Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

Foreign Direct Investment in Digital Media in China: Challenges and Opportunity

Adrian Fisher looks at the challenges and opportunities that come with foreign direct investment in digital media in China.

Foreign direct investment into the People's Republic of China (***PRC***) has traditionally been closely regulated. With the PRC's accession to the World Trade Organisation in 2001, the PRC Government has made moves to open up foreign investment in certain industries. However, foreign investment in traditional and new media industries remains a challenge. Indeed, direct investment in most forms of traditional media (e.g. print news, free to air commercial television and commercial radio) is strictly prohibited. Participation in the digital media space, whether by way of direct investment or the provision of content into the PRC, is more open but foreign investors still face challenges and the sometimes difficult task of obtaining regulatory approvals and licences to operate their businesses in the PRC.

This article summarises some of the regulatory obstacles that foreign companies may encounter when considering investment opportunities in the digital media space in the PRC, and the regulation of the delivery of foreign content into the PRC by way of satellite and Internet broadcast. It also discusses approaches that have been considered by foreign investors entering into the media market in the PRC.

Foreign direct investment regulation generally

When considering an investment into the PRC, the first consideration of the foreign investor should be the application of the *Catalogue of Industries for Guiding Foreign Investment* (the ***Catalogue***). The Catalogue categorises a number of business types as 'Encouraged', 'Restricted' or 'Prohibited' from a foreign investment policy perspective. Business types that are not listed on the Catalogue are considered 'Permitted'. The categorisation of business types in the Catalogue should guide foreign investors as to whether their desired investment is possible at all and, if it is, the restrictions and approvals that are required in relation to the investment.

As the name of the category suggests, a foreign entity may not invest in a business within an industry listed as 'Prohibited'. The Catalogue identifies a number of media-related business types as 'Prohibited', including news agencies and websites, publishing companies, radio and television stations, radio and television network infrastructure owners, radio and television program production companies and Internet service and 'cultural content' providers. This effectively captures all traditional media types and a variety of digital media businesses.

If a business type is 'Restricted', then a foreign entity must obtain approval from the PRC's Ministry of Commerce at either the State or local level. The level of approval required will depend on the value of the investment. If the investment is worth more than US$50,000,000, approval of the Ministry of Commerce must be obtained at the State level. If the investment is worth less than US$50,000,000, approval must be obtained at the local branch of the Ministry of Commerce, which tends to be a less difficult and time-consuming process. The Catalogue identifies a number of media-related business types as 'Restricted', including radio, television and movie production projects, operation of movie theatres and distribution of audio and video products. If a foreign entity chooses to invest in such 'Restricted' media-re-

Volume 30 Nº 2
September 2011

Inside This Issue:

Printing & Distribution: BEE Printmail
Website: www.camla.org.au

Contents

lated businesses, it must do so by way of a joint venture investment or cooperation with a PRC entity, which in some cases must have a controlling interest in the joint venture vehicle.

A foreign entity must also obtain the approval of the Ministry of Commerce for investments in 'Encouraged' or 'Permitted' business types, however, the monetary thresholds for approval are much higher. Only investments worth more than US$300,000,000 require State level approval. Foreign investors need to obtain local approval for investments worth less than US$300,000,000. The significance of an investment being categorised as 'Encouraged' is that such investments will generally attract tax subsidies and certain preferential treatment. The current Catalogue does not identify any media-related businesses as 'Encouraged'.

An ICP will be liable not only for the content that it transmits via its website, but also for content that any of its users transmit via its website.

The Catalogue is a live document and was last updated in 2007. The PRC Government is currently reviewing the Catalogue and has issued a revised draft which is expected to be approved in the coming months. From a media perspective there are a number of relevant changes, one of the most interesting being that the provision of music over the Internet has been specifically excluded from the 'Prohibited' category, signalling a potential easing of foreign investment restrictions in the growing online music streaming industry.

Delivery of foreign content by satellite: landing rights

The distribution of foreign television channels by satellite to the PRC is regulated principally under the *Measures for the Administration of the Landing of Overseas Satellite Television Channels* (the ***Satellite TV Measures***) which is administered by the State Administration of Radio, Film and Television (***SARFT***). Foreign satellite television signals may only be broadcast, or 'land', in the PRC with the approval of SARFT. Approved broadcasts are generally limited to hotels that have three or more stars and restaurants, residences and offices that are designated as being 'foreign-related' (e.g. expatriate workers' compounds). Landing rights are generally granted for a one year period and must be renewed annually by application to SARFT.

The Satellite TV Measures outline various technical and content requirements for approved foreign satellite television signals, including that the signal must be transmitted by an 'institution designated by SARFT' and that the broadcast content must not threaten the sovereignty, honour or interests of the PRC or otherwise place the security or stability of the PRC at risk. The Satellite TV Measures also impose numerous continuing obligations on the foreign satellite television channel provider. As an example of these continuing obligations, all corporate and management changes in the channel provider must be previously agreed with the institution that SARFT has designated as the channel's PRC agent.

The Satellite TV Measures require that the foreign entity seeking landing rights must actively assist in the landing of Chinese radio and television programs overseas. This provision seems to have been applied in at least two cases: Time Warner and News Corporation's Fox TV both commenced broadcasting CCTV content into the United States soon after AOL Time Warner and News Corporation's Star TV were both respectively granted landing rights into southern China in the early part of the last decade.

Delivery of content by Internet: ICP licensing

In 2000, the PRC Government approved the *Administrative Measures on Internet Information Services* (the ***ICP Measures***) which regulates the provision of content (referred to as 'information services' in the ICP Measures) via the Internet. The ICP Measures prohibit anyone from providing content via the Internet to end-users in the PRC for money or 'compensation' without a permit from the relevant provincial telecommunications regulator. This permit is generally referred to as an Internet content provider or ICP licence. It is unclear from the language of the ICP Measures whether a service that provides content to end-users for free (such as YouTube) but makes money from advertising or other means is a service for 'compensation'. However, the fact that Google is required to have an ICP licence (which was most recently renewed on 7 September 2011) indicates that the PRC Government may view such services as being for 'compensation'.

If an entity is able to obtain an ICP licence, it will then have continuing obligations relating to the content that it produces, reproduces, distributes and disseminates, including that such content must not impair national security, jeopardise national unity, damage the reputation or interests of the PRC, disturb the social order or damage social stability, insult or slander a person or infringe on a person's legal rights.

An ICP will be liable not only for the content that it transmits via its website, but also for content that any of its users transmit via its website. So, for example, if a user of an ICP's website was to use the website's services to disseminate content that infringes the copyright of a third party, the ICP would be required under the ICP Measures to immediately discontinue the transmission of such information, keep records of the transmission and report on the transmission to the PRC authorities. A failure to comply with this obligation could lead to the revocation of the ICP's licence to operate its website.

Approaches to investment in the PRC: VIE structures

In recent years, many foreign companies seeking to invest in businesses in which foreign direct investment is not generally permitted have explored alternatives to a direct equity investment in the target business. An approach that has become increasingly popular (particularly in the Internet / new media space) has been to set up a PRC business through a variable interest entity, or VIE, structure. Under a typical VIE structure, a domestic PRC company (the equity in which is owned by PRC nationals) is established to carry on the restricted business operation and hold any necessary licences (e.g. ICP licences). The foreign investor, who holds no equity interest in the VIE, will enter into a series of contracts with the VIE under which the foreign investor is given effective control of the VIE. Through these controlling contracts, the economic benefit of the VIE's business in the PRC will generally flow through the VIE and back to the foreign investor.

A key characteristic of the VIE structure is the ability to acquire the shares in the VIE at any time. In practice, this option would only be exercised by the foreign investor if there was an easing of any restriction on foreign direct investment in the relevant business, or if the VIE has acted inconsistently with the foreign investor's interests and the foreign investor wishes to take back and wind-up the VIE.

