LexisNexis™ Butterworths

Volume 9 Number 8
Print Post Approved 24437100049

Internet Law
Bulletin

Blogger beware: IP and defamation implications of the popular online communications tool

Arthur Artinian and **Jeremy Shirm**
BLAKE DAWSON WALDRON

contents

From relatively humble beginnings, blogs (short for 'web logs') have tracked the ascent of the internet to become a powerful and prevalent feature in the online landscape. A US-based blog tracking company, Technorati, estimates that there are approximately 57 million blogs on the world wide web.[1] According to Technorati data, around 75,000 new blogs are created and about 1.2 million contributions are posted on blog sites each day. Political blogs, such as *DailyKos*,[2] *Wizbang*,[3] and their authors have become editorial forces in their own right, powerful enough to be viewed with respect and fear by politicians. Politicians themselves have come to see blogs as an indispensable part of their armoury when on the hustings;[4] corporations are increasingly finding blogs to be an effective means of both undertaking marketing activities and of facilitating efficient communication within the workplace.[5] Newspapers and publishers are now using blogs to engage with readers by generating online debate in relation to their published articles.

What are blogs and why are we all blogging?

Blogs are internet websites where entries are made by both the owner of the blog and blog participants, in the style of a journal. They vary from the fairly basic web page, with free text functionality, to complex commercial blogs which allow posting and sharing of information, multimedia files and increased interactivity between users. A typical blog includes a combination of text, images and links to external websites. More complex blogs include other media forms such as videos, audio files and collections of photographs. Large commercial blogs have complex searching and accessibility features such as operability with mobile phone networks. Two of the most notable commercial blogs are MySpace (the online social networking site owned by News Corporation) and YouTube (the video sharing site which was started by a group of Californian twenty-something entrepeneurs in February 2005 and was recently acquired by Google).

The concept of sharing information in diary or journal form on the internet has been around for some time. Some of the earliest examples can be found in US schools and colleges where students would use pages on their local intranet to post information relating to student life. Online diaries and journals were also a popular feature of many personal websites in the early 1990s. Blogs in their current form began to emerge in the late 1990s with an initial focus on political issues, particularly from the US. Since this time, the popularity of blogging has rapidly accelerated in a wide range of industries.

There is no doubt that blogging is here to stay and it is no wonder — the blogging mechanism itself is an inexpensive and straightforward way to engage others, whether they be your customers, colleagues, students or the general public, and to share

valuable insights and information. Even legal practitioners are in the game: New York law firm Schwimmer Mitchell maintains the international 'Trademark Blog', which is accessed by intellectual property practitioners worldwide.[6] In an article in *The Age* in April 2006, James McConvill, senior lecturer at La Trobe Law School, argued that 'in the next 12 months, every academic in an Australian law school should be blogging on a regular basis, or seriously considering their future in academia.'[7]

The increase in popularity of blogging has opened up a range of legal issues for bloggers themselves as well as companies involved in these activities, whether as internet service providers (ISPs) hosting content, as employers, or as corporations running corporate blogs in their own right. The legal issues are not themselves new, but we are seeing a trend where laws around the world are being tested in the new digital environment of blogs. Like all journalists and publishing organisations, bloggers may wish to post information that other people may not want published. The reach of the internet means that online content is published to a vast, worldwide audience. The commercialisation of blogging has meant that lawsuits have become more attractive for intellectual property owners whose rights are infringed by blogging activities and persons whose confidential information is disclosed online or who are the subject of defamatory comments. Recent developments in intellectual property laws in Australia will also raise new questions for bloggers.

Defamation issues

One area of particular note is defamation, and the risk of liability in defamation presents some interesting developments on established legal principles. The starting point in the consideration of an action in defamation is jurisdiction. As *Dow Jones v Gutnick* (*Gutnick*)[8] makes clear, the traditionally confining effect of jurisdiction on liability in defamation has been considerably weakened in relation to online publication. As the court held in that case, notwithstanding that uploading may be considered to have occurred in one jurisdiction, due to the globally accessible nature of that publication, the jurisdiction of the publisher can no longer be considered the only appropriate forum to initiate proceedings. Indeed, as *Gutnick* makes clear, an appropriate jurisdiction in which to hear an action in defamation may not be the jurisdiction of publication, but rather the jurisdiction in which the damage sustained through the defamatory action occurs.

