Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

2011: The Year Ahead

Lawyers from Allens Arthur Robinson take a look at some key areas of likely reform for the communications sector in 2011.

It is widely recognised that the Australian legal and regulatory environment is always playing catch-up to the media and telecommunications industry and developments in technology.

The past few years have seen extraordinary developments in this space. Increases in network connection speeds, battery life, network capacity and unicast video uses, have contributed to the enormous take-up of new and converged services.[1] Last year's mobile data traffic was three times the size of the entire global internet in 2000.[2] Mobile *video* traffic constituted 49.8 percent of that data traffic and it is expected that this will increase to 66 percent by 2015.[3] 2010 was also the year of the tablet, which brought with it a data usage profile five times higher than that of a smart phone.[4]

While consumer habits and business models have been undergoing a rapid transformation for several years, the regulation of media and telecommunications industry has simply teetered on the cusp of change. 2011 looks to be the year that may tip these regulatory changes into reality.

The top five areas to watch in the regulatory space for 2011 are set out below:

1. The National Broadband Network

The National Broadband Network (***NBN***) has finally moved beyond political debate, with construction in pilot areas underway and the key tenets of the Commonwealth's policy either now enshrined in legislation or edging their way through the legislative process.

The *Telecommunications Legislation Amendment (Competition and Consumer Safeguards) Act 2010* (the ***CCS Act***), which received assent on 15 December 2010, has significantly altered the competitive dynamics of the Australian telecommunications industry by requiring Telstra to undergo either a voluntary structural separation or enforced functional separation. As a result, industry participants who provide retail services based on the acquisition of wholesale services from Telstra, will now deal with either NBN Co (if Telstra structurally separates and NBN Co concludes binding definitive agreements with Telstra) or with either NBN Co and a wholesale/network arm of Telstra that is at arm's length from Telstra retail (if Telstra functionally separates and NBN Co cannot conclude binding agreements with Telstra). NBN Co and Telstra are currently working towards finalising commercial terms and associated operational details of the deal, with a view to Telstra putting the proposal to its shareholders later this year.

Debate on the *National Broadband Network Companies Bill 2011* (the ***Companies Bill***) and the *Telecommunications Legislation Amendment (National Broadband Network Measures – Access Arrangements) Bill 2010* (the ***Access Bill***) resumed in February this year. Both the Companies Bill and the Access Bill have now passed both houses of Parliament after vigorous debate in the Senate and amendment to certain key provisions. The Companies Bill establishes the ownership, operating and governance arrangements of NBN Co to ensure NBN Co will adhere to its wholesale-only mandate. It also establishes the conditions for the eventual sale of the Commonwealth's stake in NBN Co and sets out the reporting and governance obligations which must be complied with once NBN Co is no longer a wholly-owned Commonwealth company. The Access Bill builds on the Companies Bill by introducing additional rules relating to the sup-

1 Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015, February 2011, p8.

2 ibid, p1.

3 ibid.

4 ibid, p2.

Volume 29 Nº 4
April 2011

Inside This Issue:

Contents

ply of services by NBN Co. The Access Bill contains new transparency and non-discrimination rules aimed at protecting the wholesale-only, open-access nature of the NBN initiative. It also seeks to establish a level playing field for 'superfast' broadband networks by imposing certain obligations on other owners of such networks.

Increases in network connection speeds, battery life, network capacity and unicast video uses, have contributed to the enormous take-up of new and converged services.

The NBN creates a unique set of regulatory requirements and the technological opportunities it enables provide the impetus for a regulatory overhaul of the entire industry. This change also underpins the remaining four areas to watch, as the NBN facilitates convergence, increases the numbers of consumers using and depending on technology, increases the demand for spectrum and the need to protect online transactions.

2. The Convergence Review

The last time the media industry underwent a major regulatory overhaul was in 2006/2007. That period saw changes to media ownership and control rules, the introduction of legislation to govern the transition to digital television and digital radio, and the reform of online content regulation in response to the infamous "Big Brother" incident.

Five years on, services that were once distinct have now converged. Fragmented and dedicated home networks carrying one or more analogue or digital services have transitioned to unified IP-based networks that can deliver multiple applications and services.

These developments have once again emphasised the need for a review of the regulatory regime. As a result, in December 2010, the government commenced the Convergence Review, announcing that a committee of independent experts will examine and provide advice to the government on an appropriate policy and regulatory framework for a converged environment. The Department of Broadband Communications and the Digital Economy (***DBCDE***) has released terms of reference to guide the work of the Committee in conducting the review.

The parameters of the Convergence Review are still unclear, though early statements suggest that it may not be as comprehensive as expected. The terms of reference focus on media and content regulation. While telecommunications are relevant to convergence, the government has indicated that, as a result of forthcoming changes to the telecommunications industry such as the NBN, it would be premature to conduct a broad review of telecommunications obligations.

The government has also stated that due to the Australian Law Reform Commission's review of the National Classification System, classification issues are beyond the scope of the review. However, given that the review is to consider "appropriate policy settings to ensure the adequate reflection of community standards and the views and expectations of Australian citizens", and that the *Broadcasting Services Act 1992* (Cth) (***BSA***) currently authorises regulatory schemes for classification of content over spectrum and the internet, the review will likely touch on the appropriateness of the current regulatory arrangements in a converged environment.

Similarly, the government does not propose to explicitly consider further changes to the anti-siphoning list as part of the Convergence Review, because Senator Conroy only recently announced a new anti-siphoning list that is to apply to listed events until 31 December 2015.

Likely areas of re-examination include Australian content quotas which act to ensure the production and dissemination of Australian content and which currently apply to commercial television and radio but not to internet broadcasting. It is expected that the Convergence Review will address this by recommending policies that promote the production and distribution of Australian content in relation to several forms of publication.

Media ownership and control restrictions are also likely to be revisited, as convergence means that these no longer sit easily with the reality of the diversified delivery of content. For example, the current restrictions on the control of broadcasting licences on the basis of audience reach, becomes less relevant where those same broadcasters may be able to reach 100 percent of the population via internet broadcasting.

3. Focus on the Consumer

As new technologies become ubiquitous, dependence on these technologies increases and so too do consumer complaints. Telecommuncations Industry Ombudsman (***TIO***) complaint numbers rose nine percent to 87,264 in the six months prior to 31 December 2010, compared to the preceding six months.[5]

Although the Communications Alliance (***CommsAlliance***) argues that the increase in complaints reflects the increased uptake of telecommunications services[6], regulators have focused on the treatment of consumers, complaints handling and the perceived deficiencies of the current self-regulatory regime.

As a consequence, both the DBCDE and the ACMA have recently taken steps to enable continuing reforms to telecommunications consumer safeguards.

ACMA's Reconnecting the Customer Inquiry, which is due to report its findings in the coming months, aims to identify the causes of, and recommend solutions for, what it regards as systemic problems in the Australian telecommunications sector with the way it deals with its consumers. The inquiry is focused specifically on customer service and complaints handling practices.

At the same time, the CommsAlliance Telecommunications Consumer Protection Code is under review and ACMA has been outspoken in its willingness to force changes to the existing regime. Registration of a mandatory standard by ACMA in the event that it is dissatisfied with the Code and unconvinced of the adequacy of the existing self-regulatory framework, remains a real possibility.

The Telecommunications Industry Ombudsman Scheme discussion paper recently released by the DBCDE requests submissions on options for reforming the TIO scheme and ensuring that it has the appropriate tools to deal with complaints.

4. Spectrum

The scarcity of spectrum and demands placed upon it by wireless access services and spectrum intensive technologies such as HDTV and IP based applications, remains a continuing issue for both the industry and ACMA, which has a mandate to manage the radiofrequency spectrum in Australia.

In March 2011, the ACMA published the Five Year Spectrum Outlook 2011-2015, which, amongst other things, outlines upcoming spectrum projects in Australia.

