would have to be truthful and accurate in order to correctly ascertain the identity of the botnet herder
• Evidence would need to be collected before proceeding to press charges

Production orders to produce subscriber information would, in most instances, be imperative to a successful prosecution of a botnet herder. The reality, however, is that many criminals do not use their real identities to subscribe to Internet services, or they register the services under an empty holding company. To add to this, stolen credit cards are often used as payment for many Internet services. The reality is that traceback of a botnet herder, depending on the sophistication of the botnet and the efforts of the botnet herder to remain anonymous, is in many instances very difficult. Where botnet herders use obfuscation tools such as proxies, fast-flux, P2P and dynamic DNS, traceback is almost impossible.

The sophisticated botnet herders are believed to be predominantly connected to organised crime. The less sophisticated group linger in chatrooms using their hacking names, discuss botnet techniques, and leave C & C channels open for long periods of time. Traceback of this type of botnet herder is more probable. Without successful traceback, a botnet herder cannot be identified and there can be no prosecution. Where prosecution is an option, you are often dealing with a lower level botnet herder who takes minimal precautions to shield their true identities in the operation of their botnet.

In the latter case of the lower level botnet herder, prosecution may be possible. Typically, however, an ISP will be involved as they will have to disclose subscriber information to link an IP address to the botnet herder. An ISP may also be called upon to intercept communications in order to collect evidence against a botnet herder. Australian telecommunications carriers (includes ISPs) are required by law to have interception capabilities, generally to be used for evidence gathering in connection with serious offences (crimes such as murder, terrorism, and child pornography). According to Part 15 of the Telecommunications Act (Cth), a serious offence includes any criminal offence which would attract a minimum of seven years in prison. The unauthorised access, modification and use provisions would qualify as a serious offence as the maximum sentence is 10 years. The use of a botnet would likely qualify as a serious offence which would allow law enforcement to compel ISPs to intercept communications between parties.

ZOMBIE/BOT REMEDIATION

The last approach involves remedying the infected zombie computers that the botnet has control of. In this approach, one could monitor the zombie computers noting which IP addresses are operating as zombies. One could then link the IP address to the relevant ISP (via the WHOIS protocol), and contact the ISP with the relevant information. This plan requires the ISP to contact the IP address subscriber, notify them of the problem, and then the owner should take measures to disinfect the computer. Again, this solution depends on the willingness of the ISP to act as middle man between the researcher and the owner of the infected computer. ISPs cannot, absent a criminal investigation and the appropriate warrant, disclose subscriber information about an IP address. To do so would be in contravention of the Privacy Act, Telecommunications Interception Act, and Telecommunications Act. At the moment, ISPs have no legal obligation to inform their customers that their computers are insecure though this type of volunteer measure is being considered by ISPs under the IIA E-Security Code which will be examined later in this article.
THE BOTNET THAT NEVER DIES

The last method differs from the first three in one significant manner. It potentially remedies zombie machines. This is critical for long-term takedown of a botnet.

The first two methods (ISP and/or domain name service (DNS) registrar disconnection of C & C when located on webpage, and Infiltration and disruption of the C & C in IRC or P2P channels), only put off the botnet herder for a period of time. The botnet herder can still set up new C & C channels, and write new bots (malicious software programs) to communicate with the zombie computers. The takedown of the botnet is, therefore, only temporary as most botnets are self-replicating worms. This means that stopping the C & C of the botnet does not necessarily prevent the botnet from continuing to spread and thus acquiring new zombie computers. It also does not prevent a botnet from spreading new bots once a new C & C is established.

Prosecuting the botnet herder also is not an absolute solution as the botnet is highly susceptible to being taken over by another botnet herder. Moreover, the zombie machines sit dormant awaiting new instructions. Only the last method, zombie/bot remediation, potentially removes the zombie computers from the equation. To use an analogy to war, one can disrupt an army by interfering with its communications systems, and one can kill the General but there will always be more Generals willing to step up, and ways of re-establishing communications. But if there are no soldiers, the General has no one to carry out the orders in his command.

THE ROLE OF ISPs

As long as a botnet herder has zombies waiting to receive instructions and carry out commands, a botnet is still susceptible to receiving new instructions to perform malicious activity. The question then becomes how do we successfully reduce the number of bots and zombies? Some alternatives look at requiring users to have a computer licence before they are allowed to connect to the Internet. Another option would require all computers sold to have pre-installed anti-virus software before a computer may be connected to the Internet. However, anti-virus software only blocks a certain percentage of malicious traffic, and is reliant on the end-user patching their systems (browser, router, hardware) on a frequent basis.

Once a user’s machine is infected and part of a botnet, they are likely to be unaware that their computer has been compromised. Where a user is aware that their computer is infected, it is extremely unlikely that they will be aware that their machine is being used to commit crimes. User and business education, therefore, is a must in any effort to better secure the Internet. There is a growing recognition that ISPs are in the best position to assist in zombie removal. It has been suggested in Australia that ISPs must be active not only in the removal and remedying of their customer’s compromised machines but must also play a role in educating users on safer online habits.

Internet Service Providers have taken an increasingly active role in combating botnets, malware and other malicious activity. ISPs have typically placed a strong emphasis on filtering spam botnets. This has predominantly taken shape through sophisticated spam filters known as ingress and egress filtering. Ingress filtering refers to filtering packets as they enter into a system whereas egress filtering refers to filtering packets as they exit a network system. The result is that much spam content does not arrive in one’s “INBOX” but find its way to the “BULK” or “SPAM” folders on a user’s computer.

This preventative measure merely quarantines the undesired content to a place where users may still access the files. This technique, while mitigating against some malicious activity, does not address the larger problem of what needs to be done once a machine is infected and part of a botnet. Many ISPs and organisations also block port 25. Much spam and malicious traffic is routed through port 25, therefore, it is thought that blocking this port reduces the problem of unwanted content distributed through botnets. As articulated in the ITU Botnet...
Mitigation Toolkit document, “attempting to combat botnets simply by blocking port 25 has been compared, colourfully (and validly) by one expert to “treating lung cancer with cough syrup”.” Only a portion of malware travels through port 25 while malware actors may simply re-channel traffic through another port. Not all ISPs do any ingress and egress filtering for malicious content nor do they all block port 25.

ISPs are generally not responsible for the security of their customer’s computers or for monitoring the content that their customers place and distribute online. ISPs are generally seen as ‘mere conduits’ of information where they have not traditionally examined the content flowing through their networks. The role of ISPs, however, is changing. ISPs often filter spam botnets, block problematic ports, and they will be filtering RC classified content under the Government’s proposed Internet filtering scheme. The next proposed change is the role of the ISP to tackle botnets more generally as ISPs are seen as a critical player in any successful initiative in the area. Recent Australian ISP initiatives are considered in the following sections.

AUSTRALIAN INTERNET SECURITY INITIATIVE

The Australian Communications and Media Authority (ACMA) introduced a project in 2005 known as the Australian Internet Security Initiative (AISI) to help address the problem of botnets. AISI is run by the ACMA. According to the ACMA website, AISI collects data on compromised computers and forwards daily reports to participating Australian ISPs. There are over 75 ISPs participating in the project. When an ISP receives the daily botnet report, they may inform their customers that their computers are compromised and they may provide advice as to how to remedy the problem. There is no obligation on the ISP to use the reported data or to inform customers where their machines are compromised. The extent of ISP involvement is completely voluntary and discretionary. The information collected by AISI generally relates to spam botnets.