The VIE structure was pioneered by PRC new media companies such as social networking and portal giant Sina.com and the PRC's largest search engine, Baidu. Putting in place VIE structures has enabled these companies, and many other PRC companies operating in sensitive sectors, to list on foreign exchanges (particularly in the United States) and raise foreign capital where they may otherwise not be able to do so. Various foreign companies have adopted this approach when investing or establishing their own businesses in the PRC.

The PRC Government has not yet sought to regulate, restrict or prohibit the use of the VIE structure, although it is arguably an illegal method to circumnavigate express prohibitions on direct foreign investment. However, the PRC Government has recently indicated that it is aware of the increased use of, and willing to regulate where necessary, VIE structures. On 25 August 2011, the PRC Government released regulations that supplemented a national security review regime that had been promulgated in February 2011. The national security review regime effectively requires an additional review of proposed foreign acquisitions of domestic PRC companies where such acquisitions may have an effect on national security in areas including technology. The PRC Government's latest regulations clarify that this national security review mechanism applies not only to foreign direct investment but also to transactions that result in foreign entities having effective control of domestic PRC entities, such as VIEs. This seems to be a clear message from the PRC Government that it will regulate VIE structures where necessary and desirable to protect the interests of the PRC. The practical implications of these new regulations remain to be seen.

Investors looking at opportunities in the PRC should carefully consider how their intended core business activities in the PRC are characterised under the Catalogue, and whether they should or need to team up with an appropriate local PRC entity in implementing their proposed business structure. Building productive relationships with PRC regulators will be an important factor for any entity considering an entry into the PRC, as all investments require initial and most often continuous regulatory approvals and oversight.

Challenges and opportunities

This article has considered some of the main regulations in the PRC relating to foreign direct investment and the delivery of foreign content into the PRC. It is important to note, however, that there are many other regulations of varying significance and application that will apply to a media business in the PRC. For example, if an investor is successful in obtaining an ICP licence, it may need to obtain approvals from other regulatory authorities in the PRC depending on the nature of the content being delivered. It is always prudent to seek independent advice on how the regulatory environment in the PRC applies to a particular investment.

Investors looking at opportunities in the PRC should carefully consider how their intended core business activities in the PRC are characterised under the Catalogue, and whether they should or need to team up with an appropriate local PRC entity in implementing their proposed business structure. Building productive relationships with PRC regulators will be an important factor for any entity considering an entry into the PRC, as all investments require initial and most often continuous regulatory approvals and oversight.

There are still opportunities for those foreign companies that are able to successfully navigate their way through the complex regulatory environment in the PRC. While there have been controversies in the United States relating to accounting practices of recently floated Chinese companies, business in the online content streaming space appears to be booming, with the video services provided by companies such as Youku, Tudou and PPTV becoming increasingly popular and (by all publicly available accounts) profitable. There also appears to be increased opportunity in the online music streaming space with Baidu recently signing a major rights deal with Sony, Universal and Warner for Baidu's free online music streaming service 'ting!', and the PRC Government signalling that it will ease foreign direct investment restrictions for online music streaming services.

Although there are great challenges in implementing a potential investment in the PRC, for those companies that are willing to start small, take a long term outlook and persist in building their business and regulatory relationships in the PRC, there is potentially great reward.

Adrian Fisher is a Senior Associate in the Technology, Media and Telecommunications practice group at Allens Arthur Robinson and is based in China.

The Twentieth Century Fox v BT Decision: A New Development in the Debate About ISP Obligations to Prevent Copyright Infringement

Donna Short and Hazel McDwyer consider the recent decision in Twentieth Century Fox Film Corp and Others v British Telecommunications plc and its potential implications in Australia.

In a recent English High Court case, *Twentieth Century Fox Film Corp and Others v British Telecommunications plc*,[1] the movie industry successfully obtained an injunction against British Telecommunications (***BT***), the UK's largest ISP, to stop the unauthorised downloading of movies from a website. This was a test case taken by the movie industry and provides an interesting insight into the issue of whether an ISP should be required to block or impede access to users who are infringing copyright.

As a result of the decision, BT must utilise a blocking system to block a website that enables users to download content infringing the studios' copyright.

As a result of the decision, BT must utilise a blocking system to block a website that enables users to download content infringing the studios' copyright.

This UK case is of particular interest in light of the iiNet case[2] in Australia in which special leave has recently been granted to Roadshow Films to appeal the decision of the Full Federal Court to the High Court.

Background - Twentieth Century Fox v Newzbin

The *BT* case followed an initial High Court injunction obtained by Twentieth Century Fox and other movie studios (***Studios***) against Newzbin Limited in 2010[3] (***20C Fox v Newzbin***).

The Studios brought an action for copyright infringement arising from the operation of a website, www.newzbin.com, (***Newzbin1***). Newzbin1 was a part of an internet system called Usenet which acted as a modern day equivalent of a public bulletin board. Usenet supports text content and any non-text (eg binary) content (such as films and software). Usenet users can upload or post messages to the system or download messages from the system.

Newzbin1 described itself as the '*most comprehensive Usenet search that exists on the internet*'.[4] It claimed to be 'content agnostic' as it was designed to index the entire content of Usenet. The Newzbin1 site focused on binary content. It stored information about films, television programs and other works. Newzbin1 had two levels of membership - free basic membership and premium membership. Premium members paid a fee and could download content on files that could be sorted using 'NZB' files on Newzbin1. The NZB files allowed premium members to obtain all of the Usenet messages and reassemble the original binary work so that the final product was an entire movie or TV show. Were it not for the NZB files, it would be a long and laborious process for a user to download all of the binary content to watch a film.

In 20C Fox v Newzbin, Justice Kitchin held that Newzbin Ltd had infringed the Studios' copyright by authorising premium members to make infringing copies of the Studios' films. He therefore granted injunctions against Newzbin Ltd restraining it from infringing the Studios' copyright in relation to their repertoire of films and TV programmes.

Newzbin2

Newzbin Ltd subsequently went into voluntary liquidation and the Newzbin1 website ceased to operate shortly after 17 May 2010. However, around 28 May 2010, a 'Newzbin2' website began operating at the same URL as Newzbin1. It was almost identical.

Newzbin2 was operated by unidentified individuals, acting under pseudonyms, and the servers hosting Newzbin2 were not located in the UK. Although BT did not provide any services to the operators of Newzbin2 and did not host the website, the Studios wanted BT to block access to the Newzbin2 website.

Cleanfeed

BT already had a blocking system in place that it used in conjunction with the Internet Watch Foundation (***IWF***). It was used to minimize the availability of content, specifically child sexual abuse images and criminally obscene adult content.

IWF produces a list of URLs that contain images of child abuse and BT has a system known as 'Cleanfeed' which disrupts access by its subscribers to URLs listed on the IWF list.

The Studios requested that BT implement similar measures with regard to the Newzbin2 website as those it already operated in relation to the URLs reported by IWF.

Justice Kitchin held that Newzbin Ltd had infringed the Studios' copyright by authorising premium members to make infringing copies of the Studios' films.

---

1 [2011] EWHC 1981 (Ch).

2 *Roadshow Films Pty Ltd and Others v iiNet Limited* [2011] FCAFC 23.

3 *Twentieth Century Fox Film Corporation and Others v Newzbin Ltd* [2010] EWHC 608 (Ch), [2010] FSR 512.

4 Ibid paragraph [17].

BT accepted that it was a service provider within the meaning of section 97A. However, it contended that the Court had no jurisdiction to grant the injunction

They sought an injunction under section 97A of the UK's *Copyright, Designs and Patents Act 1988* which relates to injunctions against service providers and implements part of the Information Society Directive.[5] Section 97A provides as follows:

> *' (1) The High Court … shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright….'*

BT accepted that it was a service provider within the meaning of section 97A. However, it contended that the Court had no jurisdiction to grant the injunction as:

1. there was no use of BT's service to infringe copyright;
2. it had no actual knowledge of the infringement;
3. it was contrary to Article 12(1) and Article 15(1) of the E-Commerce Directive;[6] and
4. it was contrary to Article 10 of the European Convention on Human Rights.