The most significant of these relates to the reallocation of spectrum that will become available as a result of digital switch-off. Digital switch-off has now commenced and steps are being taken to restack the digital television channels and realise the digital dividend spectrum. The auction of spectrum licences in respect of the digital dividend spectrum is expected to take place in late 2012, before completion of the digital switchover and restack processes.

Interestingly, the CCS Act prevents Telstra from acquiring or operating spectrum useful for advanced wireless broadband (including 520 MHz to 820 MHz and 2.5GHz to 2.69GHz), unless a structural separation undertaking is in force, in addition to Telstra divesting its interest in hybrid-fibre coaxial networks and subscription television broadcasting licences (however, the Minister may exempt Telstra from this latter requirement if it submits an adequate structural separation undertaking). Should Telstra be prevented from acquiring or operating that spectrum, opportunities will emerge for other market participants to bid for that spectrum without competition from Telstra, should it become available.

Another significant spectrum project is the reallocation of spectrum licences due to expire over the next few years. The ACMA has not yet announced whether these licences will be renewed, and if so, on what terms.

5. Electronic transactions

As the number of electronic transactions increase, so too does the need for effective regulation that protects online users whilst encouraging efficient and effective online transactions.

Following agreement at a Standing Committee of Attorneys General last year to enact a Model Electronic Transactions Bill (***Model Bill***), Attorney-General Robert McClelland has introduced into the House of Representatives the Electronic Transactions Amendment Bill 2011 (***ETA Bill***).

The Model Bill reflects the need for clarity in the current use of electronic contracting. Already in effect in New South Wales, it has been introduced in Tasmania, Western Australia and South Australia. Once enacted in all jurisdictions, the Government will accede to the UN Convention on the Use of Electronic Communications in International Contracts with the aim of facilitating international trade.

The NBN creates a unique set of regulatory requirements and the technological opportunities it enables provide the impetus for a regulatory overhaul of the entire industry.

The ETA Bill broadens the types of electronic signatures that are valid to include, in addition to methods reliable for the purpose, those proven in fact to have identified the person. It will be important for parties to agree up-front on the communication methods that will be relied on in an arrangement if a narrower definition is required.

It also broadens the definition of 'transaction' to include any statement, declaration, demand, notice or request, including offers and acceptances of offers, that a party makes in connection with the formation or performance of a contract.

The rules relating to time of dispatch and receipt of electronic communications have been amended so that dispatch is when the electronic communication leaves the information system under the control of the sender rather than when the electronic communication enters the information system outside the control of the sender. The time of receipt is when the electronic communication becomes capable of being retrieved by the addressee at the electronic address designated by the addressee rather than when it comes to their attention. Where the communication is made to an electronic address not designated by the addressee, receipt is when it is available and the addressee is aware of it.

The ETA Bill confirms the common law presumption that, unless clearly indicated to the contrary, an electronic proposal to form a contract is to be considered not an offer but an invitation to treat. It also clarifies that transactions formed through automated message systems are valid. It provides that a natural person will be allowed to correct an 'input error' they have made in transacting with a party through an automated message system where there is no opportunity to correct the error. The communication can be withdrawn by notification being given as soon as possible, so long as a benefit has not been received through the transaction. The ETA Bill states that this is not a right to rescind or otherwise terminate a contract but the notes confirm that in some circumstances the withdrawal may invalidate the entire communication. This measure is clearly directed at providing consumer protection but creates an unintended potential for what could in effect be a 'cooling off' period. The provision may be need to be amended to provide greater clarity in line with the fundamental purposes of the amendment. In any event, the implication of this change is that the owner of a website making use of automatic message systems should ensure their automatic message systems are designed to offer opportunities to correct errors prior to contract formation.

Valeska Bloch, Anna Payten, Joelle Vincent and William Watson are lawyers in the communications, media and technology practice group at Allens Arthur Robinson.

---

5 "Vodafone Boosts TIO Complaints", *Exchange Daily*, 28 February 2011.

6 Long, G. "CommsAlliance defends industry against poor performance", *Communications Day*, Issue 3934, 28 February 2011.

Contracting With Social Media

Nick Abrahams and Sara Payton discuss some of the risks facing businesses who engage in social media.

Social media work used to be about preparing policies in relation to social media use in the office and addressing human resources issues. Concerns of businesses were largely limited to the effect that use by employees had on productivity and the workplace relations issues relating to the manner of use. However social media has jumped the fence. It is no longer simply about people going to Facebook to engage directly with Facebook. Rather, social media is now becoming a key part of most media sites and businesses are increasingly turning to social media to broaden their exposure. This increased use also brings with it a variety of separate legal issues that businesses must address.

As these terms of use are prepared by the social media providers it is not surprising that they generally favour the social media provider.

How social media is incorporated into websites

With the growth in the number of businesses incorporating social media into their websites, most internet users will have had some exposure to these features. It is not uncommon for online journals and newspapers to include an option for readers to 'Share' or 'Tweet' the content on Facebook, Twitter, LinkedIn and other social media sites. Similarly, many businesses offer visitors to their website the option to follow the business through social media. However, there are many other features that may be incorporated into your website. These include:

- Facebook 'Like' button – users can indicate whether they like a business, website or product and publish that information on their 'wall'. This feature also provides a counter facility that displays the number of users who 'Like' the item.
- 'Share' feature – users can select to 'Share' specific content on their relevant social media site. A link to the website will be published on the user's wall together with information that the social media provider extracts from that site.
- Facebook and Twitter 'Feeds' – a website can display a summary of the recent activity of other followers, or 'friends' of that website or business in the form of a feed of content from the social media site.
- Facebook 'Recommendations' plugin – this feature enables a website to display information concerning the most popular content on that site.
- Single log in – users can log into a business' site via the user's social network account.

Issues to consider

How do you intend to use the social media feature?

The issues relevant to incorporating social media in your website will vary depending on what social media features you intend to include. For example, are you simply providing a link to the social media site? Will you incorporate the logo for that site? Are you incorporating an enhanced feature, such as a 'Share' or 'Tweet' button? Will you use an Application Programming Interface (or 'API')? Specific terms may apply to different features. Similarly, different terms will apply to different social media providers.

The social media providers each publish their terms of use on their sites. As these terms of use are prepared by the social media providers it is not surprising that they generally favour the social media provider. Businesses must carefully review these terms to ensure that their intended use of the social media is compliant with the terms. Often these terms will contain restrictions on the ability to compete with the social media site. The business will need to assess whether its proposed integration with the social media site could bring the business within these restrictions.

Are the terms acceptable – do they permit your intended use?

The terms of use restrict how the social media site can be used. Where a business is planning on incorporating social media into its website, the terms of use must be considered to determine any limitations on the use of the social media features and any restrictions on what content can be included on the social media site. For example, many social media providers restrict how their features can be used for advertising. Similarly, there are often limitations concerning syndication functions. Therefore, before incorporating social media into its site, a business must ensure that the feature is right for what it wants to do.

Will you need to pay?

Perhaps one of the main attractions for businesses to incorporate social media into their sites is that such use is generally free. However, various sites do provide for circumstances where payment may be required. For example, at the time of writing, the Twitter terms provided that a business will be required to compensate Twitter, where Twitter content is the primary basis of an advertising sale. Other social media sites also provide a warning that use of their sites may not be free in the future.

What is the risk if the terms change?

These terms are subject to change at the discretion of the social network provider. Such change can occur very quickly and there is no limitation on the extent of such changes. This represents a risk to businesses that include social media in their websites, as a change to the terms could cause the investment in the application to be lost. Therefore, businesses must be vigilant in monitoring changes and ensuring continued compliance with amended terms. Businesses must also evaluate how easily they can cease using the social media feature in the event that the terms change in a manner that is adverse to the business.

Can you negotiate a separate licence with the social media provider?