The focus on spam botnets may be in part due to the jurisdictional limits of ACMA. The provisions in the Spam Act 2003 designate ACMA as the overseer to the act with powers to investigate and press charges against spam offenders. Under the Telecommunications Act, ACMA may appoint officers to become inspectors for the purpose of carrying out spam investigations. Investigators are then able to request warrants and then perform search and seizures relating to breaches of the Spam Act, conduct searches to monitor compliance, and access computer data relevant to the Spam Act. ACMA does not have the same jurisdiction over malware, adware spyware, or botnets in general. While many botnets are used to deliver specific types of content such as spam, a botnet itself if neutral and may be used to distribute any form of content. The only information since its inception available about the AISI project is a few paragraphs on the ACMA website that outline the existence of a project. There is no public information available on the specifics of the project, methodology of data collection, reliability and integrity of data, the extent of ISP participation, nor reported tangible outcomes or statistics from the project.

The AISI project, however, has inspired a number of security projects to follow suit with the International Telecommunications Union (ITU) release of the “ITU Botnet Mitigation Toolkit” in January 2008, along with the Australian Internet Industry Association’s (IIA) consultation document in September 2009 regarding e-security self-regulation. The IIA E-Security Code represents a formalisation of the previous voluntary initiative to that of a more formal ISP initiative.

CO-REGULATION MODEL

Australian ISPs are co-regulated. Schedule 7 of the Broadcasting Services Act 1992 (BSA) introduces co-regulation between ACMA and the telecommunications industry. The industry’s involvement consists of the development of industry codes of practice and industry standards. The industry codes have mostly dealt with classification of content and related
issues of removal of offensive content, and on educating users on the use of content services. Schedule 7 of the BSA provides regulations targeted at content carriers. These regulations, like those of the industry code, predominantly relate to content. Where the ACMA classifies content as prohibited, Schedule 7 sets out obligations on ISPs to remove prohibited content when hosted on their network. The e-security consultation paper, if adopted by the IIA, will form part of an industry code to be adhered to by all ISPs. This move from an AISI initiative to a self-regulatory code is a formalisation of ISP involvement in dismantling botnets.

INTERNET INDUSTRY OF AUSTRALIA E-SECURITY CODE

The Internet Industry Association (IIA) e-security consultation document provides an overview of objectives, principles, a summary of terminology, and references other security organisations such as Cert Australia, AusCERT and AISA for users to consult. The core of the document relates to recommended actions for ISPs to help prevent malicious activity, in particular, botnets. The recommendations for ISPs draws on many guiding principles in the Comcast information-draft before the Internet Engineering Task Force (IETF) as well as many best practice principles in the ITU botnet policy documents. However, the IIA E-Security Code significantly departs from both the Comcast and ITU documents in that a detailed discussion of issues and ramifications of recommendations is absent.

The IIA E-Security Code provides guidance to ISPs in order to perform four functions. They are:

(a) Detect malicious activity on a customer’s compromised computer;
(b) Take steps to respond to the AISI reports or any other source of information that may relate to malicious activity;
(c) Inform a customer on what actions they can take to protect their computers from malicious activity; and
(d) Notify Australian authorities of a malicious activity without prejudice.

No agreement has yet been made amongst stakeholders as to what modifications, if any, will be made to the Internet Industry Code of Practice in order to achieve the objectives.

LIMITATIONS AND SCOPE OF BOT REMOVAL

The techniques described in this chapter are not absolute in their effectiveness. Bot removal may be beyond the ability of many users. This will increasingly be the case as users move to integrated platforms such as iPhones and tablets accompanied with the ability to migrate to a more sophisticated interface as the result of the National Broadband Network (NBN). It may be the case that bot removal requires specialized knowledge and skills. The reality is that attempts to remove bots may prove unsuccessful or only partially successful. Comcast states that “the only way a user can be sure they have removed some of today’s increasingly sophisticated malware is by ‘nuking-and-paving’ the system: reformatting the drive, reinstalling the operating system and applications (including all patches) from scratch, and then restoring user files from a clean backup”. ISPs who have used bot remediation programs, such as Comcast in the United States, Rogers in Canada and Australian ISPs participating in AISI have not published any statistics on the effectiveness of bot remediation programs.

Comcast notes that bot remediation programs “may leave a user’s system in an unstable and unsatisfactory state or even in a state where it is still infected [and] ... attempts at bot removal can also result in side effects ranging from a loss of data or other files, all the way through partial or complete loss of system usability.” Again, the effectiveness of such bot remediation programs should be analysed against any damages and side-effects of a program. Currently the IIA Code does not provide for review of the program in order to ensure its effectiveness.
Recidivism refers to the recurrence of infection in a remedied machine. Compromised machines are cleaned and basically re-infected. According to the ITU, the Internet Architecture Board considered the issue at a workshop on “Unwanted Internet Traffic”. The IETF noted that notifications by ISPs would likely have a limited impact on user’s remedying their machines. Users might ignore the notification, or clean their machine only to become re-infected within a short period of time.

Notification where coupled with a mechanism designed to illicit expedient customer action such as speed throttling, walled gardens, and suspension of services and ultimately, termination of services where machines are unremedied, will prove more effective than mere notification with a link to how to clean up a machine. It is possible that machines will become re-infected once cleaned up. By installing anti-virus software and software to update routers and operating systems, the likelihood of re-infection is reduced significantly. One must remember that ISP involvement will be infinitely more effective with an overall cyber strategy where multiple-enablers, along with law enforcement agencies are involved. Changes, for example, to domain name resolving, along with changes to law enforcement, and additional regulatory changes to financial enablers will form an overall cyber strategy that may positively affect botnet proliferation, and the commercial malware industry in general. These areas are not, however, fall outside of the scope of this article.

THE EVOLVING LIABILITY STRUCTURE FOR ISPs

As a cultural phenomenon, the Internet has been strongly associated with freedom of communication. Since their inception in the early 1990s, ISPs have not been required to police the content their users place upon the Internet in the same way as for traditional telecommunications switching providers. At the same time, ISPs are in an unrivalled position to suppress content held on their systems by removing access to resources – web space, connectivity, file access permissions, and so on – from their customers. The ISP is often the only entity that can identify customers in the real world, and so they must necessarily become involved before the true originator can be held accountable for the presence of unlawful content.

Hence many content removal regimes make ISPs liable for content once they have been informed of its existence. If they fail to ‘take-down’ the material then sanctions against them may then proceed. This gives rise to various complexities because the ISP, and the network professionals working for them, may be constrained by data protection legislation, by professional codes of practice or ethics, or by common law notions of confidentiality, from disclosing the information haphazardly. ISPs, intermediaries and network professionals are also reluctant to be drawn into acting as a plaintiffs’ agent against their own individual or business customers – and at the very least demand recompense for their efforts, along with immunities when errors are made.

While potential liability proves as a disincentive in many respects, the role of ISPs is shifting to that of a vital intermediary to collect and broker information to law enforcement and other parties. ISPs are being asked to censor in an indirect way. As Clarke describes it, “It’s not ‘censor’: it is ‘monitor, contact, report/disconnect’”, whereby ISPs are certifying whether a computer is ‘fit for connection to the Internet’.

This can be seen in a number of contexts outside of Internet security. ISPs, for example, are required by law to takedown materials that violate copyright law once they have been notified of the infringing content if certain conditions have been met. Defamatory material and other types of offensive material must likewise be taken down within a reasonable timeframe once an ISP is notified. Clause 91 of Schedule 5 of the Broadcasting Services Act 1992 (Cth) shield ISPs and Internet Content Hosts (ICHs) from liability for carrying or hosting offensive third party Internet content where they were not aware of the nature of the content. Once an ISP becomes aware of the nature of content, they must act expeditiously to remove such content. Recent 2010 amendments to the Telecommunications (Interception and Access) Act 1979, remove much of the ambiguity of ISPs ability to actively monitor, collect data, and
protect their networks. The liability, however, is not absolute. ISPs must still comply with privacy law, telecommunications law and the contractual provisions in any terms of service agreements.