Use of BT's services to infringe copyright

The Studios contended that the users and operators of Newzbin2 were using BT's service to infringe their copyright. This was disputed by BT. After some discussion of the case law as to the meaning of an 'intermediary' within Article 8 of the Information Society Directive, Arnold J held that BT subscribers who are users of Newzbin2 do use BT's services to infringe the Studios' copyright. Users of Newzbin2 actively download material using BT's services. They are not merely passive recipients of such material as contended by BT[7].

He held that once it was concluded that users were using BT's services to infringe copyright, then it followed that the operators of Newzbin2 also did so.

Did BT have actual knowledge of the infringements?

The main issue in the BT case was whether BT had 'actual knowledge' of the infringements. The Studios contended that it was sufficient if BT had actual knowledge of the use of its services for infringing activity. BT argued that it must have actual knowledge of the use of its services to commit a particular infringement of a particular copyright work by a particular identified and identifiable individual.

There was some discussion of the fact that section 97A implements Article 8(3) of the Information Society Directive. Recital (59) of this Directive states that:

> *'in many cases, such intermediaries are best placed to bring such infringing activities to an end. Therefore…rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network.'*

This indicated to Arnold J that the purpose of Article 8(3) of the Directive, and hence section 97A, is to enable an injunction to be granted against a service provider that 'carries' an infringement, as the service provider is best placed to bring the infringing activities to an end.

Arnold J held that '*what must be shown is that the service provider has actual knowledge of one or more persons using its service to infringe copyright… but it is not essential to prove actual knowledge of a specific infringement of a specific copyright work by a specific individual*'.[8]

In addition, he held that BT had actual knowledge of users and operators of Newzbin2 using its services to infringe copyright on a large scale and in particular infringe the copyright of the Studios in large numbers of their films and television programmes.[9] Therefore, the Court found it had jurisdiction to grant the injunction against BT.

Order contrary to Article 12(1) and Article 15(1) of the E-Commerce Directive

Article 12(1) of the E-Commerce Directive relates to the circumstance in which a service provider acts as a mere conduit of information. A service provider is not liable where it does not initiate or select the receiver of the transmission or select or modify the information in the transmission. It was common ground that BT was protected from liability for infringement. However, BT also argued that the injunction would contravene Article 12(1). This argument was not successful and it was held that the protection accorded by Article 12(1) to would not preclude orders requiring service providers to disable access to illegal information.

Article 15(1) of the E-Commerce Directive provides that member states shall not impose a general obligation on service providers to monitor the information they transmit or store. BT argued that the injunctions sought amounted to such a general obligation to monitor.

However, Arnold J, citing *L'Oréal v eBay*,[10] held that the order did not require BT to engage in active monitoring of all data of the website's customers to prevent future infringement via that website. He held that the order simply required BT to block, or at least impede access to the Newzbin2 website by automated means. Further, he held that to the extent that this amounts to monitoring, it is actually a specific obligation rather than a general one of the kind proscribed under Article 15(1).

Arnold J held that BT subscribers who are users of Newzbin2 do use BT's services to infringe the Studios' copyright. Users of Newzbin2 actively download material using BT's services. They are not merely passive recipients of such material as contended by BT[7]

---

5 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

6 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

7 Above n. 1 paragraph [108].

8 Above n.1 paragraph [148].

9 Ibid paragraph [157].

10 Case C-324*/09 L'Oréal SA v eBay International AG.*

the purpose of Article 8(3) of the Directive, and hence section 97A, is to enable an injunction to be granted against a service provider that 'carries' an infringement, as the service provider is best placed to bring the infringing activities to an end

Scope of the injunction to be granted

BT submitted that the scope of the injunction should not extend beyond the film and television programmes in which the Studios had rights or to prevent its subscribers from visiting any part of the Newsbin2 website for any purpose.[11]

In *20C Fox v Newzbin*, Kitchin J had limited the injunction to the copyright in the Studios' repertoire only and would not extend it to that binary and text material in respect of which the Studios did not have rights.

Arnold J noted that it is common for rightholders such as Phonographic Performance Ltd to be granted injunctions over their entire repertoire even though infringement of a small number of copyrights has been proved.

On the evidence in this case, it was clear that the Studios' rights were being infringed on a massive scale through Newzbin. The Judge also believed that other rightholders would also be supportive of the action. He also held that the instances of BT subscribers using Newzbin for non-infringing purposes were de-minimus. Therefore, he granted the injunction requiring BT to block Newzbin being accessed via its services.

BT had also argued that there were technical measures that users could adopt to circumvent the blocking. However, for a number of reasons, Arnold J was not persuaded that the order would be ineffective as a result.[12]

Arnold J therefore granted orders broadly as requested by the Studios, namely, that BT would use technology to enable IP address blocking and DPI based blocking in respect of the Newzbin1 and Newzbin2 websites.[13]

Conclusion

This case provides an interesting alternative means of addressing copyright infringement taking place on the internet through ISPs. It sets a precedent in the UK to ensure that ISPs will assist content owners with the protection of copyright over the internet. It will be welcomed by owners of copyright, but it may lead to further cases being brought against ISPs.

It is also one alternative to graduated response regimes, such as the three strikes rule, that are being instigated in various countries around the world.

There are a number of issues which have been widely discussed regarding ISPs blocking individual users from having access to the internet because they have engaged in copyright infringement by file sharing. For instance, it can be difficult to ascertain who in a household is carrying out the infringement. There are also issues regarding the defences to such infringements such as fair dealing.

The cost of implementing such systems is also an issue. Blanket blocking of websites in the manner granted via the *BT* case is an alternative means to try to stop such infringing activity, particularly where the operator of the website is difficult to identify.

No doubt, this case will be reviewed with interest in Australia in light of the *iiNet* case[14] where special leave has recently been granted to Roadshow Films to appeal the decision of the Full Federal Court to the High Court.

The High Court Special Leave application[15] raises several points including whether the Full Federal Court erred in:

1. its application of the principles of authorisation from *Moorhouse*;[16]
2. respect of its findings regarding iiNet's knowledge of the infringements; and
3. finding that iiNet was not provided with reasonable notice of the infringements (via robotic notices).

The analysis of actual knowledge in the BT case may be of interest in respect of the question of iiNet's knowledge in the High Court appeal.

The outcome in the *iiNet* case will be particularly interesting in light of the approach taken in the UK with respect to Newzbin1 and Newzbin2. The High Court appeal in the *iiNet* case is expected to be heard by the end of 2011.

Donna Short is a partner and Hazel McDwyer is a senior associate at Henry Davis York.

the instances of BT subscribers using Newzbin for non-infringing purposes were de-minimus. Therefore, [Arnold J] granted the injunction requiring BT to block Newzbin being accessed via its services

11 Above, n.1, paragraph [179].

12 Ibid paragraphs [193] to [198].

13 Ibid paragraphs [11] and [12].

14 Above n 2.

15 *Roadshow Films Pty Ltd & Ors v iiNet Limited* [2011] HCATrans 210 (12 August 2011).

16 *University of New South Wales v Moorhouse and Angus & Robertson (Publishers) Pty Ltd* (1975) 133 CLR 1.

Hacking By Australian Journos? A Risky Proposition

Nick Sinclair considers how existing laws in Australia would apply to electronic hacking by the local media.

Introduction

For much of July, the now defunct *News of the World* (***NOTW***) was just that. The revelations leading to the closure of the 168-year-old London tabloid reverberated around the globe, and were pursued with particular zeal in Australia, not least by those who favour an overhaul of privacy laws.

The events in the United Kingdom have prompted questions about the practices of Australian media outlets and their reporters.[1] Amongst some in the political class, these questions have led to calls for government inquiries into media regulation, including media ownership.[2] Among lawyers (including the Minister for Justice, Brendan O'Connor), the NOTW saga has triggered a fresh round of debate about the merits of a tort of invasion of privacy.[3] Although no such cause of action is currently available in any Australian jurisdiction, either under statute or at common law, a 2008 Australian Law Reform Commission report[4] which recommended statutory recognition of a cause of action for serious invasions of privacy is now being dusted off and reconsidered.