Where a social media provider's terms prevent the intended use of the relevant feature, a business may need to seek a separate agreement with the provider to allow the proposed use. Where a separate licence is negotiated, a business will not be limited to the general terms and can more specifically address the manner that it intends to use the social media features. Businesses may also consider this approach where the risk associated with a change to the terms is high. However, ultimately there is no obligation on the social media provider to enter into such an agreement.

Where to from here?

If a business is contemplating incorporating social media into its websites, ensure that you review the social media providers' terms and, where in doubt, seek legal advice on how those terms will apply to the business.

Nick Abrahams is a partner at Norton Rose Australia and Sara Payton is a lawyer at Norton Rose Australia.

Computer Monitoring of Government Employees: Not An Invasion of Privacy

Marlia Saunders, Melanie Bartlett and Sophie Dawson consider a recent Federal Court decision which found that monitoring a Commonwealth employee's personal use of IT systems was not an invasion of privacy.

The Federal Court of Australia has confirmed in *Griffiths v Rose* [2011] FCA 30 (31 January 2011) that the monitoring by a government department of its employees' personal use of IT systems will not constitute an invasion of privacy so long as employees are informed that such scrutiny will occur.

Although the case preserves the rights of Commonwealth agencies to check their employees' emails and internet browsing habits, such employers should take care to ensure that their IT usage policies are broad enough to cover all types of personal information that they may collect in the course of undertaking such monitoring activities, in order to avoid a finding that they have collected information by unfair means in breach of s16 of the *Privacy Act 1988* (Cth) (***Privacy Act***).

Background facts

Mr Griffiths (the ***Applicant***), a senior public servant, was fired from a Commonwealth department after being found to have viewed a number of websites which contained pornographic images on his work laptop. He had viewed the websites at home using his own internet connection, then deleted the website entries from the browser's internet history.

The Applicant claimed he was not aware that the department used a software program which logged the occurrence of particular keywords on its IT systems, took snapshots of the desktop every 30 seconds and collected all emails, attachments, internet searches and instant messages performed or sent by a user. The information gathered was then retained on the department's server when the laptop was reconnected to the network, and the department would conduct regular audits of the information.

The department became aware of the Applicant's conduct during such an audit, and after conducting an internal investigation, found the Applicant had breached the department's IT policy, which prohibited employees from using departmental IT facilities to deliberately access or download pornography. In the course of the investigation, the department found that the Applicant was in breach of the 'Australian Public Service Code of Conduct' contained in the *Public Service Act 1999* (Cth) (***Code of Conduct***), which requires public servants to comply with any lawful and reasonable direction by an agency, to use Commonwealth resources in a proper manner and to uphold the values, integrity and good reputation of the Australian public service. The Applicant's employment was consequently terminated.

The Applicant's argument

The Applicant claimed that his privacy had been grossly invaded by the department using software to monitor his browsing habits during periods of personal use. The Applicant sought orders quashing the finding that he had breached the Code of Conduct and the decision that his employment be terminated. He also sought a declaration that the Commonwealth could no longer investigate his conduct insofar that it related to him accessing lawful pornography in private and outside working hours.

The Applicant argued that the direction in the department's IT policy not to view pornography was not lawful or reasonable because it invaded his privacy to the extent it permitted the department to monitor his personal usage of the laptop, and no legitimate interest of the department was protected as a result of such monitoring. In particular, he submitted that:

- the direction infringed Information Privacy Principle 1 (***IPP 1***) and was therefore contrary to s16 of the Privacy Act;
- even if the direction was lawful, it was not reasonable because it infringed common law and equitable rules relating to privacy, including Article 17 of the *International Covenant on Civil and Political Rights* (***Article 17***), which provides for a right not to be subjected to any 'arbitrary or unlawful' interference with privacy; and
- the direction was not reasonable in the ordinary sense.

the information obtained by the Commonwealth was for the lawful purpose of ensuring compliance with the Code of Conduct, and the means of collection could not be regarded as 'unfair' in circumstances where employees had been specifically warned by the department that their computer use is monitored for this purpose

The Commonwealth's argument

The Commonwealth argued that since it was the owner of the laptop, it had the right to regulate how it was used, and to insist that it not be used to look at pornography. In particular, the department had a legitimate interest in ensuring that its equipment was not used in connection with pornography so that it did not accidentally reappear or display in the workplace. Further, the Applicant had been clearly warned of the risks of viewing this type of material. It was submitted that, although the Applicant had rights of privacy, it did not follow that he had a right to use the laptop contrary to the express instructions not to view pornography.

The Decision

Breach of IPP 1

IPP 1 provides that the Commonwealth may only collect personal information which is necessary for a lawful purpose directly related to a function of the Commonwealth and that it must not be collected by unlawful or unfair means.

The Applicant argued that the direction in the department's IT policy not to look at pornography indirectly breached IPP 1 because

of the risk that the direction might be enforced in a way that interfered with an individual's privacy and thereby breach Article 17. The Applicant sought to rely on a finding by the United Nations Human Rights Committee in *Toonen v Australia* (CCPR/C/50/D/488/1992, UN Human Rights Committee (HCR), 4 April 1994), which held that Tasmanian laws banning homosexuality were unlawful since the only way to detect a breach of the laws would constitute an invasion of an individual's privacy.

Justice Perram rejected this argument, and found that the information obtained by the Commonwealth was for the lawful purpose *of ensuring compliance with the Code of Conduct*, and the means of collection could not be regarded as 'unfair' *in circumstances* where employees had been specifically warned *by the department* that their computer use is monitored for this purpose. The department's IT policy explicitly stated that the department may record all emails sent and received by staff and all URL logs, to make sure that employees were not using the department's systems for improper purposes, and the Applicant had signed a document recording that he understood the IT policy.

there may be circumstances where the collection of data by the software program may give rise to unfair collection of information in some circumstances

However, his Honour did note that there may be circumstances where the collection of data by the software program may give rise to unfair collection of information in some circumstances. For example, the department's policy did not warn employees that it may inadvertently collect personal banking information or credit card details during periods of personal use, even though the policy permitted limited personal use for these purposes.

Breach of privacy under common law, equity and Article 17

The Applicant argued that his general rights to privacy under common law and equity were infringed by the direction not to view pornography, insofar as it related to his use of the laptop at home while connected to his own internet service.

Justice Perram stated that, since it was the Commonwealth's laptop, the department was entitled to request that the Applicant not use it to view pornography and had explicitly warned him that his use of the laptop would be monitored with a view to detecting any prohibited use. Given these conclusions, his Honour found that this case did not provide an appropriate vehicle to look at how an equitable action to prevent misuse of confidential information (which has been recognised in a number of lower Courts in Australia) might extend to the personal affairs and private life of a plaintiff.

Justice Perram also rejected the Applicant's argument that the Commonwealth had breached Article 17, finding that there was nothing 'arbitrary or unlawful' about monitoring the Applicant's internet usage when he had been told that it would happen. His Honour distinguished Article 17 from the broader right of privacy contained in Article 8 of the *European Convention on Human Rights*. Even so, his Honour stated that there is authority that even Article 8 will not be infringed where an employee's use of a work phone is monitored, provided that the employee is expressly warned.

Whether the direction was generally unreasonable

Finally, as to whether the direction was reasonable in the ordinary sense, Justice Perram held that it was, reiterating the point that the Commonwealth had a right to stipulate how its own property is used and had a legitimate concern to avoid accidental viewing by others in the workplace.

Conclusion

This decision confirms that it is not a breach of the Privacy Act for a government agency to monitor its employees' use of work computer equipment where they have been warned that such monitoring may take place.

The current employee records exemption under the Privacy Act means that private sector organisations are not required to comply with the Privacy Act in respect of acts or practices directly related to the employment relationship with their employees and to employee records held by the organisations. However, the lessons from this case are also relevant to private sector employers, since any monitoring activities by employers might also access non-employment related information about their employees, in which case the Privacy Act could apply.