The recent amendments to the *Telecommunications (Interception and Access) Amending Act 2010* allow ISPs to detect and monitor their network for security and protection purposes without invoking the obligations of warrants, and interception of communications. The Explanatory Memoranda (EM) of the 2009 bill succinctly summarises the main points of the recent amendment to the TIA. The main points of the EM are provided below:

The amendments contained in the Bill will:

- enable all owners and operators of computer networks to undertake activities to operate, maintain and protect their networks
- enable Commonwealth agencies, security authorities and eligible State authorities to ensure that their computer network is appropriately used by employees, office holders or contractors of the agency or authority
- limit disclosure of secondary use and disclosure of network protection activities to:
  a. network protection activities
  b. undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network, and
  c. reporting illegal behaviour that attracts a minimum of three years’ imprisonment penalty threshold to the relevant authorities
- require the destruction of records obtained by undertaking network protection activities when the information is no longer required for those purposes.

The 2010 amending act sets out a concrete definition of network protection duties, establishes who is entitled to perform such duties, sets limits to third party disclosure, and places limits and penalties against unlawful use of the data collected by government agencies. The 2010 amendments to the TIA define ‘network protection duties’ as “in relation to a computer network, means duties relating to:

- the operation, protection or maintenance of the network; or
- if the network is operated by, or on behalf of, a Commonwealth agency, security authority or eligible authority of a State – ensuring that the network is appropriately used by employees, office holders or contractors of the agency or authority.

Network protection duties specifically includes the right to intercept communications with the exception of voice communications. Interception of communications must be performed by an authorised person of a computer network.

Authorised person in this context has two meanings. The amendments establish that a responsible person for the network must be designated, and that any other person performing interception of communications must have authorisation from the responsible person in writing. Further restrictions are then placed on disclosure of the content of the intercepted communication to third parties. An ISP may elect to disclose to “an officer of an agency” any content of an intercepted communication whether there is reason to believe that a prescribed offence has been committed. “Officer of an agency” is not defined in the legislation.

Under the TIA, ‘agency’ means interception agency or another enforcement agency where these two terms essentially refer to similar agencies that are able to obtain interception warrants such as the Australian Federal Police, ACMA and so forth. It remains unclear whether the restriction to disclose information is limited to officers of an agency, and therefore sharing of any list of IP addresses connected to bots with other ISPs would violate
this provision. It appears that an ISP could disclose the information to ACMA who could then relay the information to other ISPs providing there was reason to believe that a prescribed offence had been committed. The direct disclosure bot information retrieved from interception of communications to other ISPs remains legally ambiguous under the 2010 amendments.

The Amendments, however, do not address liability for a situation where ISPs have disconnected users from the Internet under the bot remediation program. Where ISPs take action against customers who have been identified as having a compromised machine, and/or have been identified as a source of a cyber-attack, the ISP is exposed to liability. The customer may initiate civil court action for wrongful disconnection. Telstra made a submission to the Inquiry Into Cybercrime calling for ISP immunity. Specifically, the Telstra document asks the government to:

"Provide legislative protection for a carrier or Internet Service Provider (ISP) from third party claims when it undertakes activities, in good faith (or as agreed with government and/or industry), to protect their networks and services and customers from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or the States or Territories. (This would be similar to the protection given under section 313(5) of the Telecommunications Act 1997)."

This seems like a reasonable request given that telecommunications carriers are being asked to actively monitor and remedy insecure computers, and thus may be seem to be making content determinations. There have been a number of vexatious civil actions taken against security software vendors for blacklisting websites.

Anti-spyware, anti-virus and anti-spam organisations have found themselves exposed to legal challenges. Spamhaus Project, an organisation of volunteers in the computer industry, composes blacklists of some of the worst spam propagators to aid ISPs and businesses to better filter spam. The company E360insight.com sued Spamhaus Project in the Northern District of Illinois Federal Court alleging it was a legally operating direct marketing company and should not be blacklisted as a spam provider. Spamhaus did not file a response and did not appear before the court. As such, the arguments presented before the court were unilateral such that the court issued a default judgment. It should be noted that the ruling did not consider the merits of the case because no defence was mounted.

The court ordered Spamhaus to pay $11.7 million USD, to post a notice that E360 was not a spammer, and ordered that the Spamhaus Internet address be removed from the Internet Corporation for Assigned Names and Numbers (ICANN). Spamhaus ignored the ruling, did not pay the money, did not post a notice on its website that E360 was not a spammer, nor did ICANN remove the Spamhaus website from its root server. In a similar situation, the anti-virus and anti-spyware company Symantec was taken to court in California by a company which it defines and reports in its services as spyware. Hotbar.com claims that the classification of its software as spyware is in violation of trade libel, and constitutes interference with contract. The suit was reported as settled with Symantec agreeing to classify Hotbar as ‘low risk’. A series of cases of a similar nature have been filed and heard between 2005 and 2009, with most settling.

The notion of “good faith” or its equivalent will be imperative to ensure that ISPs do not abuse this power. The Canadian case of Telus is a good example. Telus, a major telecommunications carrier, was in a labour dispute with its employees where there was a lengthy strike. Telus blocked a pro-union website during the strike. There are also instances where large security vendors blacklist websites that point out vulnerabilities of their products by categorising such sites as “pornography”. These websites, that have nothing to do with pornography, are then blocked from those users who use the vendor’s products. The vendor’s filtering products might also be used at the ISP level or on the backbone of a nation with a heavy filtering mandate.
CONCLUDING REMARKS

Entities that enable malware actors are a critical component to cyber security. This article has looked at the role of ISPs as a connectivity enabler. Bot remediation programs are imperative in cleaning up infected machines. Takedown of a botnet through other methods does not remove the very real and significant problem that compromised machines remain infected, and therefore, ready to be taken over by another botnet herder or ready to receive instructions in a different manner such as through peer to peer or through Google search queries. Disinfecting bots is an imperative element of any long-term solution to botnets.

The recommendations put forth by Comcast are well thought out and should be considered further by the IIA. Comcast argues that detection and monitoring technologies be restricted to small and medium packet inspection – that which is already being used, and that such technologies not be used for surveillance of individuals unless in the lawful cooperation with an criminal investigation. Detection and monitoring methods should adhere to several principles. Privacy principles and protection of personal information should be maintained. Passive monitoring methods should be use as opposed to pervasive methods such as deep packet inspection. Methods should be non-disruptive and should not block legitimate traffic. Multiple Point Bot Detection data points should be used to minimize false-positive identification of computers. ISPs should err on the side of caution when a likely bot infection has taken place, and should notify a customer even in the event of a benign or dormant botnet. Time-sensitive detection methods are imperative.

ISPs should not be expected to shift their role to an active filter or intermediary without liability exemption. As seen in the 2010 amendments to the Telecommunications (Interception and Access) Act, Australian ISPs may legally perform content inspection in connection with network protection. This ability to perform content inspection does not equate to an exemption from liability where a customer has been wrongfully disconnected. Any liability exemption should, however, contain a good faith clause so that ISPs do not use their position in an abusive manner.

Function creep remains a concern with Australia’s shift to use intermediaries for network protection. If ISPs are actively monitoring their systems for malware, there is no reason to think that they may be asked in the future to monitor their systems for copyright infringement, counterfeit goods, and possibly even defamatory materials.

Finally, it is recommended that the proposed e-Security Code be reviewed after a year of implementation. This review should outline the Code’s objectives, unforeseen impacts, and should produce statistics where outcomes are measures against objectives. Such a review should include statistics on what portion of computers were detected as compromised? What portion of detected computers were remedied after ISP notified the customer? Rates of recidivism should be detailed along with recommendations to improve the process. Reviews of the program will additionally allow ISPs to constantly improve bot remediation.