Notwithstanding the potential merits of such a reform (particularly as it might relate to unintentional conduct by large organisations in the course of handling of personal data), there has been little analysis of existing laws in Australia and how they might apply if Fleet Street hacking techniques were ever deployed in this country. This article explores the existing sanctions and remedies that would apply to electronic hacking conducted by or on behalf of media outlets in Australia. Despite the media exemption in the *Privacy Act 1988* (Cth),[5] Australian reporters are not immune from prosecution for intentionally intercepting or accessing private communications. This article also proposes a modest amendment to State and Territory criminal codes, which would better safeguard electronic files stored on a computer.

Telecommunications

The *Telecommunications (Interception and Access) Act 1979* (Cth) (the ***Interception and Access Act***) broadly prohibits the interception of communications,[6] except where authorised in special circumstances.[7]

Section 7 of the Interception and Access Act deals with communications 'passing over a telecommunications system', where 'passing over' is defined to cover communications that are in transmission.[8] Section 7 would apply to sophisticated methods of electronic interception to listen in on telephone calls in real time and/or record them for subsequent replay.

there has been little analysis of existing laws in Australia and how they might apply if Fleet Street hacking techniques were ever deployed in this country

The methods used in the NOTW saga were far more rudimentary. Essentially, they were designed to take advantage of security weaknesses around stored voice mail messages. The techniques described as 'hacking' often consisted of nothing more than obtaining the target individual's mobile phone number, dialling a general voice mail retrieval service and entering a default PIN code in the hope that the target had not already adopted a new PIN.[9]

The unauthorised access of a target's voicemail messages is not caught by section 7 of the Interception and Access Act because like SMS messages and email, a voicemail, for the purposes of the Interception and Access Act, stops passing over a telecommunications system when 'it becomes accessible to the intended recipient of the communication'.[10] Nonetheless, in 2006 the federal government amended the Interception and Access Act,[11] making it an offence to access 'stored communications' (including SMS, email and voicemail) without the knowledge of the sender or the intended recipient of the stored communication.

Section 108 of the Interception and Access Act, which makes the unauthorised access of stored communications an offence, stipulates that the penalty for breach can include up to two years' imprisonment.[12] Of particular interest to editors, publishers and others who

1 To date, there have been no serious suggestions, let alone evidence, of phone hacking (or similar conduct) by employees or contractors of any Australian media outlet.
2 See, eg, Shane McLeod, "Bob Brown pushes for media inquiry" (14 July 2011), ABC News <http://www.abc.net.au/news/2011-07-14/bob-brown-calls-for-media-review/2794992> at 6 September 2011.
3 On 21 July 2011, the Minister for Justice cited the NOTW scandal in announcing that the Gillard Government would issue a public issues paper "canvassing the prospect of introducing a statutory cause of action for serious invasions of privacy": "A right to privacy in Australia", Minister for Home Affairs/Minister for Justice/Minister for Privacy and Freedom of Information (21 July 2011) <http://www.ministerhomeaffairs.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2011_ThirdQuarter_21July2011-ArighttoprivacyinAustralia> at 6 September 2011.
4 Australian Law Reform Commission, *"For Your Information: Australian Privacy Law and Practice"*, Report 108 (12 August 2008).
5 *Privacy Act 1988* (Cth), s7B(4).
6 *Telecommunications (Interception and Access) Act 1979* (Cth) s7.
7 These include law enforcement and certain acts done by employees of carriers in the course of their duties.
8 *Telecommunications (Interception and Access) Act 1979* (Cth) s5F. "Communications" is defined to include "conversation and a message, and any part of a conversation or message", whether in the form of: (i) speech, music or other sounds; (ii) data; (iii) text; (iv) visual images, or (v) signals, "in any form or in any combination of forms". A "telecommunications system" is a telecommunications network within Australia (or partly within Australia), including equipment, a line or other facility connected to such network.
9 Default PIN codes are usually '1234' or '0000'.
10 *Telecommunications (Interception and Access) Act 1979* (Cth) s5F.
11 Via the *Telecommunications (Interception) Amendment Act 2006* (Cth)
12 In respect of live communications, under s105 it is an indictable offence (punishable by up to 2 years imprisonment) to contravene s7 by intercepting communications that are passing over a telecommunications system.

the NOTW saga has triggered a fresh round of debate about the merits of a tort of invasion of privacy.

manage journalists is the provision in section 108 of the Interception and Access Act that extends the offence to a person who 'authorises, suffers or permits' another to access stored communications, and to anyone who 'does any act or thing' that enables them or another to gain access.[13]

Supplementing these criminal sanctions are the civil remedies in the Interception and Access Act,[14] which empower both civil and criminal courts to grant remedial relief to an 'aggrieved person' whose communications (including stored communications) are accessed in breach of the Interception and Access Act. Section 165, which sets out the civil remedies for the unlawful access of stored communications, includes a non-exhaustive list of orders that a court can make. These include an order for damages (specifically including punitive damages),[15] injunctive relief and an order to pay the aggrieved person 'total gross income derived by the defendant as a result of the access or communication, as the case requires'.[16] A plaintiff can obtain the benefit of these civil remedies in relation to both the unlawful access of communications and the subsequent communication of information obtained from such access.[17]

These civil remedies allied with possible criminal sanctions make for a particularly robust legislative framework, which would likely apply if NOTW's methods were replicated in Australia. Especially significant, in the event of interception of private communications by a media organisation, is the possibility of an order to pay an aggrieved person an amount equivalent to the income earned by the defendant from accessing the communication (in addition to general and punitive damages).

A harsher range of consequences for anyone found to have illegally intercepted communications or accessed stored messages is difficult to imagine. For Australian media organisations, the Interception and Access Act should act therefore as a powerful deterrent of the type of behaviour that brought down NOTW.

Computer Hacking

Rudimentary as NOTW's techniques were, it is easy to imagine a modern-day reporter trying their hand (or at least engaging someone else in the task) at something more sophisticated than simply hacking into voicemail message banks. The application of the provisions of the Interception and Access Act detailed above to computer hacking would depend primarily on whether the accessed information was contained in a stored communication or was passing over a telecommunications system (in, for example, an email).

In many if not most instances of computer hacking, it is likely that the Interception and Access Act would apply, given that communications passing over the internet, and those stored on an internet service provider's equipment, fall within its ambit.

But what about a simple Word or PDF document, saved on an individual's hard drive but never transmitted over a telecommunications system or stored on an ISP's equipment, which is somehow hacked into and accessed by a reporter (or anyone else for that matter)? In most parts of Australia, this kind of hacking would be unregulated. The computer offences contained in the Commonwealth Criminal Code[18] do not prohibit access per se. The same is true in the equivalent state legislation in New South Wales, Victoria, the Australian Capital Territory and South Australia.[19] As the Australian Institute of Criminology has explained, '[i]n this scheme there has been a deliberate choice to peg criminal liability at four levels based on the defendant's intent or the way access to data is secured on a computer'.[20] In other words, under the Criminal Code and the equivalent State laws, a computer offence is not committed unless the act of hacking is accompanied by some other intent or motivation (for example, the intent to commit some other serious offence against a law of the Commonwealth, or of a State or Territory, by the access, modification or impairment of the computer in question).[21]

As illustrated by the example of a hacked Word or PDF document, there appears to be a gap in the law in Australia, at least outside of the Northern Territory.[22]

Section 276B of the *Criminal Code Act* (NT) is unique in Australia. It prohibits the unlawful access of data held in a computer with intent to 'gain benefit or advantage, whether personally or for a third party'.[23] This provision would likely apply to computer hacking

The application of the provisions of the Interception and Access Act detailed above to computer hacking would depend primarily on whether the accessed information was contained in a stored communication or was passing over a telecommunications system (in, for example, an email)

---

13 *Telecommunications (Interception and Access) Act 1979* (Cth) s108(1)(a)(ii) and (iii).

14 *Telecommunications (Interception and Access) Act 1979* (Cth) ss107A and 165.

15 *Telecommunications (Interception and Access) Act 1979* (Cth) s165(10).