All employers should ensure that their IT policies adequately inform employees of the types of information that they may collect in the course of undertaking such monitoring activities, particularly where software systems may gratuitously capture unnecessary information. Employers should also ensure that any monitoring engaged in is reasonable in the circumstances, such as to ensure that prohibited practices are not being conducted by employees.

Marlia Saunders is a Senior Associate, Melanie Bartlett is a Paralegal and Sophie Dawson is a Partner at Blake Dawson.

Editors note

In related developments, significant privacy law reforms are currently working their way through the Australian Parliament. The Australian Law Reform Commission (***ALRC***), in Recommendation 40-1 of its report *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008), recommended that the employee records exemption be removed.

If implemented this reform would mean that employers would be required to comply with the Privacy Act in relation to all personal information about their employees. This recommendation is to be considered by the Australian Government in the second stage of its two-stage response to the ALRC Report. Various other reforms are also proposed – see the website of the Office of the Australian Information Commissioner for more information: http://www.privacy.gov.au/law/reform.

The first stage of reforms will be debated after the Senate Finance and Public Administration Committee delivers its final report on its inquiry in the Exposure Drafts of Australian Privacy Amendment Legislation, due on 1 July 2011. It is expected that the reforms will be put in place in late 2012.

Personal Property Securities Reform

Rebecca Sadleir considers the impact of reform of securities regulation on the communications sector.

The *Personal Property Securities Act 2009* (Cth) (the ***PPSA***) is due to come into force in October this year. It is complex and far-reaching, and businesses in most industry sectors will be affected by the sweeping changes this new legislation will bring to Australia's commercial law. The communications industry is no exception. The PPSA, is similar but not identical to equivalent legislation in New Zealand. It covers a wide range of transactions, not just security interests. It is not limited to consumer transactions, and it significantly alters aspects of commercial law and contracts. This article gives an overview of the PPSA and how it will affect the communications sector.

Background to the reforms

Current position

More than 70 Commonwealth, State and Territory pieces of legislation currently regulate personal property securities, with around 40 separate registers recording interests in different types of property. There are significant practical limitations on the use of personal property as security due to complexities and gaps in the arrangements for registering security interests.

Aim of the reforms

By introducing the Personal Property Securities (***PPS***) reforms, the Federal Government's stated intention is to streamline the law, increase certainty and consistency and reduce complexity and costs by introducing:

- a generic set of rules that apply to nearly all personal property;
- a single set of priority rules for competing security interests; and
- a single, definitive, online, national register on which all personal property securities will be registered and searchable by the public.

According to the Federal Attorney-General's website, the aim of PPS reform is to improve the ability of individuals and businesses, particularly small-to-medium-size businesses, to employ all of their property in raising capital.

Given the highly complex nature of the legislation, it remains to be seen whether the reforms will achieve the intended effect.

Legislation status and timing

The PPS legislation comprises:

- *Personal Property Securities Act 2009* (Cth) (received Royal Assent on 14 December 2009);
- *Personal Properties Securities (Consequential Amendments) Act 2009* (Cth) (received Royal Assent on 14 December 2009);
- *Personal Property Securities (Corporations and Other Amendments) Act 2010* (Cth) (received Royal Assent on 6 July 2010); and
- *Personal Property Securities Regulations 2010* (registered on the Federal Register of Legislative Instruments on 26 November 2010).

The bill for the third (and probably final) round of amendments to the PPSA, the Personal Property Securities (Corporations and Other Amendments) Bill 2010 (Cth), was released on 25 February 2011.

The original timetable for implementation of the PPS reforms was ambitious and implementation has been significantly delayed. In mid-February 2011, COAG agreed to defer the commencement date of the new legislation again, from May to October 2011.

Key terminology and concepts

Key to the reforms is the functional approach of the new regime, where generally (although not always) it is the commercial effect of a transaction, rather than its legal form which, determines how it is characterised by the legislation. *Under the 'form over function' approach*, the distinctions between different types of security interest and terminology such as 'charge' and 'mortgage' will become less significant. The new law signals the end of the floating charge, to be replaced by the concept of 'security interest over a circulating asset'.

Under the 'form over function' approach, the distinctions between different types of security interest and terminology such as 'charge' and 'mortgage' will become less significant.

Key terminology introduced by the PPSA

Personal property is all property other than land and certain statutory licences. It includes tangibles such as goods and equipment as well as intangible property such as intellectual property (***IP***) and IP licences.

A ***security interest*** is an interest in relation to personal property that in substance secures payment or performance of an obligation.

The PPSA gives examples of arrangements that are security interests (provided they are interests in property that secure payment or performance of an obligation). These include:

- charges, mortgages and pledges;
- conditional sale agreements (including an agreement to sell, subject to retention of title);
- hire purchase agreements;
- consignments;
- leases of goods; and
- flawed asset arrangements.

In certain cases, the PPSA adopts a 'form over substance' approach, and deems some transactions to be security interests, even though they do not secure anything. Examples of this include:

- transfers of accounts (receivables for goods or services supplied) and 'chattel paper' (documentation governing certain financial interests in goods, such as a hire-purchase agreement);
- a consignor's interest in a commercial consignment; and
- most relevantly to the communications industry, a lessor or bailor's interest in goods under a 'PPS lease'.

A ***PPS lease*** is defined as a lease or bailment of goods for more than one year or an indefinite term, or 90 days for serial numbered goods. A PPS lease does not include arrangements where the lessor or bailor is not regularly engaged in the business of leasing or bailing goods and it only includes bailments where the bailee (the party that gets possession) provides value.

PPS leases will include operating leases as well as finance leases. This will be particularly relevant to the communications industry where there are numerous arrangements where equipment is provided as

part of a service. For example, where a content service provider provides customer premises equipment such as set top boxes or other reception equipment to customers on a lease basis, or when equipment is supplied as part of an outsourcing arrangement.

Key concepts under the PPSA

Attachment is the description of the successful creation of a security interest in personal property. A security interest attaches when:

- the secured party has given value (e.g. a loan) or done an act by which the security interest arises (e.g. execute a document); and
- the grantor has rights (or the power to transfer rights) in the personal property.

Enforceability of security interests. A security interest that has attached is enforceable against a third party when one of the following has occurred:

- the grantor has signed a written security agreement which adequately describes the personal property; or
- the secured party has possession or control of the property.

Perfection is the process that the security holder must undertake to ensure its security interest will take priority over other security interests created in the same personal property. Perfection of a security interest puts a potential secured party on notice of an existing security interest. A security interest is perfected when:

- it has attached to the collateral and the security interest is enforceable against a third party; and
- one of the following has occurred:
    - it has been registered on the PPS register; or
    - the secured party has taken possession or control of the property. For intangible property such as IP, registration is the relevant method to perfect.

Perfection is particularly important in the event of insolvency because, subject to only a few exceptions, on appointment of a liquidator, bankruptcy trustee or voluntary administrator, unperfected security interests 'vest' in the company. The secured creditor loses its security and becomes unsecured.

Priority Rules and Remedies. The PPSA establishes a complete set of rules for determining priority between security interests, and for determining under what circumstances a purchaser of collateral will take the collateral free of any security interests. *In relation to priority between security interests*, the general rule is that perfected security interests take priority over unperfected interests. *Another general rule is that* perfected interests take priority according to the order of perfection, *but there are many exceptions.* These rules replace the old principles-based approach of the common law and equity.

The PPS Register

The PPSA establishes an electronic register, which is designed to provide a simple, quick and cheap registration process. The register is a 'red flag' register, it draws attention to the security interest without giving too many details. While registration is generally simple, there will be some traps in deciding how to describe the collateral (for example with unregistered IP such as copyright), and also in deciding under which category to file the interest.

Because so many arrangements are security interests, hundreds, or even thousands, of security interests may need to be registered against a particular company, and so there is likely to be a lot of data or 'noise' on the register.