BIBLIOGRAPHY:

LEGISLATION:

Broadcasting Services Act 1992 (Cth)
Communications Legislation Amendment (Content Services) Act 2007 (Cth)
Copyright Act 1968 (Cth)
Spam Act 2003 (Cth)
Telecommunications Act 1997 (Cth)
Telecommunications Interception and Access Act 1979 (Cth)
Telecommunications (Interception and Access) Amendment Act 2010 (Cth)

**LITIGATION:**

1-800 CONTACTS, INC. v. WhenU. com, Inc., 414 F. 3d 400 - Court of Appeals, 2nd Circuit 2005

180 Solutions v. Zone Labs, 2:2005cv02025, Washington Western District Court 2005 (180 Solutions dropped the suit shortly after commencement of proceedings)

Cassava (Casino On Net) v Sunbelt Software, (settled before trial) December 2005


Roadshow Films Pty Ltd v iiNet Limited (No. 2) [2009] FCA 1391 (26 November 2009)

Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24 (4 February 2010)

University of New South Wales v Moorhouse [1975] 133 CLR 1. (1 August 1975)

**JOURNAL ARTICLES:**


**GOVERNMENT REPORTS AND POLICY DOCUMENTS:**


PRESENTATIONS:


BOOKS:


ONLINE ARTICLES:


ENDNOTES

1 Internet Industry Association, Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security (September 2009).


3 According to Clarke, R., bots and botnets are explained as: “Generally, a program that operates as an agent for a user or another program. More specifically: software that is capable of being invoked remotely in order to perform a particular function. Typical functions include emailing spam or repetitively sending messages to a target device in order to overload it and thereby deny service; but also despatch of meta-data for files held on the device. A device on which a bot is installed is called a zombie. A set of devices on which bots are installed is called a botnet. Generally intended for largely automated operation, but under the control of a person who may be called a botnet master or botnet herder.” Clarke, R. Malware Glossary, available at http://www.rogerclarke.com/II/MalCat-0909.html (last accessed March 8, 2010).

4 The Mariposa Botnet is said to have had 13 million zombies. See Finkel, J. of Wired Magazine “Spain Busts Hackers for Infecting 13 Million PCs” (March 2, 2010) available at http://www.wired.com/threatlevel/2010/03/spain-busts-hackers-for-infecting-13-million-pcs/ (last accessed April 21, 2010).


7 Vincent Cerf in many ways is “Father Internet”. This is not surprising given that he was involved in the original ARPANET project, was Chair of ICANN, has worked at a number of internationally reputed universities, and has held key positions at IBM and Google. He is considered to be one of the most influential researchers in computer science and the Internet.
8 Presentation given at the World Economic Forum 2007. The statistics have been highlighted in a number of news reports and blog sites. See, for example, Anderson, N. “Vint Cerf: one quarter of all computers part of a botnet” (January 25, 2007) Ars Technica available at http://www.arstechnica.com/news.ars/post/20070125-8707.html.


14 The Cyberspace Law and Policy Centre (Lauren Loz and Alana Maurushat) mapped out the various list of registrars and resellers relevant to the .au including contractual agreements between the various resellers and registrars with ICANN and the .auDA. This table is included in Appendix 7(A) at the end of the chapter.

15 The term ‘security researchers’ is used broadly here. This may include security organisations, security experts, individual researchers, security companies or simply hacker activists.

16 I-defense, for example, documents several holding companies in Hong Kong as being used to register many Internet web pages, IP addresses etc. for organised crime. See Jellenc, E. and Zenz, K. Global Threat Research Report: Russia (2007) available at http://versign.com/static.042139.pdf (last accessed April 20, 2010).

17 Section 324 of the Telecommunications Act requires carriage service providers (which includes ISPs) to be able to intercept a communications passing over the network or facility in accordance with a valid warrant under the Telecommunications Interception Act.

18 See sections 474 generally of the Criminal Code (Cth).


26 Telecommunications Act 1997 (Cth). See section 533 Inspectors.


28 Telecommunications Act 1997 (Cth). Divisions 5 and 5A, sections 547-547H.

29 Telecommunications Act 1997 (Cth). Section 547J.


31 ITU Botnet Mitigation Toolkit: Background Information (January 2008).

32 Broadcasting Service Act 1992 (Cth), Schedule 7(BSA).

33 Reference to industry codes and standards is made in Part 4 Industry Codes and Industry Standards in Schedule 7 of the BSA. Additional reference to industry codes and standards may be found in Part 6 Industry Code and Standards in the Telecommunications Act 1997 (Cth).

34 Schedule 7 of the BSA was introduced in the Communications Legislation Amendment (Content Services) Act 2007 (the ‘CSA’), which came into effect on 20 January 2008.


36 According to Jeremy Malcom, “the IETF, as the body responsible for the development of a large majority of such standards, it is unquestionably the Internet’s pre-eminent standards development body.” Malcom, J. Multi-Stakeholder Governance and the Internet Governance Forum (Terminus Press 2008) page 51.

37 Comcast, note 31 above.

38 Comcast, note 31 above, page 7.


42 Clarke, R. Comments made in the Link-ed list serve, February 2010.

43 Service providers were found liable for secondary copyright infringement in the seminal case of University of New South Wales v Moorhouse [1975] 133 CLR 1. Since this 1975 High Court of Australia decision the Copyright Act 1968 was amended following the signing of the United States and Australia Free Trade Agreement. ISPs now have a safe
harbour where they are compliant with a series of requirements related to notice and takedown of infringing material. The shielding parameters of the safe harbour provision were fortified in the recent iiNet decision. See Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24 (4 February 2010), Roadshow Films Pty Ltd v iiNet Limited [2009] FCA 332 (15 April 2009) and Roadshow Films Pty Ltd v iiNet Limited (No. 2) [2009] FCA 1391 (26 November 2009), and Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16 (20 April 2012)

An “Internet content host” is defined under the Broadcasting Services Act 1992 (Cth) as a person who hosts or proposes to host Internet content in Australia. ICHs would include bulletin board hosts, blogs, email companies and so forth. They are contrasted with ISPs who are defined under clause 8 of Schedule 5 as “a person who supplies or proposes to supply an Internet carriage service to the public.”

TIA Amending Act 2010, section 7(3) excludes voice communications such as VOIP and SKYPE.

TIA Amending Act 2010, section 7(2).

TIA Amending Act 2010, section 63E.

TIA, Interpretation section.


1-800 Contacts v WhenU., 1-800 Solutions v. Zone Labs, Cassav (CasinoOnNet) v Sunbelt Software, Claria (Gator) v Internet Advertising Bureau.

This article explores the domestication of mobile technologies by women and how their traditionally slow adoption of new technologies is being mirrored through their adoption of smart-phone applications. Building on existing gender and mobile communications literature, this paper provides a needed overview of how women are strategically deploying the use of 'apps' on their smart phones in both 'fun' and 'useful' ways.

Two groups are analysed in this article. The first comprises women who only use a single Internet connection, identified as 'single connectors'. This group is contrasted with a second group who use multiple Internet connections, identified as 'triple connectors'. In this article we playfully name the social seeking Triple Connectors Social Consumers and the Mobile Internet Single Connectors have been identified as Information Seeking Consumers. 'Social networking' was identified as a 'fun' app rather than a 'useful' app by both groups of female connectors: what does this say about women and their definitions of leisure? Are women still viewing networking as part of their commitment to emotional labour rather than something that is 'useful'?

INTRODUCTION

Australians have a growing appetite for apps that enable them to perform a range of tasks from mobile banking through to selecting a restaurant (AIMIA 2010, 86). Worldwide, 60% of smart-phone users download an app every month, paying on average $4.00 to do so (Fraser 2011). Convergent devices such as smart-phones provide busy Australians with the opportunity for immediate communication through voice or data. While voice is seen as essential for intimate contact with loved ones (Licoppe 2004, Lloyd 2010) it is Internet data services that continue to drive growth in the take-up of mobile services rather than voice (ACMA 2011, 19). Initially, interest was piqued with telephony data in the form of short message service (SMS) and multimedia message service (MMS) (Goggin 2006). Australian uptake of texting grew unexpectedly fast providing telecommunications providers with 'continual growth' (ACMA 2010, 50) and the recognition that possible future data services could outstrip voice sales. The sending or receiving of SMS messages remains the most popular non-voice activity (84% received and 83% sent) in 2011 (ACMA 2011, 42). Smart-phones offer end users the enticing combination of voice and Internet data, so enabling communication, information seeking and transactions in the one converged device. Australians are increasing their transactions through their phones; PayPal Australia reports that throughout 2010 mobile transactions increased by 25% every month (Moses 2011). As part of this shift to mobile usage Ryan Hayward, Google's mobile product marketing manager for the Asian-Pacific region states that 'mobile usage and smart-phone usage (is) starting to
approach or even match PC usage…we found that Google Maps…usage on the mobile phone has already exceeded the desktop globally’ (Moses 2011).