16 *Telecommunications (Interception and Access) Act 1979* (Cth) s165(7)(d).

17 Section 165 of the Interception and Access Act also provides for remedial relief where a person breaches s133 by communicating information obtained from the unlawful accessing of a stored communication.

18 *Criminal Code Act 1995* (Cth), Schedule – The Criminal Code, Part 10.7.

19 Each of these States has implemented a series of computer offences broadly similar to those added to the Commonwealth Criminal Code by the *Cybercrime Act 2001* (Cth): see *Crimes Act 1900* (NSW) Part 6; *Crimes Act 1958* (Vic) Part 1, Division 3, Subdivision 6; *Criminal Law Consolidation Act 1935* (SA) Part 4A; *Criminal Code 2002* (ACT) Part 4.2.

20 'High tech crime brief no. 5: Hacking offences', Australian Institute of Criminology (January 2005) <http://www.aic.gov.au/en/publications/current%20 series/htcb/1-20/htcb005.aspx> at 6 September 2011.

21 *Criminal Code Act 1995* (Cth), Schedule – The Criminal Code, s477.1(1)(d).

22 This is not to say that other remedies would not available under Australian law, depending on the circumstances in which the document was accessed. A victim in such a case might be able to prevent dissemination of the information in the document through an action grounded in unconscionability or the equitable doctrine of breach of confidence. The tort of trespass could also be an option in certain circumstances.

23 *Criminal Code Act* (NT), s276B(1).

under the Criminal Code and the equivalent State laws, a computer offence is not committed unless the act of hacking is accompanied by some other intent or motivation

by a journalist seeking private information, even if it fell outside the ambit of the Interception and Access Act.[24] The prescribed penalty in the NT is up to 10 years' imprisonment.

A move by the other States and Territories to adopt the NT's position on computer offences would be a modest reform in the face of fresh concerns about electronic hacking.[25] Given the small gap that currently exists in Australia vis-à-vis electronic privacy invasions by media, this may be a wiser course of action than holding out for a wide-ranging new tort of privacy.

Conclusion

Despite the possible merits of a comprehensive new tort of invasion of privacy, either statutory or at common law, Australian legislators and judges have been reluctant to pursue it. The reluctance may be explained by the limited constitutional protection of free speech in Australia. Not only does the existing range of laws provide a number of sanctions, remedies and safeguards (particularly against the sort of conduct canvassed in this article), but the concept of privacy is both fluid and nebulous, and not necessarily amenable to broad-brush legal reform.[26]

Australia is not out of step with other common law countries; indeed it seems there are almost as many legal approaches to privacy as there are jurisdictions. Since the *European Convention on Human Rights* was implemented in the UK by way of the *Human Rights Act 1998* (UK), British courts have certainly become more willing to award damages for invasion of privacy, albeit by broadening the equitable action for breach of confidence rather than recognising a new tort.[27] After years of competing judgments on the issue in the Canadian province of Ontario, a judge of the Superior Court recently held that 'there is no tort of invasion of privacy in Ontario'.[28] Although Ontario, like Australia, does not have a statutory tort (unlike several other common law provinces in Canada),[29] Whitaker J noted in *Jones v Tsige* that 'it cannot be said that there is a legal vacuum that permits wrongs to go unrighted – requiring judicial intervention'.[30] The case, which had no media connection, involved the access by a bank employee of a colleague's private financial records stored on a workplace computer, the plaintiff also being a customer of the bank in question (interestingly, if an Australian reporter accessed similar electronically-stored information, the case may fall into the legal gap identified above). The court squarely rejected the plaintiff's assertion that she would be without a remedy in the absence of a tort of invasion of privacy.[31]

US courts recognise four distinct strands of an invasion of privacy tort.[32] However, members of the High Court of Australia commented on US privacy law in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* as follows:

> *'Privacy law in the United States delivers far less than it promises, because it resolves virtually all these conflicts in favour of information, candour, and free speech. The sweeping language of [US] privacy law serves largely to mask the fact that the law provides almost no protection against privacy-invading disclosures.'*[33]

A minor tweak to existing statutes could adequately cover a small gap in the law that applies to electronic invasions, which in any event is already robust and potentially quite severe

Rather than reacting to the NOTW story in a manner that risks constraining local journalists – who are not shielded by protections such as those contained in the US Constitution – and possibly compromising free speech, proponents of Australian privacy law reform may wish to carefully consider the existing legal framework. A minor tweak to existing statutes could adequately cover a small gap in the law that applies to electronic invasions, which in any event is already robust and potentially quite severe.

Nick Sinclair is a lawyer in the Technology, Media and Telecommunications Practice Group at Allens Arthur Robinson.

---

24 Queensland (*Criminal Code 1899*, s408E), Western Australia (*Criminal Code Act Compilation Act 1913*, s440A) and Tasmania (*Criminal Code Act 1924*, Chapt XXVIIIA) each have unique computer offences unlike those in the NT and the other States and Territory. But none of the respective offences in those States would be as likely to apply to a journalist who hacked into private computer files which were not stored communications as the offence in the NT. Section 257D of Tasmania's *Criminal Code Act 1924*, which prohibits any computer hacking "without lawful excuse", is the most robust; but the lack of a definition for "without lawful excuse" creates uncertainty.

25 The Commonwealth would arguably be precluded from adopting such an amendment to its own Criminal Code, given that its Constitutional authority in relation to creating criminal offences is limited.

26 In extracurial remarks seven years after the High Court's decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, Chief Justice Gleeson remarked that "[t]he ground seems to me to be shifting under the concept of privacy... I wrote a judgment a few years ago in which I said there seemed to me to be certain things that were self-evidently private. I'm not so sure about that any more. When you look at the kind of information that people publish about themselves it makes you wonder": Nicola Berkovic, "Why Privacy isn't what it used to be," (22 August 2008) *The Australian* <http://www.theaustralian.com.au/business/legal-affairs/why-privacy-isnt-what-it-used-to-be/story-e6frg97x-1111117263398> at 6 September 2011.

27 Australian Law Reform Commission, *"For Your Information: Australian Privacy Law and Practice"*, Report 108 (12 August 2008) at 74.27-74.28.

28 *Jones v Tsige* 2011 ONSC 1475 at [57].

29 Including British Columbia, Saskatchewan, Manitoba and Newfoundland & Labrador: see Australian Law Reform Commission, *"For Your Information: Australian Privacy Law and Practice"*, Report 108 (12 August 2008) at 74.23.

30 *Jones v Tsige* 2011 ONSC 1475 at [53].

31 The judge suggested an alternative cause of action could have been found in Canada's *Personal Information Protection and Electronic Documents Act 2000*, which applies to the banking sector.

32 'Intrusion Upon Seclusion', 'Appropriation of Name or Likeness', 'Publicity Given to Private Life' and 'Placing a Person in False Light': *Restatement of the Law, 2nd, Torts, 1977* (US).

33 (2001) 208 CLR 199 at [119].

Cush v Dillon: A Boost for the Defamation Defence of Qualified Privilege in the Context of Inaccurate Communications

Sophie Dawson and Lucienne Cassidy examine the High Court decision in Cush v Dillon which confirms common law qualified privilege as an important defamation defence

In *Cush v Dillon*,[1] the High Court affirmed a decision by the NSW Court of Appeal confirming the strength of the common law qualified privilege defence in relation to inaccurate communications. This is important because many had doubted the strength of that defence after the High Court's decision in *Aktas v Westpac Banking Corporation Limited* [2010] HCA 25 (***Aktas***). The defence has an important role to play in protecting a plethora of day to day communications.

The common law qualified privilege defence applies where a communication is made by a person with a duty or interest in making it to a person with a reciprocal duty or interest in receiving it

The common law qualified privilege defence applies where a communication is made by a person with a duty or interest in making it to a person with a reciprocal duty or interest in receiving it. The defence can be destroyed if the person defamed can establish that the person who made the communication made it maliciously. Malice in this context means an improper purpose.

For a long time, the defence has been relied upon in a variety of contexts including, for example, in relation to employment references, employee management processes and reports of crimes, or suspected crimes, to law enforcement agencies.