Security interests currently registered in certain registers, such as the charges register maintained by ASIC under the *Corporations Act 2001* (Cth), will be automatically migrated across. There will be no automatic migration for the IP registers for trade marks, designs and patents.

The Commonwealth has begun to deploy the IT resources needed to establish the PPS register. Fujitsu has been engaged to build the register and user acceptance testing is due to commence in June 2011.

Implications for the communication sector

The PPSA will have a significant impact on the communications industry, where relationships are highly contractual and equipment is often supplied without passing over full ownership. The PPSA will affect not only financing transactions, but also many transactions in which companies supply goods or services to customers, or have goods and services supplied to them. Interests that were not previously treated as security interests will become subject to the new regime.

Below is a list of scenarios that might be caught by the new legislation (it will ultimately depend on the circumstances of each case):

Equipment use: Any bailments or leases between parties concerning plant, equipment and other property may be registrable security interests. The supply of equipment in an agency, outsourcing or franchise arrangement might also be covered by the PPSA.

Transfers of receivables: Transfers of receivables (for example, the cash flows associated with consumer contracts for the provision of services) are caught by the PPSA.

Phone handsets, set-top boxes and other stock: If a business has acquired finance by offering security over its mobile handsets, set-top boxes or other retail stock, a registrable security interest may be created. This includes where goods are held on consignment. Also, consumer contracts governing, for example, any provision of services where the company retains ownership of an asset used by the consumer may be security interests.

Joint venture arrangements: Cross charges and default clauses in joint venture agreements may also fall within the regime and will need to be reviewed.

Intellectual property: The PPSA contains specific rules in relation to security interests in goods that have closely associated IP rights and, in some cases, the PPSA may deem IP rights to be covered by a security agreement. Security interests in relation to computer equipment, master recordings, copyright material (such as source code, music and photographs) and other assets with closely-related IP should be reviewed in this light.

Film financing: The structuring of financing transactions in the film and television industry may also be affected by the PPSA and will need to be reviewed.

Franchises: Transactions raising finance against projected franchise fees using franchised IP as the collateral will need to be reviewed.

What should companies in the communications sector (and their lawyers) be doing now?

The industry should begin preparing immediately for the new PPSA regime to protect their interests and minimise disruption to businesses once the PPSA takes effect. Preparations should include, where applicable:

- Scoping the task. This will involve checking in particular standard terms of supply, as well as financing arrangements and other potentially affected contracts.
- Identifying the assets affected.
- Compiling inventories of existing security interests (including interests that are currently registered on other registers) in order to register them and take any other steps necessary to protect them.
- Where necessary, developing new policies and procedures on the requirements for transactions and documentation and giving training and guidance to staff.
- Developing new systems to record and manage future security interests and deal with enquiries and other requirements of the legislation.
- For suppliers of goods or services, registering interests and redrafting supply terms.

Rebecca Sadleir is Special Counsel in the Intellectual Property practice group at Allens Arthur Robinson

A Pyrrhic Victory For "Doing Squat": A Short Critique Of The Full Court's Decision In *Roadshow Films v iiNet*

Wen Hui Wu[1] reviews the Full Court of the Federal Court's decision in *Roadshow Films v iiNet* and considers the interplay between copyright authorisation and the "safe harbour" provisions.

On 24 February 2011, the Full Court of the Federal Court handed down its keenly-anticipated decision in *Roadshow Films Pty Limited v iiNet Limited* [2011] FCAFC 23 (***iiNet***). A majority of the Full Court dismissed the film companies' appeal from the trial judge's decision that the internet service provider (***ISP***) iiNet was not liable for "authorising" copyright infringement by its users via the BitTorrent peer-to-peer network. However, as the conclusion to Justice Emmett's reasons makes clear, the Full Court's decision does not bring to an end the dispute between content owners and ISPs over online copyright infringement.[2]

This article will review and critique the Full Court's decision in *iiNet*. First, it is necessary to review, briefly, the doctrine of authorisation in copyright infringement. Second, this article will survey their Honours' reasons in *iiNet*. Third, this article will show that there is a confused interplay between the doctrine of authorisation and the "safe harbour" provisions for carriage service providers in Part V, Division 2AA of the *Copyright Act*. Lastly, the significance of the *iiNet* decision to online copyright infringement will be considered.

The doctrine of authorisation

The Australian doctrine of authorisation has been criticised as being "a litany of competing and contrasting considerations",[3] "built on shaky foundations",[4] "uncertain"[5] and "shift[ing] the balance in copyright too far in favour of the owner's rights".[6] Detailed studies of its "tortuous"[7] development have been undertaken by Birchall, Napthali, Giblin and Brennan.[8]

Section 13(2) of the *Copyright Act 1968* (Cth) (***Copyright Act***) confers upon a copyright owner the exclusive right to authorise another person to exercise the acts comprised in the copyright. A person infringes copyright if, not being the copyright owner and without the licence of the owner, that person does in Australia, or authorises the doing in Australia of, any act comprised in the copyright (see Sections 36(1) and 101(1)). Thus there are two types of copyright infringement: the doing of an infringing act ('primary infringement') and the authorising of the doing of a primary infringing act ('authorisation'). It has been established that the two types of liability are distinct, actionable torts.[9]

the Full Court's decision does not bring to an end the dispute between content owners and ISPs over online copyright infringement

The High Court in *UNSW v Moorhouse* (1975) 133 CLR 1 (***Moorhouse***) adopted the definition of "authorise" in the *Oxford English Dictionary* – to "sanction, approve, countenance".[10] Liability may be found by omission – indifference may reach a degree from which authorisation may be inferred.[11] Two different approaches were posited in *Moorhouse*: Jacobs J's approach, where there has been an express or implied invitation by the alleged authoriser to infringe, and Gibbs J's approach, where the alleged authoriser con-

---

1 The author gives thanks to Michael Handler of UNSW Law School and Nic Suzor of QUT Law School. All errors and omissions are, of course, the author's own.

2 *Roadshow Films Pty Limited v iiNet Limited* [2011] FCAFC 23 (***iiNet***), [274] (Emmett J).

3 *Roadshow v iiNet (No 3)* [2010] FCA 24, [358] (Cowdroy J).

4 Sydney Birchall, 'A doctrine under pressure: The need for rationalisation of the doctrine of authorisation of infringement of copyright in Australia' (2004) 15 *AIPJ* 227, 236.

5 Rebecca Giblin, 'The uncertainties, baby: Hidden perils of Australia's authorisation law' (2009) 20 *AIPJ* 148.

6 *CCH Canadian Ltd v Law Society of Upper Canada* [2004] 1 SCR 339, [41] (Supreme Court of Canada).

7 *WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274, 285 (Gummow J) ('*Hanimex*').

8 Sydney Birchall, above n 4; Michael Napthali, 'Unauthorised: Some thoughts upon the doctrine of authorisation of copyright infringement in the peer-to-peer age' (2005) 16 *AIPJ* 5; Rebecca Giblin, n 5; and David Brennan, 'ISP Liability for Copyright Authorisation: The Trial Decision in *Roadshow Films v iiNet* Part One' (2010) 28(4) *CLB* 1.

9 *Hanimex*, 284 (Gummow J), approved in *APRA v Jain* (1990) 26 FCR 53, 57 (Sheppard, Foster and Hill JJ). As a result, *"authorises the doing of an act"* in ss 36(1) and 101(1) is wider than *"the exclusive right to authorise"* in s 13(2), a controversy first recognised by Gummow J in *Hanimex*, 286, but, in light of the High Court's decision in *UNSW v Moorhouse* (1975) 133 CLR 1 (***Moorhouse***), never satisfactorily resolved.