The 2010 AIMIA report confirmed 'Australians' increasing consumption of data via their smart-phones. AIMIA noted an increase in those that had data included in their payment plan, up 16% from 2009, as well as an increase in the amount of data included in plans (Mackay 2010, 4). There was a 19% increase in the more than 50MB category and a spike in the 251-500MB category from 6% to 19% (Mackay 2010).

While women are often seen as the later adopters of technology to men, when women do adopt technology it is usually for social rather than business or professional purposes. This can be seen in a range of technologies from Fischers' (1988) seminal investigations with the telephone in the 1980s, which uncovered that historically women used the telephone for social connectedness, while men used it for business through to even earlier explorations with long distance telegraphy (Sterne 2003). With these findings in mind it might be extrapolated that women might prefer applications or 'apps' as they are known, for their phones that enabled greater communication through the multiple methods currently available: text, voice, and video.

RELEVANT LITERATURE

AUSTRALIANS' USE OF APPS

Currently 12% of product share of online retail sales in Australia is attributable to software and apps (ACMA 2011b, 10). In relation to fun apps in AIMIA's results for 2010 '66% stated that they used an entertainment or information service' during the last twelve months, and '48% of all respondents used games' (Mackay 2010, 6). These figures do not include Mobile Internet specific data downloads. Only 31% of AIMIA's respondents use Mobile Internet to access entertainment services and content (Mackay 2010, 7). However while there are hundreds of thousands of apps to download and use on smart phones and tablets (Fraser 2011), there is little investigation into actual end user preferences for apps. Total downloads of apps is a commonly used measure; however it does not reflect consumer preferences for the app once they have begun to use it. It is possible that after downloading an app a consumer becomes dissatisfied with the product and they may even delete it from their device. This paper investigates consumer preferences for self-defined fun and useful apps.

WOMEN ADOPT AND DOMESTICATE TECHNOLOGIES SLOWLY

The pattern of women adopting technology slower than men has been seen over time with technologies such as the telephone, computers, the Internet, and mobile phones (Ewing & Thomas 2010; Wajcman et al. 2008). In Australia, the female adoption rate for the Internet in 2007 was 71% increasing to 80% in 2009 (Ewing & Thomas 2010, 2). The average time online shows the most dramatic difference between the genders. In 2009 male users had on average been online longer than female users by around four months (Ewing & Thomas 2010, 6). In 2007 the gap was around 16 months (Ewing & Thomas 2010). This is a dramatic increase of female use of the Internet since the previous World Internet Project (WIP) survey in 2007. This shows that Australian women's adoption rate of the Internet when compared to that of Australian men is slow. This adoption trajectory can be seen in relation to the major technology developments over the last few decades including the mobile phone (Ewing & Thomas 2010, Wajcman et al. 2008).

As women adopt technologies, two key differences emerge; women are seen to use technology in different ways and consumerisation occurs. Supriya Singh contends that 'as a technology becomes domesticated and feminised, gender differences are seen in the use of the technology rather than access' (Singh 2001, 396). Again this applies across all technologies. Early studies reported that men view the telephone primarily as a business tool (Fischer 1988,
Wajcman et al. 2008) and women use it to maintain social contact (Fischer 1988; Lohan 2001; Wajcman et al. 2008).

**WOMEN AS NETWORKERS AND 'SOCIAL CONSUMERS'**

The use of technology for maintaining social bonds by Australian women can also be seen through their use of web 2.0 platforms. Australian women are frequent users of social networking sites (SNS) specifically Facebook, LinkedIn, Twitter and MySpace (Sensis 2011, 10), enabling them to maintain their image as being socially connected or for the purposes of this paper to act as Social Consumers. Reportedly the predominant use of SNS by Australian females is to 'catch up with friends and family' (96%) (Sensis 2011, 19). According to the Sensis survey the majority of females using these sites are young women 14-39 who are most likely to visit the sites daily (Sensis 2011, 10). Older women 30+ are less frequent users of the sites and some never visit (ibid). Facebook is still the dominant SNS for Australians with 99% of their Australian female participants using the site (Sensis 2011, 13).

Significantly for the purposes of this paper the devices being used to access social media are changing. Currently the device most used to access social media and to connect with friends and contacts is a laptop computer (Sensis 2011, 17). A laptop computer is the device most used among all age groups to access social media. However, smartphone access is slowly catching up, with 31% of all females using a smart-phone to access social media (Sensis 2011, 17). This percentage increases to 52% in the 14-19 age group (Sensis 2011, 17).

Part of the rationale for women to use social media and to act as 'Social Consumers' is their persistent role as emotional caregivers within the context of family and friends. In telephony studies Wajcman has reported that among Australians the highest calls made are between spouses (18%), and by women to their children (13%), parents (11%), and extended family (12%) (Wajcman et al. 2008, 18). Wajcman also reports that with texting, family (47%), and friends (43%) are the highest recipients of text messages (Wajcman et al. 2008, 19). Supporting this work is the recent Pew Internet report, which reveals that Americans are using SNS to keep in contact with close ties (Smith 2011). American ‘women are slightly more likely than men to say that staying in touch with current friends is a major reason for using online social tools (70% vs. 63%)’ (Smith 2011, 4). For an older age group such as those of middle age or older, ‘female social media users are more likely than male users to cite family connections as a major reason for using these [social networking] sites (72% vs. 55%)’ (Smith 2011, 4).

'THE FRONTIER HAS BEEN TAMED' (Consalvo 2002, 132)

The diffusion of the Internet among greater numbers of people made it mainstream. Becoming mainstream means ‘the Internet often operates on a naturalised gender difference’ (Paasonen 2002, 29). This has meant that websites and other online services are now targeted towards women, and they ‘rarely promote deconstructive approaches to gender with their horoscopes and tips on relationships, home and food’ (Paasonen 2002, 29). Consalvo's own research has detected that in the mid to late 1990s there was a push towards consumption and commodification, when businesses began to refine the idea that individuals could buy products online (Consalvo 2002, 131). When women began to adopt the Internet in greater numbers they became viewed as potential consumers and as an audience for online advertising (Consalvo & Paasonen 2002, 8). Consalvo contends that,

‘it is no accident that commerce has arrived in tandem with women. Women are an important demographic for marketers, and the Internet during this period has become more of a place for selling than for exploring or creating’ (Consalvo 2002, 133).

When women went online the same discourses repeated in line with previous technologies. Women are now perceived and discussed in their traditional roles as social networkers as avid users of social networking sites (Sensis 2011), of e-Reading (Nielsen 2011) and now in the
US a PEW report indicates that women especially older women are downloading more apps to tablets than men (Purcell 2011, 3).

In 2010 Ewing and Thomas revealed that 88% of Australians currently use the Internet for product research prior to purchase (2010, 44), and more recently an ACMA report, *e-commerce marketplace in Australia: Online shopping* revealed that the 'majority of Internet users are online shoppers' in Australia (ACMA 2011, 1).

Indeed Australian women are well poised as potential consumers. Of the 4% of the Australian population who make purchases using a mobile phone 43% are women (ACMA 2011, 20). In keeping with their femininity (Paasonen 2002, 30) Australian women are shopping online for clothing/fashion and it is the highest product search conducted through social networking sites (Sensis 2011, 20).