The *Cush v Dillon* case concerns a communication made in a management context concerning allegations about the conduct of a board member and a manager. Appeals were brought by Ms Amanda Cush and Mr Leslie Boland, who alleged that they were defamed by Mrs Meryl Dillon. Ms Cush was the General Manager of the Border Rivers-Gwydir Catchment Management Authority (***CMA***) and Mrs Dillon and Mr Boland were both members of the CMA Board. Mrs Dillon held a meeting with the Chairperson of the CMA Board, Mr Croft, and it was at this meeting that the communication was made. At trial, the jury found that Mrs Dillon told Mr Croft that it was 'common knowledge among people in the CMA' that Ms Cush and Mr Boland were having an affair. The version of the conversation Mrs Dillon said she had with Mr Croft in relation to the affair was different to that found by the jury. Mrs Dillon gave evidence that at the time the conversation occurred she considered that the veracity of the information she had been given about the alleged affair was questionable. She accepted for the purpose of the proceedings that Ms Cush and Mr Boland were not having an affair.

The jury found that the statement conveyed a number of defamatory imputations. In defence, Mrs Dillon pleaded that she had made the statement on an occasion of qualified privilege. However, the trial judge considered that any protection based on privilege was destroyed by malice. The finding of malice was made on the basis of a finding by him that she knew the statement to be untrue. He considered it unnecessary to consider whether the occasion actually gave rise to privilege.

The High Court unanimously upheld the decision by the New South Wales Court of Appeal overturning the primary judge's finding. In three separate sets of reasons, all judges agreed that the defence of qualified privilege was available to Mrs Dillon and that the statement had the prima facie protection of the qualified privilege defence.

The court considered that before determining whether there had been malice, it was first necessary to apply the test of qualified privilege to determine whether the person had a duty to make the statement and whether the recipient had a corresponding interest in receiving it. The question of whether Mrs Dillon had a duty to communicate the existence of a *rumour* of an affair was not in issue in the High Court because the parties agreed that such a duty arose. However, the court made clear its view that such a duty did exist. French CJ, Crennan and Kiefel JJ held that:

> *'[T]he duty Mrs Dillon had in disclosing and the interest Mr Croft had in receiving the information concerning CMA staff-related matters, including the nature of the relationship between members of the Board and members of staff, gave rise to an occasion of privilege.'*[2]

In a joint judgment, French CJ, Crennan and Kiefel JJ described the requirement for reciprocity of duty and interest, as the '*hallmark of the common law defence of qualified privilege*',[3] holding that it is to be '*tested by the connection of the statement to the subject*.'[4] They noted that the duty arose in the case in light of three factors, namely

before determining whether there had been malice, it was first necessary to apply the test of qualified privilege

1 [2011] HCA 30.

2 Paragraph [23].

3 Paragraph [11].

4 Paragraph [19] citing *Adam v Ward* [1917] AC 309 at 320-321.

'*the positions of Mr Croft and of Mrs Dillon within the CMA, the nature and importance of the matters conveyed and the relationship of the defamatory statement to those matters*.'[5]

French CJ, Crennan and Kiefel JJ reinforced the public policy behind the defence:

> *'The defence of qualified privilege is based upon notions of public policy, that freedom of communication may in some circumstances assume more importance than an individual's right to the protection of his or her reputation.'*[6]

French CJ, Crennan and Kiefel JJ upheld the finding by Bergin CJ in Eq in the Court of Appeal that there was sufficient reciprocity between Mrs Dillon's duty and Mr Croft's duty because the rumour of the affair was 'intrinsically intertwined with' the concerns Mrs Dillon raised about the nature of the relationship between members of the Board and staff members and how complaints about the grievance process were dealt with. To have allowed Mr Croft to remain ignorant of the existence of the rumour would have been in breach of Mrs Dillon's duty as Board member.[7]

The court considered the appellants' submission that, while the occasion of privilege to communicate the existence of the rumour arose, the words 'common knowledge' used by Mrs Dillon gave the rumour 'the quality of a known fact' and in this way took the statement outside the 'umbrella of the applicable privilege'. The court unanimously rejected this submission. French CJ, Crennan and Kiefel JJ held that:

> *'It could not, in our view, then be suggested [by the appellants] that the communication of the fact of an affair was less relevant to the matters discussed than a rumour. The error inherent in the statement does not deny the privilege.'*[8]

Bell, Gummow and Hayne JJ also accepted that *'an inaccuracy in relation to the relevant subject matter will not necessarily render what was said irrelevant to the privileged occasion.'*[9] Heydon J reached the same conclusion in separate reasons.

This confirmation by the court of traditional, core qualified privilege principles is likely to provide some comfort to people concerned about the status of the defence after the High Court's decision in *Aktas*, in which a majority of the court (French CJ, Gummow and Hayne JJ, Heydon and Kiefel JJ dissenting) found that qualified privilege was not available where a bank had communicated a 'refer to drawer' notification to the payee of a cheque after making a mistake as to whether funds were available to meet it. This decision is also likely to provide comfort to employers, who routinely rely upon this defence in relation to communications about staff and management issues.

It is also significant that the court affirmed that it is necessary to determine whether an occasion of privilege exists *before* reaching any conclusion as to malice. French CJ, Crennan and Kiefel JJ held that before considering the issue of malice, an enquiry must be undertaken to determine the boundaries of the privilege; a statement that lies beyond those boundaries may then be capable of being malicious.[10]

French CJ, Crennan and Kiefel JJ stated the test for malice as '*the existence of an improper motive that causes the person to make the statement*.' Their honours confirmed that '*lack of belief in the truth of the statement, or even ill-will felt towards the person defamed*' will not be sufficient to destroy privilege. Rather, they held that it is necessary to show evidence '*that the making of the statement was actuated by improper motive*'. Ultimately, the court did not determine whether Mrs Dillon had been actuated by malice and ordered a new trial on that issue. [11]

Their honours noted that:

> *'Knowledge on the part of a defendant that a statement is untrue may be almost conclusive evidence of malice. This is because a person who knowingly publishes false and defamatory material will usually have an improper motive. A lack of belief in the statement may stand in a different category. But in neither event is there warrant for equating knowledge or lack of belief with actual malice.'*[12]

The defence of qualified privilege is based upon notions of public policy, that freedom of communication may in some circumstances assume more importance than an individual's right to the protection of his or her reputation.

Heydon J highlighted in his judgment that the defence of qualified privilege needs to be sufficiently robust to deal with differences between what the jury finds was said and what was in fact said. His Honour noted that the difference between what was found to have been said and what Mrs Dillon believed arose because the jury did not accept her version of the relevant conversation, and instead accepted a slightly different version. His Honour said that submissions by the plaintiff that the statement made was not sufficiently connected to the occasion of qualified privilege:

> *'[…] do not give sufficient significance to the difficulties a witness may have in giving a recollection of a small part of a long conversation long after the event, coupled with the possibility that a jury may choose for itself one among a number of available versions of the conversation. An account of why something – whatever precisely it was – was said may satisfy the two conditions for qualified privilege under discussion even though what the witness says was said does not correspond with what the trier of fact finds was said.'*[13]

There will now be a new trial dealing with the issue of whether or not the plaintiff can establish malice.

This judgment affirms the strength of common law qualified privilege in an employment context. It also confirms that the defence is sufficiently robust to apply in relation to inaccurate communications so long as they are relevant to the occasion of privilege and so long as there is no malice.

Sophie Dawson is a partner and Lucienne Cassidy is a graduate at Blake Dawson.

---

5 Paragraph [13].
6 Paragraph [12].
7 Paragraph [16].
8 Paragraph [23].
9 Paragraph [52].
10 Paragraph [15].
11 Paragraphs [28] to [30].
12 Paragraph [29].
13 Paragraph [59].

The Author's Guild et al v Google Inc. 05 Civ 8136 (DC)

Henry Fraser examines the Google Books decision and considers its potential implications for the digital copyright regime in Australia.