10 *Moorhouse* (1975) 133 CLR 1, 12 (Gibbs J) and 20-21 (Jacobs J, with whom McTiernan J agreed), citing *Falcon v Famous Players* [1926] 2 KB 474, 471 (Bankes LJ), which in turn cited *Evans v E Hulton & Co Ltd* [1924] All ER 224 (Tomlin J). It is remarkable that the doctrine of authorisation has come to be defined by this all-encompassing "catchphrase", which seems to have been largely determined by lexicographical choice from a number of meanings of the verb "authorise". For example, if their Honours in *Moorhouse* had adopted an alternative definition in the *Oxford English Dictionary* (*"to give legal or formal warrant to (a person) to do something; to empower, permit authoritatively"*) or the *Macquarie Dictionary* definition (*"to give authority or legal power to; empower (to do something); formally sanction (an act or proceeding)"*), the doctrine may be very different to what it is now.

11 *Moorhouse*, 12 (Gibbs J) and 21 (Jacobs J, with whom McTiernan J agreed).

trolled the means by which infringement was committed, knew or had reason to suspect those means were likely to be used for infringement, and had failed to take reasonable steps to limit their use to legitimate purposes.[12]

In 2001, the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) amendments inserted three statutory factors into the doctrine, set out in ss 36(1A) and 101(1A). Those provisions state that, in determining liability for authorisation, the factors that must be taken into account include:

while the Moorhouse principles continue to be relevant, their application is subject to any inconsistency with the statutory factors in s 101(1A)

- The extent (if any) of the alleged authoriser's power to prevent the doing of the infringing act;
- The nature of the relationship between the alleged authoriser and the primary infringer; and
- Whether the alleged authoriser took any (other)[13] reasonable steps to prevent or avoid the doing of the act, including compliance with any relevant industry codes of practice.

The Full Court's reasoning in *iiNet*

The trial judge's decision, *Roadshow Films v iiNet (No 3)* (2010) 263 ALR 215, has been reviewed by Brennan in an earlier issue of this publication.[14] At trial, Cowdroy J held iiNet was not liable for authorisation because the internet service provided by iiNet was not the "means of infringement", and that the true "means" was the use of the BitTorrent system, over which iiNet had no control.[15] The trial judge further held that a warning and termination scheme suggested by the film companies was neither a "relevant" power to prevent infringement (s 101(1A)(a)),[16] nor a reasonable step to take in the circumstances (s 101(1A)(c)).[17]

On appeal, the Full Court was divided on the primary issue of whether iiNet had "authorised" the copyright infringements by its users via the BitTorrent peer-to-peer system. The majority, Justices Emmett and Nicholas, narrowly concluded that iiNet had not.[18] Justice Jagot, dissenting, found that authorisation had been made out.[19] Aside from matters of impression,[20] their Honours differed in their approach to the doctrine of authorisation and its application.

All three judges agreed that the pre-existing case law, including *Moorhouse*, continued to apply to the doctrine of authorisation. Justice Emmett found that it was important to have regard to the *Moorhouse* principles, although his Honour's reasons are largely structured around each of the statutory factors.[21] Justice Nicholas agreed that *Moorhouse* assists with the interpretation of s 101(1A).[22] Justice Jagot stated that while it is apparent that s 101(1A) is based on the concept of authorisation as developed in *Moorhouse*, the fundamental obligation is to apply the statutory factors.[23] Thus it appears from the Full Court decision that while the Moorhouse principles continue to be relevant, their application is subject to any inconsistency with the statutory factors in s 101(1A). On that basis, all three judges rejected the trial judge's threshold "means of infringement" test.[24]

As to s 101(1A)(a) (the extent (if any) of the alleged authoriser's power to prevent the doing of the infringing act), Justice Emmett held that any power to prevent the doing of the act must be taken into account, and a qualification of "reasonableness" should not be read into this statutory factor.[25] Curiously, however, "reasonableness" features significantly in his Honour's assessment of iiNet's power to prevent infringement.[26] Justice Jagot, too, held that the extent of any power to prevent should be considered: from no power to an absolute power to prevent.[27] Her Honour remarked that, due to the presence of "reasonable steps" in s 101(1A)(c), the reasonableness of the exercise of any particular power to prevent (found to exist under s 101(1A)(a)) is a relevant consideration.[28] While Justice Nicholas also thought "reasonableness" was a gloss, his Honour expressed a view that, in cases founded on inactivity or indifference (as in *iiNet*), there must be *some* power to prevent before authorisation is found.[29] All three judges held that iiNet had the contractual and technical power (by way of warning, suspension and termination) to prevent copyright infringement by its users.[30]

As to s 101(1A)(b) (nature of the relationship between the alleged authoriser and the primary infringer), all members of the Full Court emphasised the contractual power iiNet had under its customer relationship agreement.[31] Under clause 14.2 of that agreement, iiNet users were prohibited from using the internet service to

12 *Moorhouse*, 21 (Jacobs J, with whom McTiernan J agreed) and 13 (Gibbs J)
13 The word "other" appears in s 101(1A)(c) and not in s 36(1A)(c). In *iiNet*, both Emmett J (at [179]) and Nicholas J (at [730]) reject the significance of the word "other". See also Sydney Birchall, "Authorisation of Copyright Infringement: Is the Word 'Other' an Impostor in Section 101(1A)(c)?" (2006) 66 *IP Forum* 34.
14 David Brennan, "ISP Liability for Copyright Authorisation: The Trial Decision in *Roadshow Films v iiNet* Part Two" (2010) 29(1) *CLB* 8.
15 *Roadshow Films v iiNet (No 3)* (2010) 263 ALR 215 (***iiNet (No 3)***), [400]-[407] (Cowdroy J).
16 *iiNet (No 3)*, [425]-[436], [438] and [444] (Cowdroy J).
17 *iiNet (No 3)*, [421]-[422], [436], [438] and [458] (Cowdroy J).
18 *iiNet*, [257] (Emmett J) and [798] (Nicholas J).
19 *iiNet*, [475] (Jagot J).
20 Compare, for example, their Honours' assessment of internal emails and an iiNet press release: *iiNet*, [448] (Jagot J), [770] (Nicholas J), [434] and [469] (Jagot J) and [753]-[754] (Nicholas J).
21 *iiNet*, [23], [25] to [27], [178]-[211] (Emmett J).
22 *iiNet*, [703] (Nicholas J). See also *iiNet*, [704]-[708] (Nicholas J).
23 *iiNet*, [369] (Jagot J).
24 *iiNet*, [126] (Emmett J), [371]-[372] (Jagot J) and [695]-[696] (Nicholas J).
25 *iiNet*, [179] (Emmett J).
26 *iiNet*, [188]-[189], [194] (Emmett J).
27 *iiNet*, [424] (Jagot J).
28 *iiNet*, [399] (Jagot J).
29 *iiNet*, [700], [719] (Nicholas J).
30 *iiNet*, [188]-[189], [194] (Emmett J), [426] (Jagot J) and [720] (Nicholas J).
31 *iiNet*, [192] (Emmett J), [428]-[430] (Jagot J) and [727]-[728] (Nicholas J). See also clause 14.2 of iiNet Customer Relationship Agreement, set out in *iiNet*, [380] (Jagot J).

infringe copyright, and iiNet could, without liability, immediately cancel, suspend or restrict the internet service if it reasonably suspected copyright infringement.