**ABOUT THE STUDY**

This paper draws on data compiled from a larger study, *Discovering Connectors: A Guide to The Australian Wireless End User* (Rickard 2010), that investigates the ways in which Australian end users are adopting wireless broadband for individual use. The study is based on end user perspectives and explores the possibility that Australians are moving towards a sense of multimodal connectedness (Schroeder 2010) by using an increasing number of devices and forms of wireless connectivity. For many Australian end users wireless Internet connectivity takes the form of Mobile Broadband, Mobile Internet and WiFi, where Mobile Broadband is understood as using a USB 'dongle' or datacard in computers to connect to the Internet, mobile Internet as using a mobile phone or iPad/Tablet to connect to the Internet (3G), and WiFi as a fixed form of connectivity made available wirelessly, in public spaces like cafes, airports, libraries, and places of study. The data for the study was collected using an online questionnaire circulated in 2010. The research method applied involved collecting data through an online questionnaire, then the data was analysed using SPSS.

**PARTICIPANT RECRUITMENT**

Participants were recruited via email using networks which included industry and universities, and online advertisements on the University of the Third Age website and Australian Policy Online. An email was circulated through the networks mentioned above which included details about the project and how to participate. Respondent recruitment relied on the email snowballing through those networks. Participation in the online questionnaire was voluntary, and no incentives were offered for participation. The criteria for participation were deliberately broad. Participants needed to be at least 18 years of age and Australian residents. The questionnaire took approximately 15 minutes to complete; however times varied depending on the number of different forms of connectivity and devices used by respondents. Data was collected using Opinio software over a three-month period from June to August 2010.

172 participants aged between 18 and 69 answered the online questionnaire. Compared with the results reported in Australian studies such as those conducted by AIMIA (Mackay 2010, 2011) and the World Internet Project (Ewing and Thomas 2010) this study attracted only a small number of respondents. As a result of the small number of respondents, the conclusions drawn in this paper can only be indicative of adoption and usage practice in Australia. Respondents were residents of New South Wales (38.8%), Victoria (35.9%), Queensland (14.7%), Western Australia (4.1%), Australian Capital Territory (3.5%), South Australia (2.4%) and Tasmania (0.6%). The female respondents comprised 92 females aged between 18 and 63. The male respondents comprised 82 males aged between 22 and 69.
QUESTIONNAIRE STRUCTURE AND CONTEXT FOR THIS PAPER

There were three sections to the questionnaire.

1. In the first section, participants were presented with a number of demographic questions relating to their age, living arrangements, marital status and employment status. No socio-economic questions were asked regarding income levels or education. Likewise the study was not structured to analyse the ways in which apps are used according to a range of other possible demographic characteristics. Hence participants were not asked questions relating to their ethnicity, language/s used, or disability and socio-economic status.

2. Following the first section, participants were asked a number of general questions about their use of communication technologies, such as 'How do you make telephone calls at home?' and 'Who pays for your internet connection at home?'

3. After this initial set of questions participants were required to indicate which type of internet connection they used when away from home and depending on their selection participants were sent down various paths of the questionnaire relating to their choice of wireless connectivity. If the participant did not use wireless connectivity they then exited the questionnaire.

Most of the questions in the online questionnaire presented the participants with multiple choices although there was an open comments box on each question for participants to contribute additional comments as they felt appropriate.

The context for this paper is two questions posed to participants who stated that they connect to the Internet using a mobile phone.

In Question 23 of the questionnaire participants were asked 'Which three phone apps do you find the most fun?'. Participants then entered their responses into a free text field. The following Question 24 asked respondents to enter into another free text field their responses to 'Which three phone apps do you find the most useful?'. The question was expressed this way to ensure that we recorded respondent preferences according to genre and delineated from what they downloaded and did not use.

The terms fun and useful are therefore subjective to the respondents and yet provide a form of measurement for the purposes of this paper. In total there were 52 fun app responses and 71 useful app responses.

THE CONNECTOR TYPES

Identified in the main report Discovering Connectors (Rickard 2010) were three discrete groups: Single Connectors, Twin Connectors and Triple Connectors. The Triple Connectors connect to the Internet using three types of wireless broadband: Mobile Broadband, Mobile Internet, and public Wi-Fi. The other two groups, 'Single Connectors' use one type of wireless broadband, and 'Twin Connectors' a combination of two.

In the main report the make up of the connector groups are:
This paper focuses on the results and discussion in relation to the responses of only two of these connector groups: the Triple Connectors and the Single Connector group 'Mobile Internet'.

**PROFILING THE TRIPLE CONNECTORS**

The Triple Connectors are the respondents who connect to the Internet using all three forms of wireless broadband: Mobile Broadband, Mobile Internet and WiFi. The Triple Connectors are the largest single group identified by the study, and make up 25.6% or 44 of all the respondents. The gender breakup is 15 females between 18 and 50 years of age and 29 males between 27 and 66 years of age.

### Triple Connector Marital Status (male and female respondents)

<table>
<thead>
<tr>
<th>Marital Status</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>25%</td>
</tr>
<tr>
<td>Married and living with children</td>
<td>34.1%</td>
</tr>
<tr>
<td>In a relationship with no children</td>
<td>13.6%</td>
</tr>
<tr>
<td>Married with children, but none living at home</td>
<td>11.4%</td>
</tr>
<tr>
<td>Married with no children</td>
<td>9.1%</td>
</tr>
<tr>
<td>Single with children but none living at home</td>
<td>2.3%</td>
</tr>
<tr>
<td>In a relationship with children but none living at home</td>
<td>2.3%</td>
</tr>
</tbody>
</table>

### Triple Connector Employment Status

<table>
<thead>
<tr>
<th>Employment Status</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full time employed</td>
<td>65.9%</td>
</tr>
<tr>
<td>Full time students</td>
<td>22.7%</td>
</tr>
<tr>
<td>Employed part-time or casually</td>
<td>15.9%</td>
</tr>
<tr>
<td>Stay at home parent</td>
<td>2.3%</td>
</tr>
<tr>
<td>Retired</td>
<td>No responses</td>
</tr>
<tr>
<td>Unemployed</td>
<td>No responses</td>
</tr>
</tbody>
</table>
**Profiling the Mobile Internet Single Connectors**

The Mobile Internet Single Connectors make up 15.1% or 26 of all the questionnaire respondents aged between 18 and 60 years of age\(^2\). Of these, nine are males aged between 23 and 60 years and 17 are females between 18 and 45 years of age.

<table>
<thead>
<tr>
<th>Mobile Internet Single Connectors Marital Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>42.3%</td>
</tr>
<tr>
<td>Married and living with children</td>
<td>30.8%</td>
</tr>
<tr>
<td>In a relationship with no children</td>
<td>19.2%</td>
</tr>
<tr>
<td>Married with no children</td>
<td>7.7%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile Internet Single Connectors Employment Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Full time</td>
<td>46.2%</td>
</tr>
<tr>
<td>Full-time students</td>
<td>34.6%</td>
</tr>
<tr>
<td>Part-time or casually employed</td>
<td>26.9%</td>
</tr>
</tbody>
</table>

**Social Consumers and Information Seeking Consumers**

Figure 1 below indicates the genre of apps preferred by the respondents. When the fun and useful apps are contrasted against each other the most popular apps by genre are social networking, weather, communication and navigation.
Figure 1 - Fun and Useful apps comparison

There is also a wider range of useful apps (19) to those that are considered fun (8) by respondents.

When the results of the Triple Connectors are contrasted with those of the Single Connectors they indicate two possible consumer groups: 'information seeking' and 'social'. The connectors who selected more apps of a genre considered to be seeking or looking up information are called 'information seeking consumers' and those connectors whose app selections reflected a greater range of social needs are called 'social consumers'.

In this next section of the paper the apps are organised according to whether they are fun or useful, and contrasted against whether they are being used by information seeking or social consumers. The data presented in the figures also reveals the gender preferences by app.
In Figure 2, 58.6% of male and 40% of females use fun apps. The male social consumers use a wider range of fun apps than the females.