Introduction

The Author's Guild et al v Google Inc. 05 Civ 8136 (DC) (the ***Google Books Case***) is a class action case of authors and publishers against Google. Google entered into an agreement with a number of major US libraries in 2004 to digitise their collections. To date Google has copied more than 12 million books without the permission of their copyright owners. While Google had the permission of the libraries to undertake the copying, it did not have the permission of the copyright owners of the books and their contents. The plaintiffs brought the action in 2005, but after a period of discovery, representatives of the class of plaintiffs began settlement negotiations with Google in 2006. On October 28 2008, the parties filed a proposed settlement agreement, which received preliminary approval by the court. There was a multitude of objections to the terms of the settlement by class members after which the settlement was amended and filed for approval with the court on 13 November 2009.

The forward looking nature of the parties' proposal was of itself a strong reason for the rejection of the settlement

Under rule 23(e) of the *US Federal Rules of Civil Procedure*, the court may approve a settlement in a class action only if it determines that the settlement is "fair, adequate, and reasonable, and not a product of collusion". A number of parties intervened on both sides. Amazon.com, a high profile competitor of Google, argued against court approval of the settlement, and Sony argued for it. [1] In a judgment on 22 March 2011, Circuit Judge Denny Chin of the US District Court for the Southern District of New York rejected the proposed settlement.

This article summarises the reasons for Judge Chin's decision and considers the policy and implications of the Google Books Case on the reform and development of the digital copyright regime in Australia.

The terms of the proposed settlement

The proposed settlement would have given Google a non-exclusive licence to:

- continue to digitise books;
- sell subscriptions to an electronic database;
- sell online access to individual books; and
- sell advertising in the books,

as well as a number of other prescribed uses.

Google could display out-of print books without permission of their copyright owners, but the owners would be able to 'opt-out' by asking that their books be removed from, or not uploaded to, Google's registry. As for commercially available, 'in-print', books, Google could not use the books without the permission of their copyright owners.

Under the proposed settlement, Google agreed to pay 70% of net profits from the commercial exploitation of the books to the relevant rights holders. It agreed to set up a registry of rights holders for the administration of revenue, funding the registry with a US$34.5 million payment. It would appoint an 'independent Fiduciary' tasked with representing the interests of owners of unclaimed or 'orphan' works. Google would be bound to make commercially reasonable efforts to find the rights holders in these works.

In addition to the registry fund, under the settlement, Google would establish a US$45 million fund to pay rightsholders for the copying of their books. As a minimum, authors would receive US$60 per 'principal work' (such as a book) US$15 per 'insert' (such as an introduction or prologue to a book), and $5 per partial insert. If these payments could be covered by less than US$45 million, Google would distribute the remainder of the fund by giving a greater amount per work: up to US$300 per Principal Work, US$75 per entire insert, and US$25 per partial insert.

The Decision

Weighing the 'Grinell factors' – judicial cost-benefit analysis of settlement

In weighing up whether to approve the settlement, Judge Chin considered the 'Grinnell' factors, so named after the US case which set them down as the factors to consider in approving a class action settlement.[2] The factors include, among other things, the expense and time of litigation proceeding to judgment; the reaction of class members to the proposed settlement of their class action; and the reasonableness of settlement in light of likely outcome of litigation.[3]

Judge Chin held that of the nine 'Grinnell' factors, only the reaction of class members to the settlement provided adequate grounds for rejection of the settlement. Approximately 6800 members of the plaintiff class, including foreign authors, academic authors, and authors of 'inserts' objected to the settlement on the basis that it was against their interest. The structure of the arrangement brought the interests of some members of the plaintiff class into conflict with other members. For example, there would be little incentive for identified copyright owners to identify owners of orphan works because it would reduce the amount of money available for payments to them. In this case, class members would not only be settling past liabilities, by keeping silent, owners of copyrights would also be deemed to grant licence to Google for

1 Under the terms of the proposed settlement, see Objection of Amazon.com, Inc. to Proposed Settlement (Dkt. 206), *The Authors' Guild, Inc. et al v Google, Inc.*, 05-cv-8136(DC)(S.D.N.Y. Sept. 1, 2009); *Amicus Curiae* Brief of Sony Electronics Inc. in Support of Proposed Google Book Search Settlement (Dkt. 314), *The Authors' Guild, Inc. et al v Google, Inc.*, 05-cv-8136(DC)(S.D.N.Y. Sept. 8, 2009).

2 *City of Detroit v Grinnell Corp.*, 495 F.2d 448 (2d Cir. 1974).

3 *Authors Guild* at 14-15.

future exploitation of copyrights. This, said his Honour, was going too far, given the numerous objections.

That basis for objection was connected to a number of policy considerations that also bore against the settlement. At the heart of the objections and countervailing policy considerations were:

- the fact that the settlement went beyond the scope of the initial issues in contention and proposed forward looking arrangements;
- the arrangements operated on an 'opt-out' basis, rather than acknowledging that Google could not exploit copyrights until rightsholders had opted in; and
- the arrangements would give Google a significant market advantage over its competitors, in effect rewarding it for mass copying without permission.

Scope of the settlement – suitability for decision of the court

The forward looking nature of the parties' proposal was of itself a strong reason for the rejection of the settlement. Initially, when Google began copying books, it contemplated using 'snippets' for the purpose of searching and indexing. Google's defence to a copyright suit would have been that the provision of mere snippets fell under the broad US defence of fair use. However, if Google had sought to exploit full copyright works, as provided by the settlement agreement, there would have been no defence for the copying.[4] Judge Chin was concerned that proposed settlement did not simply release Google from liability in relation to its past acts and intentions but transferred rights in exchange for future conduct and future acts.[5] In that sense, its scope went beyond that of the issues in contention before the court.

In particular, Judge Chin was concerned about the scope of the arrangement of Google's management of orphan works. Given the scale of Google's enterprise, the settlement would effectively have set the standard for the digital exploitation of 'orphan works' (works whose copyright owners are not known), and put the administration of orphan works into Google's hands for the digital future. His Honour thought the establishment of broad policy and mechanisms for the guardianship and exploitation of unclaimed books was a matter more suited for the Congress than for the Court.[6]

Opt-out system

As well as giving power to Google over orphan works, Judge Chin observed that the settlement would in effect give Google the power to expropriate the rights of copyright holders without their consent. Copyright owners in out of print works would be deemed to have consented to Google's use of their works unless they gave notice to the contrary. His Honour said:

> *'A copyright owner's right to exclude others from using his property is fundamental and beyond dispute… It is incongruous with the purpose of the copyright laws to place the onus on copyright copyright owners to come forward to protect their rights when Google copied their works without first seeking their permission.'*[7]

For Judge Chin the opt-out proposal was too radical a departure from the basic premises of copyright law to be approved by the court.

Competition and 'Anti-trust' issues

If the settlement had stood, Google would have gained first mover advantage in the digital market, enabling it to establish a monopoly over the digital use of works it had copied. As Judge Chin put it:

> *'The [settlement] would grant Google control over the digital commercialization of millions of books, including orphan books and other unclaimed works. And it would do so even though Google engaged in wholesale, blatant copying without first obtaining copyright permissions. While its competitors went through the "painstaking" and "costly" process of obtaining permissions before scanning copyrighted books, Google by comparison took a shortcut by copyrighting anything and everything regardless of copyright status.'*[8]

Judge Chin was concerned that proposed settlement did not simply release Google from liability in relation to its past acts and intentions but transferred rights in exchange for future conduct and future acts

The power inherent in the copyrights of all the books – the rights owner's control over works - would effectively have been taken, rather than given, and concentrated in the hands of one player that was ignoring the rules of the game.

Privacy and International Law

Judge Chin also addressed objections relating to privacy and breach of international law, however these did not contribute to his Honours reasons for rejecting the settlement and are consequently not addressed in this article.

Issues raised by 'opt-out' arrangement

There is no doubt that there would have been significant public benefits if the settlement had been allowed. Judge Chin noted that in addition, some of these:

- out-of-print books would have been given a second life;
- the digitisation would make books more accessible, enabling conversion and printing into braille and other formats for people with reading disabilities; and
- new audiences and new revenue could be generated for the copyright owners.[9]

Many of the out-of-print books copied by Google had fallen out of common use and if the settlement had been permitted, their copyright owners could also have benefited from Google's new revenue stream.