As to s 101(1A)(c) (whether the alleged authoriser took any reasonable steps to prevent or avoid the doing of the act), each of their Honours took a different approach:

(a) Justice Emmett held that s 101(1A)(c) mandated an enquiry as to the steps actually taken by iiNet and a consideration of whether there were any reasonable steps not taken.[32] His Honour thought that iiNet's contractual prohibition and its webpage were insufficient in the circumstances.[33] Although his Honour found that suspension and termination were relevant powers to prevent under s 101(1A)(a), Justice Emmett held that their exercise was unreasonable ***unless***:

  (i) iiNet had been informed in writing of the particulars of the alleged infringement by iiNet users;

  (ii) iiNet has been requested to take specific steps:

    (A) to notify its customers of the alleged infringement;

    (B) to invite those customers to indicate whether iiNet's service has been used for the alleged infringement;

    (C) to request customers to refute the allegations or give assurances that there will be no repetition of infringement;

    (D) to warn the customer that, if no satisfactory response is received within a reasonable time, the iiNet service will be suspended until a reasonable response is received;

    (E) to warn the customer that, if there is continued infringement, the service will be terminated; and

    (F) to terminate the service in the event of further infringements;

  (iii) iiNet has been provided with unequivocal and cogent evidence of the alleged infringements, perhaps including adequate information on collection methodology so as to allow iiNet to verify the accuracy of the data, or verification on oath of the collection methodology; and

  (iv) the copyright owners have undertaken to reimburse iiNet for the reasonable cost of verifying the allegations and monitoring its network, and to indemnify iiNet for any liability as a result of mistaken suspension or termination.[34]

  In the circumstances, because paragraphs (iii) and (iv) above had not been fulfilled in the present case, his Honour did not consider that iiNet had failed to take reasonable steps to prevent the infringing acts.[35]

(b) Justice Jagot held that iiNet should have adopted and implemented a general policy or specific response, which could have included the type of information required before action would be taken, warnings to customers, bandwidth shaping, suspension and termination.[36] As to iiNet's specific responses, her Honour thought they carried little weight in light of iiNet's (internal) attitude to the film companies' allegations.[37]

(c) Justice Nicholas also found that "it was open" to iiNet to adopt a system providing for warnings, suspension and termination of accounts and the failure of iiNet to implement any system was a relevant matter under s 101(1A)(c).[38] In the absence of regulations or industry codes, ISPs should be given latitude to work out the details of such a system.[39]

iiNet could, without liability, immediately cancel, suspend or restrict the internet service if it reasonably suspected copyright infringement.

From the above it can be seen that two judges (Justices Jagot and Nicholas) took the view that iiNet had not taken the reasonable step of implementing a "warning, suspension and termination" scheme.

Despite their concurrence on s 101(1A)(c), Justice Nicholas did not form a majority with Justice Jagot because his Honour characterised iiNet's knowledge of infringement differently. For Justice Nicholas, the notices sent by the film companies were insufficient to provide iiNet with the requisite level of knowledge about specific acts of infringement.[40] The notices did not contain any verification of the accuracy of the collected data or explanation of the collection methodology.[41] Nor was it incumbent upon iiNet to seek out this information when the film companies had not provided it.[42] Justice Emmett appeared to adopt similar reasoning in discussing whether suspension and termination were reasonable steps.[43] For Justice Jagot, the film companies' notices rose above mere or unreliable assertions and provided credible evidence of infringement.[44]

With the above considerations in mind, the Full Court determined whether iiNet "sanctioned, approved or countenanced" the copyright infringements by its users. Justice Emmett did not expressly say so – his Honour's conclusion on authorisation seems premised on the absence of unequivocal and cogent evidence of infringement, cost reimbursement and indemnification.[45] Justice Nicholas recognised the breadth of the third aspect, "countenance", but qualified its scope by stating that "authorise" connotes a mental element of *"consent or permission of some kind or a carelessness from which such consent or permission may be inferred."*[46] iiNet did not ignore the film companies' rights, but did not believe it was

32 ***iiNet***, [195] (Emmett J).
33 Ibid.
34 ***iiNet***, [210] (Emmett J).
35 ***iiNet***, [257] (Emmett J).
36 ***iiNet***, [431] (Jagot J).
37 ***iiNet***, [448] (Jagot J).
38 ***iiNet***, [751] (Nicholas J).
39 ***iiNet***, [750] (Nicholas J).
40 ***iiNet***, [762]-[765] (Nicholas J).
41 ***iiNet***, [762] (Nicholas J).
42 ***iiNet***, [764] (Nicholas J).
43 See third and fourth dotpoints at ***iiNet***, [210] (Emmett J).
44 ***iiNet***, [402], [405] (Jagot J).
45 ***iiNet***, [257] (Emmett J).
46 ***iiNet***, [779] (Nicholas J).

required to act on allegations that required further investigation. The inference of consent or permission could not, in his Honour's view, be drawn.[47] Justice Jagot held that iiNet's responses, in sum, evidenced iiNet's countenance, tolerance or tacit approval of its users' copyright infringements.[48]

iiNet had not taken the reasonable step of implementing a "warning, suspension and termination" scheme

Interplay between authorisation and the "safe harbour" provisions

In 2005, as a result of the Australia-US Free Trade Agreement, the "safe harbour" provisions were introduced in Part V, Division 2AA of the *Copyright Act*.[49] That Division, based on the US *Digital Millennium Copyright Act*, limited the remedies available against carriage service providers (including ISPs) for certain classes of carriage service provider activity, including, relevantly, the provision of facilities or services for the transmission, routing or providing connections for copyright material (Category A).[50] Provided that an ISP meets the conditions in s 116AH(1), under section 116AG(2) of the Copyright Act, the Court cannot award pecuniary remedies against that provider in respect of copyright infringement that has occurred in the course of that activity.

Notwithstanding its conclusion on authorisation, the Full Court reversed the trial judge's holding that iiNet could take advantage of the protection afforded under the "safe harbour" provisions. On the evidence, their Honours held that iiNet did not meet the Condition 1, Item 1 in s 116AH(1) because it did not reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers.[51]

It is apparent from the Full Court's reasons that their Honours drew on various aspects of the "safe harbour" provisions in reaching their respective conclusions on authorisation. For example, in considering whether termination of internet access was a reasonable power to prevent copyright infringement, Justice Emmett reasoned:

> Even where a service provider such as iiNet has the benefit of the Safe Harbour Provisions, the Court is specifically empowered, under s 116AG(3)(b), to order termination of a specified account. It can hardly be concluded, therefore, that termination was, per se, unreasonable. Rather, the *Copyright Act* itself contemplates such a step. Accordingly, it must be regarded as a reasonable step, at least in some circumstances, including circumstances involving repeat infringements, to terminate or suspend an account of a customer.[52]

Likewise, in rejecting iiNet's submission that a "warning, suspension and termination" scheme was complex, expensive and unreasonable, Justice Jagot remarked:

> [T]here is no reason that a scheme of warnings and suspension or termination could not specify the minimum requirements for the provision of information about copyright infringement before action would be taken. In other words, working out these issues is part and parcel of the scheme itself. Moreover… the legislature contemplated a scheme for repeat infringers that would include termination "in appropriate circumstances" (s 116AH(1) of the *Copyright Act*).[53]

Similarly, Justice Nicholas' observation that it was not incumbent to the ISP to seek independent verification of allegations[54] is reminiscent of the statutory qualification that the conditions to the "safe harbour" provisions are not to be taken as requiring an ISP to monitor its service or to seek facts to indicate infringing activity.[55] His Honour also draws on the prescribed "take down" notice in the "safe harbour" provisions[56] as a "useful illustration" of what an ISP might reasonably expect to receive from a copyright owner who asserts the provider's internet facilities are being used for copyright infringement.[57]

Most worrying, however, is Justice Emmett's analysis of reasonable steps at [210] (see above), which reads like a thinly-veiled reference to his Honour's preferred form of "warning, suspension and termination" scheme.[58] Given that other jurisdictions like France, the United Kingdom and New Zealand, have adopted or are adopting legislative schemes to address online copyright infringement (and not without controversy), it is strongly open to question whether the common law doctrine of authorisation should be shaped to apply to ISPs in the prescriptive manner suggested by his Honour Justice Emmett.[59]

Furthermore, with respect, there are three reasons why their Honours' drawing on the "safe harbour" provisions is inappropriate. First, as the trial judge observed, the relationship between the doctrine of authorisation and the "safe harbour" provisions is one-way:

---

47 *iiNet*, [780] (Nicholas J).