In Figure 3, 79.3% of males and 46% of female Social Consumers use fun apps. In these results the men use a greater range of genres than women.
In Figure 4, 88.9% of male and 64.7% of female Information Seeking Consumers use fun apps on their phone. It can also be seen that the females use a wider range of apps in this category although the males use a greater number in concentrated genres overall. It is also apparent that the women, in greater numbers to the men, consider social networking a useful app.

In Figure 5, 88.9% of male and 70.6% of female Information Seeking Consumers prefer the above categories of useful apps on their phones. It is also clear from Figure 6 that among this group the females use a wider range of apps than the males.
DISCUSSION

The results indicate that Information Seeking Consumers prefer more 'useful' apps than the Social Consumers. The respondent data shows that our Information Seeking Consumers prefer the most apps overall when compared to those used by the Social Consumers.

The types of apps downloaded by both the Social Consumers and the Information Seeking Consumers were consistent with those recorded by AIMIA in the 2010 reporting period (Mackay 2010, 9). AIMIA respondents downloaded and installed games, maps and navigation, news, weather, instant messaging, social networking, photos and search applications (Mackay 2010).

As discussed earlier, women are slower to domesticate new technologies and services. There's a clear alignment between offline services such as newspapers, magazines and books migrating across into the app market. The uptake for these particular services has held wide appeal for women; older women in particular have adopted e-Readers and tablets such as the iPad. Sensis reports that 6% of Australian women reported using iPads or another tablet to access social media (Sensis 2011, 17).

Women's slow uptake of yet another form of technology – apps is also clear here in the results between the males and the females participating in the study. In all categories the female participants lag behind the males in app uptake. The greatest difference is between the social consumers – 79.3% of male Social Consumers download 'useful' apps whereas only 46.7% of female Social Consumers do, providing a remarkable difference of 32.6%.

Another point of differentiation is between the spread of apps used. The situation differs between the Social Consumers and the Information Seeking Consumers. Among the Social Consumers the males download and prefer a wider range of apps. It is the female Information Seeking Consumers who download and prefer a wider range of fun and useful apps than the Information Seeking males.

WOMEN AS SOCIAL CONSUMERS

Our results indicate that the Social Consumers are entertainment focused, enjoying games (40%), entertainment (10%) photography (28%) sport (8%), music (8%) and travel (8%) along with their expected interest in communication; social networking (20%) and communication (17%). Social Consumers are able to increase their use of social networking sites through their phones and tablets because of the development of SNS-specific apps. These shortcut apps provide easy access to the existing online platform by removing the need to navigate through a browser and the use of such apps is often supported in Australia through unlimited social networking plans by telecommunication providers such as Telstra and Optus. Unlimited plans encourage further use of these apps potentially reducing the need to use traditional services such as voice, or even SMS.

It is interesting to note that overall Social Consumers use fewer apps than Information Seeking Consumers irrespective of gender. This suggests that while Social Consumers may spend time and money on entertainment they are less likely to spend as much time online as Information Seeking Consumers, and perhaps in the long run less money.

WOMEN AS INFORMATION SEEKING CONSUMERS

A difference in the apps used by the Social Consumers as opposed to those used by Information Seeking Consumers is that apps designed to offer products and services are most likely to be standalone and not tied into an existing online platform like a SNS such as Facebook. Standalone apps designed specifically for use on phones and tablets are value added as they offer the potential to act as points of sale and Australians are interested in mobile commerce as recent figures indicate. Australian m-commerce doubled from 2% to 4% in the period from November 2009 to April 2011 (ACMA 2011, 4).
Information Seeking Consumers are more likely to spend time monitoring their interests such as they are the group of consumers who spend most of their mobile online time checking emails, weather, reading online news and magazines (Rickard 2010). Spending time online while information seeking is possibly more likely to result in a transaction or sale. Searching is one of the most popular uses of the mobile Internet and searching while instore is increasingly popular (Moses 2011).

The ability of mobile apps to act as points of sale is likely to be especially important when the take-up of apps for everyday services such as grocery shopping actions reaches mass adoption levels. While it is currently possible to create grocery shopping lists using a mobile device it is possible to purchase your shopping list using your phone with only one large Australian supermarket chain. This is a distinct disconnect for the end users wanting to complete the transaction. A future trend highlighted by developments in Internet Protocol Television (IPTV) indicates that video tagging technology will make it possible to purchase items during the broadcast of a television show by simply selecting the item and then completing the transaction (Canning 2011). The use of augmentation or augmented reality in relation to apps, such as Layar could be another future possibility.

**CONCLUSION**

The adoption and domestication of mobile technologies by women has been consistent with the uptake of previous 'new' technology. Building on previous gender, intimacy and mobile communications research, this paper offers a needed 'snapshot' of the ways women are intentionally engaging with apps on their mobile devices. It can be seen that two distinct groupings of women, the 'Social Consumers' and the 'Information Seeking Consumers' choose and use a different range of apps.

Social Consumers are women who spend time online for entertainment purposes and for communicating with friends and family whereas the Information Seeking Consumers are more likely to be searching for information and performing tasks.

It is important to note that whilst this research aligns with previous work done on gendered uses of technology, intimacy and identity, it is always possible that through the use of mobile technologies ‘gendered types of performance can be both reinforced and subverted’ (Hjorth & Kim 2004, 49). Hence whilst this article outlines the choices that women make to remain connected identities and highly social, the gendered use of technologies is not a simple matter and it is both socio-culturally and demographically nuanced.

It is also important to note in this study that women are again slow to adopt this new form of technology. The results show the slow adoption of apps by women compared with the men in the study, and the differences are not small. The minimum difference in uptake is 18.3% and the maximum 32.6%. The results indicate that significant improvement can be made in the adoption rate of apps by women. Improvement can also be made on the part of app developers who perhaps need to consider the unique differences of the female market place. Female confidence and experience with technology could also play a part in the slow adoption rate.

Since technology is now clearly enmeshed in the everyday lives of women from domestic to communication technologies (Ewing & Thomas 2010; Fischer 1988; Mackay 2010) further research is now required that investigates both qualitatively and quantitatively women's nuanced uses of apps on mobile phones. This research could focus on other possible demographic characteristics as well as compare usage across genders and cultures.
REFERENCES


Canning, S. 2011. 'Touch and it's yours while the show goes on', The Australian, November 21, p. 24.


ENDNOTES

1. M=37; SD=13.43
2. M=44.11, SD=13.54
3. M=31.92, SD=14.224
DAVID J BRENNAN
Melbourne Law School

Associate Professor David Brennan's primary fields of research and teaching are patent and copyright law, with a particular focus upon their interface with other private law regimes such as contract, property and restitution. He is a member of the Intellectual Property Committee of the Law Council of Australia and is the editor of the *Australian Intellectual Property Journal*. David is also a long-standing consultant to Screenrights – The Audio-Visual Copyright Society. In this capacity he has participated extensively in copyright law reform and in royalty-setting determinations.

d.brennan@unimelb.edu.au

MELISSA DE ZWART
Adelaide Law School, The University of Adelaide

Dr Melissa de Zwart is an Associate Professor, Adelaide Law School, and a Member of the Classification Review Board (Cth). She has published widely on matters affecting the regulation of the online environment, including copyright, virtual worlds, social networking
and contractual communities. Her current projects include a book examining the consequences of the WikiLeaks experience for the future of online communication and a multidisciplinary project considering governance of virtual worlds.

melissa.dezwart@adelaide.edu.au

LIZ FELL

Liz Fell is a freelance communications journalist, whose coverage of the telecommunications industry began in 1982 with contributions to Communications Australia and weekly broadcasts for ABC Radio Australia and ABC Radio National. She became a contributing editor of International Communications Digest, Communications Update and Hub, and a regular contributor of keynote interviews to Australian Communications and CommsWorld. At an international level, she was Australian correspondent for Television Business International and Cable and Satellite Asia, and contributed a monthly column to Asia Pacific Satellite. Since 1993, she has conducted regular interviews for the Telecommunications Journal of Australia.