Nonetheless, the practical changes which the settlement would have brought about in the day-to-day administration of copyright would have been radical, and would have permitted an expropriation of the rights of copyright owners, particularly owners of out-of-print works. For that reason, it was not surprising that the settlement was rejected and that Judge Chin preferred to leave the more controversial issues for the US Congress.

4 At 25.
5 At 12.
6 At 22.
7 At 33.
8 26-27.
9 For all the above see p.3.

The conceptualisation of creative works as property is what gives them value in our market society

The case stands as a clear prompt for the legislature (the US Congress, or indeed the Parliament here in Australia) to consider the current regulation of copyright and to make changes that acknowledge the new frames of reference for works in the digital age.

Legislative changes to consider

Copyright is intended to promote writing and creativity by rewarding authors with proprietary rights that allow them to commercialize their work. There is, however, a popular argument that if copyright operates ultimately to reduce and stifle access to books, then the follow-on effect will be a lessening of literary output. The greater the body of literature available, the more opportunities arise for would-be authors to be educated, stimulated and inspired to create new work. An opposing argument acknowledges that access is desirable, but not at the expense of the proprietary right in copyright material. The conceptualisation of creative works as property is what gives them value in our market society.

There is increasingly a perception that access and copyright protection must be opposed and to a certain extent this is true. What gives copyright the character of intellectual *property* is the presence, among the bundle of rights which constitute it, of the right to exclude others from using the material in which the copyright subsists. In a capitalist society, there are few who question the fact that a property right in land is as much about controlling the use of the land as it is about being able to profit from that use. A land owner could develop and exploit the land; or he or she could choose simply to enjoy the exclusive control of the land. Nobody would seriously consider allowing a corporation to take control over the use of a person's land unless the person 'opted-out' of the arrangement. The same principle applies to copyright, even if the author is not exploiting the copyright. It is the capacity to exclude use which gives the copyright owner the power to dictate terms. It is not in the public interest to allow a corporation to dictate the exploitation of copyrights to the copyright owner, especially if that arrangement would result in the corporation obtaining a monopoly over a certain kind of work. There is no doubt that it would not be proper for a court to endorse this course. Legislative action, however, might be able to deal with the issue of access to out-of-print works more broadly, without favouring any particular corporate interest.

A compulsory licence for digitisation of out-of-print books?

It is possible for the Parliament to increase access to copyright material within the bounds of the copyright regime. One way of doing this is to create specific exceptions to copyright infringement and to create compulsory licences for forms of access that are in the public interest. For example, there is a compulsory licence under part VB of the *Copyright Act 1968* allowing limited use of literary work for educational purposes. Under ss 108 and 109, there is also a compulsory licence allowing venues to play music provided they pay equitable remuneration to the copyright owners. Failing agreement between the parties, the Copyright Tribunal decides on the licence fee. With regard to the music licence, public policy favours access to music over the right to exclude use.

This paper is not intended to advocate such a compulsory licence for digitisation of out-of-print books. It is, however, intended to raise the issue for consideration. Enacting a compulsory licence of this kind would not be the same as allowing a corporation like Google to expropriate the copyrights of owners of out-of-print books. Any legislative decision would be based on public policy consideration and would be made by elected representatives. Rather than terms being dictated by a monopolistic market leader, the Copyright Tribunal would be the ultimate arbiter of equitable remuneration to copyright owners for the renewed use of their works. A debate on whether public policy favours creating a form of compulsory licence for out-of-print works in order to increase access would be worthwhile, regardless of the outcome.

Clearance and licensing reform

In order for copyright in out-of-print works to be effectively administered, through a compulsory licence or otherwise, the Parliament needs to enact serious reform in the area of copyright licensing and clearance. Even as an advocate of copyright, it is hard not to sympathise on some level with Google's impatience with the copyright clearance process. As Judge Chin noted, the process of obtaining copyright licences (both in the US, and here in Australia) can be 'painstaking' and six months after the decision in this case, Google and the Author's Guild have been unable to reach a settlement based on an 'opt-in' arrangement. The amount of resources necessary to track down rights holders and persuade them to opt in is prohibitive.

One solution that has been proposed to this problems, in Australia and in the UK, is the development of a centralised registry, a single market place or portal for copyright licensing transactions. Such a proposal is similar to the registry in the proposed Google Books settlement, except that it would be managed by a public body, and one of its goals would be to obtain licensing details in relation to as many copyright works as possible.

In the UK, Professor Ian Hargreaves recommended the establishment of a 'digital copyright exchange'.[10] Such an exchange would be a publicly governed registry, which would eventually contain licensing and contact information for all copyright protected works in the UK. Certain licensing uses could be automated, and where this was not possible, it would at least be easy to seek licensing clearances from one central source.

In Australia prior to the release of the Hargreaves Report, Professor Michael Fraser advocated a similar concept of a 'National Content Network'.[11] The Network would, like Hargreaves' copyright exchange, be a register of copyright licensing data but it would also contain links to digital content. It would be a market not only for the licences, but also for the content.

A centralised registry of this kind would go a long way to overcoming the complications of copyright 'clearance'. It would facilitate greater access to copyright material while leaving intact the fundamental principles of copyright ownership. It would be dependent, however, on ensuring compulsory registration of copyright works on the copyright exchange or network. It would also be expensive and time-consuming to build; factors which inevitably weaken political will for change. One thing is clear though: by making licensing more practicable, this reform would make copyright works more easily accessible, and reduce the tension between access and copyright.

Orphan Works

A related area, that also requires urgent reform, is the licensing of orphan works. Any regime for dealing with out-of-print works needs to account for the clearance of rights by copyright owners who are not readily identified.

---

10 Prof Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth*, May 2011, 4.14ff.

11 Professor Michael Fraser, 'Copy Right or Wrong', *UTSpeaks*, 20 April 2010.

12 *Ibid*, see p.56ff.

13 David Brennan and Michael Fraser, 'The Use of Subject Matter with Missing Owners – Australian Copyright Policy Owners', August 2011.

The Hargreaves Report recommends a clearance procedure for orphan works, involving a diligent search for the copyright owner. It also recommends a mass licensing regime administered by the Government or registered collecting societies for works whose authors cannot be located after a diligent search.[12]

In Australia, Screenrights (the copyright collecting society for film and television) has recently commissioned a discussion paper on orphan works.[13] In that discussion paper, David Brennan and Michael Fraser propose an exception to infringement for non-commercial use of orphan works. For commercial use, the paper proposes a regime requiring a diligent search, a notice period in which a missing copyright owner may come forward, and ultimately a statutory licensing regime administered by collecting societies. The paper recommended a full review of copyright licensing before any further steps towards mass licensing are taken.

Conclusion

Google's copying of millions of books without permission in the US is a clear expression of frustration with the current US system for obtaining copyright licensing permissions, in particular in relation to books which are out of print and orphan works. Likewise, the proposed settlement between Google and the authors and publishers who sued it represents an attempt to create a functional system for increasing digital access to copyright material. The rejection of the settlement was sensible given that the settlement went beyond the scope of the matters in issue in the case, and proposed radical changes to the administration of copyright. Nonetheless, the case highlighted that a change to the current approach is necessary. Importantly, the same problems with rights clearance exist here in Australia as in the US.

The *15th biennial Copyright Law and Practice Symposium* will take place in October 2011. The speakers at the conference will include the Director General of the World Intellectual Property Organisation, Dr Francis Gurry, the Senior Copyright Counsel for Google, William Patry, and the Australian Attorney-General, Robert McClelland. A number of speakers will also be proposing copyright reform. The Google Books settlement, and the issues that it raises, should be seen as an instructive case study for Australian copyright reformers.

Henry Fraser is a lawyer in the technology, media and telecommunications practice group at Allens Arthur Robinson.

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 telecommunications 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

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: ....