48 *iiNet*, [477] (Jagot J).

49 Part 11, Schedule 9, *US Free Trade Agreement Implementation Act 2004*.

50 Sections 116AC to 116AF, *Copyright Act*.

51 *iiNet*, [264]-[272] (Emmett J), [520]-[526] (Jagot J) and [803]-[806] (Nicholas J).

52 *iiNet*, [189] (Emmett J).

53 *iiNet*, [417] (Jagot J).

54 iiNet, [764] (Nicholas J).

55 Except to the extent required by a standard technical measure in a relevant industry code: s 116AH(2), *Copyright Act*.

56 Reg 20I and Schedule 10, Part 3, *Copyright Regulations 1969.*

57 *iiNet*, [760]-[761] (Nicholas J).

58 See Kim Weatherall, 'A few thoughts on iiNet FFC decision' (17 March 2011) *Fortnightly Review* at URL: http://fortnightlyreview.info/2011/03/17/a-few-thoughts-on-iinet-ffc-decision/.

59 The *iiNet* case can be contrasted with the recent High Court of Ireland decision in *EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd* [2010] IEHC 377 (Charleton J) (***EMI v UPC***), which was decided on very similar facts. The case was not run on authorisation, but on s 40(4) of the Irish *Copyright and Related Rights Act 2000*. At [119]-[129], Charleton J considers the approaches adopted in other jurisdictions. In holding that s 40(4) of the Irish Act does not provide a proper basis for prescribing a "warning, suspension and termination" scheme, his Honour states (at [86]):

"For the Court to pursue the course of granting an injunction on the basis not of law but of economic abuse or moral turpitude would lead the Court beyond the threshold of the judicial arm of government and into legislation. It would undermine respect for the rule of law: for *no one would know quite what the rule of law might be if it depended on attitudes forged through legal argument in individual cases as to what was acceptable conduct*." (emphasis added)

[Reasonable implementation of a repeat infringer policy] may be evidence in favour of a finding that the [carriage service provider] did not authorise the infringement of copyright… [But] the reverse is not true. That is, failure to comply with the requirements of the safe harbour provisions ***cannot*** be relevant and is not evidence that goes to a finding that a [carriage service provider] is liable for copyright infringement, since this would defeat the voluntary nature of the safe harbour provisions. Parliament has implemented a voluntary inducement, which, if not taken up, cannot, per se, be used as evidence that a [carriage service provider] has authorised infringement.[60]

It does not follow, in the author's view, from a legislative intent to create a voluntary industry scheme, and the subsequent breakdown of industry negotiations,[61] that Parliament therefore must have intended to amend the doctrine of authorisation for ISPs and to compel them to unilaterally assume a "warning, suspension and termination" scheme.

the Full Court reversed the trial judge's holding that iiNet could take advantage of the protection afforded under the "safe harbour" provisions.

Secondly, and as a corollary, if the doctrine's duty to take reasonable steps to prevent infringement compels an ISP to adopt and reasonably implement a "repeat infringer policy", there is no room left for the operation of the "safe harbour" provisions with respect to the provision of internet access. In other words, if the condition to limitations on remedies ***becomes*** the condition to non-liability, the limitations themselves become superfluous.

Thirdly, drawing on the "safe harbour" provisions led Justices Emmett and Nicholas to question the level of knowledge of infringement raised by the film companies' notices of alleged infringement. The majority took the view that the film companies' notices were deficient because they did not contain verification of the data and its collection methodology. However, as Justice Nicholas accepted, those notices must have given the ISP reason to suspect that such infringements had occurred.[62] His Honour then appears to draw a distinction between knowledge and reason to suspect, a distinction which, with respect, was not drawn by Justice Gibbs in *Moorhouse* ("*…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…*").[63]

Significance for online copyright infringement

Ultimately, the significance of the ***iiNet*** decision may lie in its power to compel copyright owners and the internet industry to resume their negotiations. iiNet may have won the case, but it is clear that the film companies have gained significant leverage with which to negotiate. The film companies have since announced they have applied for special leave to appeal to the High Court.[64] Unsurprisingly, the Internet Industry Association announced shortly after the Full Court's decision that it was accelerating the development of an industry code.[65] iiNet has itself proposed the establishment of an independent body to investigate infringements, to issue warning notices and to seek fines and other remedies, similar to the HADOPI model in France.[66] The Attorney-General has also announced that the Government will be looking closely into the outcomes of any industry discussions.[67] Failing industry agreement, legislative intervention may be appropriate. In particular, as the above analysis shows, Parliament should give reconsideration to the confused interplay between authorisation and the "safe harbour" provisions.

Wen Hui Wu is a Lawyer in the Intellectual Property, Technology & Competition group at Corrs Chambers Westgarth.

60 *iiNet (No 3)*, [589] (Cowdroy J).

61 For the background to these failed negotiations, see *iiNet*, [277]-[284] (Jagot J).

62 *iiNet*, [763] (Nicholas J).

63 Ibid.; *Moorhouse*, 13 (Gibbs J) (emphasis added).

64 Australian Federation Against Copyright Theft Limited, press release (24 March 2011), at URL: http://www.afact.org.au/pressreleases/pdf/2011/AFACT%20Media%20Release%2024.3.11.pdf.

65 Internet Industry Association press release, 11 March 2011.

66 See iiNet position paper, 'Encouraging legitimate use of Online Content' (15 March 2011), 9 at URL: http://www.iinet.net.au/press/releases/201103-encouraging-legitimate.pdf. The HADOPI model ("*Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet*") is discussed in *EMI v UPC*, above n 60, [122].

67 Attorney-General, Robert McClelland, Address to the Blue Sky Conference on future directions in Copyright law, 25 February 2011, at URL: http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2011_FirstQuarter_25February2011-AddresstotheBlueSkyConferenceonfuturedirectionsinCopyrightlaw.

Communications Law at Melbourne Law School

Interested in honing your knowledge in communications law? Melbourne Law School offers an advanced understanding of the existing and developing law affecting the media and communications industries and its impact on the publication of information, ownership, services and technology.

The Graduate Diploma in Communications Law is one of 32 courses from 20 specialist legal areas offered as part of the Melbourne Law Masters and offers students a huge range of subjects taught by Australian and international experts. All of our communications law subjects are taught on an intensive basis over consecutive weekdays making it easy for busy professionals and interstate students to participate.

The program allows students to choose from a range of subjects including for 2011:

- Communications Law
- Competition and New Technologies
- Copyright Law
- Entertainment Law
- Free Speech, Contempt and the Media
- Information Technology Contracting Law
- Privacy Law

The next subject being taught is Copyright Law from 4 - 10 May taught by Professor Graeme Austin, (University of Arizona, United States), Ms Kimberlee Weatherall and Associate Professor David Brennan.

For further information, visit the Melbourne Law Masters website

www.masters.law.unimelb.edu.au/communicationslaw

Communications & Media Law Association Incorporated

The Communications and Media Law Association (**CAMLA**) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the tele-communications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in hard copy and electronic format and comments should be forwarded to the editors at editors of the Communications Law Bulletin at editors@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens Arthur Robinson
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

Please note the change to CAMLA details:

Email: camla@tpg.com.au
Phone: 02 9399 5595
Mail: PO Box 237
KINGSFORD NSW 2032

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association (**CAMLA**) which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

CAMLA Website

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

Application for Membership

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 9399 5595

Name:.....

Address: .....

Telephone: .....Fax: .....Email: .....

Principal areas of interest: .....

.....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ I Ordinary membership $130.00 (includes GST)

☐ Student membership $45.00 (includes GST)
(please provide photocopy of student card - fulltime undergraduate students only)

☐ Corporate membership $525.00 (includes GST)
(list names of individuals, maximum of 5)

☐ Subscription without membership $150.00 (includes GST)
(library subscribers may obtain extra copies for $10.00 each + GST and handling)

Signature: .....