She has worked as a part-time Lecturer/ Senior Lecturer in a number of Humanities/Arts faculties, including teaching Journalism and coordinating research theses for Master in Journalism students at the University of Technology Sydney. She has also reported for the Federal Government on Journalism Education in Australian Universities.

She has been the recipient of several important awards for her journalism, including the George Munster Award for Freelance Journalism in 1986. She was elected a Distinguished Fellow of the Telecommunications Society of Australia in 2003 for her notable and enduring contributions to Australian telecommunications.

felled10@gmail.com
Neil Gane is the Managing Director of the Australian Federation Against Copyright Theft (AFACT), an organization established in January 2004 by the Motion Picture Association International (MPA) to promote and protect its members’ films and television programs in Australia as well as the commercial and creative interests of the local screen communities.

After helping to start up AFACT, Neil joined the MPA’s regional office in Singapore, working as the Senior Director of Operations, Asia-Pacific and managing its programs in a number of key markets for two years. He first served the MPA as an external consultant, managing its Philippines program and successfully implementing initiatives that led to the seizure of over seven million illegal optical discs there. At the time, he was Country Manager in the Philippines at Hill & Associates, a multi-national risk consultancy firm.

In each of these roles, Neil has leveraged his broad expertise in Intellectual Property Rights, and security and risk analysis gleaned throughout his career in Asia, which began in the Royal Hong Kong Police Force, where he spent more than a decade working primarily within Special Branch. He was awarded a Commissioners Commendation for his role in the planning and implementation of security arrangements during the handover of Hong Kong’s sovereignty to China in 1997.

info@afact.com.au
Peter Gerrand has been Editor-in-Chief of the Telecommunications Journal of Australia since 1994, and Managing Editor since 2009.

He was awarded the Charles Todd Medal by ATUG in 1998 'for outstanding contributions to the telecommunications industry', an Australian Government Centenary Medal in 2003 'for outstanding service to science and technology particularly to public science policy', and Life Membership by the TSA in 2003.

Amongst career highlights, he has been an engineering executive in Telecom/Telstra, successively heading network research, network product development, planning and network strategy units (until 1993). He subsequently was appointed as Professor of Telecommunications at two universities (first RMIT and then Melbourne); and became the founding CEO of a publicly listed company (Melbourne IT: from 1996 to 2000). He developed AUSTEL’s interconnect Model as an expert consultant to the Australian telecommunications regulator in 1994-5. From 1993 to 2003 he was Chairman of the Telecommunication Society of Australia Ltd.

From 2004-2007 he carried out research at La Trobe University in the School of European and Historical Studies, and was awarded a PhD in Spanish and Catalan studies in 2008. His thesis, “Minority languages on the Internet: promoting the regional languages of Spain”, was published by VDM Verlag in 2009.

He is currently an honorary Professorial Fellow at the Melbourne School of Engineering, University of Melbourne; and an Adjunct Senior Research Fellow in the School of Languages, Cultures and Linguistics at Monash University.
Dr Rebecca Giblin has recently returned to Monash University after spending part of 2011 at Columbia Law School as the Kernochan Visiting International IP Scholar. Her recent book Code Wars (Edward Elgar, 2011) tells the legal and technological history of the first decade of the P2P file sharing era, focusing on the innovative and anarchic ways in which P2P technologies evolved in response to decisions reached by courts with regard to their predecessors (and developing a compelling new theory to explain why content industry victories against providers of those technologies failed to reduce the range and availability of P2P software). See www.codewarsbook.com. A selection of her other work can be found at http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=656650.

rebecca.giblin@monash.edu

Dr David Lindsay is an Associate Professor in the Faculty of Law at Monash University, and an expert on copyright law, Internet law, privacy law, and communications law and policy. He is a board member of the Australian Privacy Foundation (APF) and, currently, a member of the ALRC’s Copyright Inquiry Advisory Committee.

david.lindsay@monash.edu.au
Dr Clare Lloyd joined the Department of Internet studies after teaching communication and media studies at the University of Newcastle. Her publications include a co-authored book chapter on identity practices and the mobile phone (in *Handbook of Research on Discourse Behaviour and Digital Communication: Language Structures and Social Interaction*).

**ALANA MAURUSHAT**  
*University of New South Wales*

Alana Maurushat is Acting Academic Director of the Cyberspace Law and Policy Centre, sessional lecturer, and PhD candidate at the Faculty of Law at UNSW. She was Assistant Professor and Deputy Director of the LLM in Information Technology and Intellectual Property at HK Faculty of Law. She teaches Advanced Legal Research. Her current research is focused on technical, ethical and legal dimensions of computer Malware, building on past research projects on the impact of surveillance technologies on free expression and privacy. She is a partner investigator in the Regulating Malware research project.
HOLLY RAICHE  
*University of New South Wales*

Holly Raiche is adjunct lecturer at the Faculty of Law, UNSW and teaches undergraduate and graduate classes in the areas of telecommunications and broadcasting law. She is a Research Fellow at the Cyberspace Law and Policy Centre at the University of NSW, and a Research Associate at the Communications Law Centre.

Holly is on the policy committee of the Internet Society of Australia (ISOC-AU) and on the Board of the Australian Communications Consumer Action Network, Australia’s peak body for consumer advocacy in communications. Previously, Holly was the Project Manager for Consumer Codes and Compliance Officer at Communications Alliance, Communications Advisor to the Australian Democrats party, and Policy Advisor at the Communications Law Centre.

h.raiche@internode.on.net

SCOTT RICKARD  
*University of Canberra*

Scott Rickard was a Senior Researcher at the Smart Services CRC at Swinburne University of Technology investigating end user adoption and usage of wireless technologies. She now holds a position as an Assistant Professor in Communication at the University of Canberra and her current research includes end user investigations into video-calling practice. In the past Scott worked in communications, public relations and multimedia in the private and not-for-profit sectors in Melbourne.
WARWICK A ROTHNIE
Barrister

Warwick Rothnie practises as a barrister in all aspects of intellectual property, having previously been a partner in the intellectual property and telecommunications group of Mallesons Stephen Jaques. He is a contributing author to Lahore, Lindgren and Rothnie, Copyright & Designs and, the author of, amongst other things, Parallel Imports (Sweet & Maxwell, 1993). He is a UDRP panellist for WIPO and a member of the Law Council of Australia’s Intellectual Property Committee. Warwick is a past member of the Commonwealth Attorney-General’s Copyright Law Review Committee and was a consultant to the ALRC’s Designs Law reference.

war@vicbar.com.au

KIMBERLEE WEATHERALL
The University of Sydney

Kimberlee Weatherall is an Associate Professor at the Sydney Law School. Prior to joining the School in 2012, Kimberlee held positions at the University of Queensland, the University of Melbourne and the Intellectual Property Research Institute of Australia. Kimberlee teaches and researches in intellectual property law, with a particular interest in digital copyright, the relationship between international trade and intellectual property, and the systems for administration and enforcement of intellectual property rights. She has published in a range of Australian and international journals, has been invited to speak in the US, Japan, Taiwan, China, the UK, Europe, Singapore and New Zealand, and has given expert evidence to Parliamentary and law reform committees. She has been a member of the Law Council of Australia IP Subcommittee since 2006.

kimberlee.weatherall@sydney.edu.au
ACS-TSA (the Telecommunication Society of Australia, a special interest group within the Australian Computer Society), is grateful to the following sponsors for supporting its journal TJA and the TSA’s other activities in support of a well-informed telecommunications industry:

**Silver Sponsor**

![iiinet](image)

**Standard Sponsors**

-Nec
-Alcatel-Lucent
-CSIRO
-NICTA
-‘yes’ OPTUS
-Telecommunications