This was precisely the case in *Gutnick*, where Victoria, Australia was found to be an appropriate forum for defamation proceedings (or more precisely, was found *not* to be clearly inappropriate, according to the test set out in *Voth v Manildra Flour Mills*)[9] in relation to an article published on the *Wall Street Journal* website, published in New Jersey, US. This action has found approval in the English courts,[10] although more recently a UK court refused to allow a Saudi businessman to sue Dow Jones in the UK, on the basis that it would be improper for the suit to proceed where a limited number of people had read it in that jurisdiction.[11]

The *Gutnick* decision has since been overruled in Australia as to choice of law, by the enactment of the uniform defamation laws. It remains the case, however, that courts are likely to continue to find that there are multiple appropriate forums for online defamation suits.

Further, those who provide the vehicle for online publication, namely ISPs, have also been held liable for defamatory content on their website. The case law suggests that knowledge of the defamatory material is a central consideration in establishing liability. This issue has been considered in a series of UK cases, which is considered further below.

United Kingdom

In *Godfrey v Demon Internet* (1999) EWHC QB 244 (26 March 1999) (*Godfrey*), a US resident posing as the plaintiff, Godfrey, posted a number of defamatory comments about Godfrey on a newsgroup hosted by the defendant. Godfrey subsequently sent a fax to Demon Internet, alerting them of the forgery and asking for the comments to

be removed. The defendants failed to do so, and Godfrey commenced proceedings against Demon Internet for defamation.

Notwithstanding consideration of the defence of 'innocent dissemination' under UK defamation legislation, the court found the defendant liable, holding that the defendant was not 'merely a passive owner of an electronic device through which the postings were transmitted'. The court further noted that, following Godfrey's facsimile, Demon Internet also knew about the defamatory posting.

In March 2006, in *Bunt v Tilley*,[12] the UK courts considered the liability of ISPs for defamatory comments made on websites that they hosted. In that case, John Bunt brought an action in defamation against David Tilley, who had posted defamatory content online, and America Online (AOL) UK, which hosted the relevant websites. Tilley had made several defamatory comments about Bunt on a discussion board hosted by AOL UK. Bunt subsequently sent an email to AOL UK, informing AOL of the comments, asking what procedures should be taken in order for them to disclose the identity of the comments' author.

The question for the court was whether the ISPs could be 'liable in respect of material which is simply communicated via the services which they provide'.[13] The court considered *Godfrey* and concluded that that there was no prospect that the plaintiff could establish that the defendants had knowingly participated in the publications. The defendants also raised the same statutory 'innocent dissemination' defence pleaded in *Godfrey*, on the basis that they were not aware of the defamatory statements posted on websites hosted by them. This argument succeeded, and the court held that Bunt's facsimile had not put the ISPs on notice, since it did not effectively communicate the nature of the defamatory statements to them. More generally, the court held that 'an ISP who performs no more than a passive role in facilitating postings on the Internet cannot be deemed to be a publisher at common law'.[14]

Liability for defamation online was further considered in *Keith-Smith v Williams*.[15] In that case, Michael Keith-Smith, a minor UK politician, engaged in discussions on a Yahoo! discussion board with Tracey Williams. Both were operating under pseudonyms, so that their identities were not readily ascertainable, although their identities could be revealed by clicking on their pseudonyms.

According to the judgment in that case, differences in political opinion between them saw the discussion lead to name-calling and eventually to Williams making allegations about Keith-Smith, including in relation to his sexual predilections. Williams's comments continued when Keith-Smith ascertained her personal details in order to serve suit. Williams never appeared nor filed a defence, and was found to have defamed Keith-Smith. It is noteworthy that media coverage questioned the decision, querying firstly the likelihood that the comments would be viewed by more than a few individuals, notwithstanding it was posted online, and further querying whether any such people would consider these comments as anything more than ramblings.

Most recently, Ashley Cole, a footballer famous in the UK, filed suit against the *News of the World* and *The Sun*, for their publication of photographs of people, de-identified through pixellated faces, with the headlines 'allegedly bisexual but unnamed (English) Premiership players'. The article also provided a few details regarding the identity of the players. Bulletin boards and chat rooms avidly discussed the players' identity, and Cole was quickly singled out. Cole brought proceedings soon afterwards.[16]

Cole's case is noteworthy in that his arguments are not based on any material posted by the defendant. Rather, he is alleging that the defendants should be liable for the discussions and allegations arising in online chat rooms following publication of the articles. In this sense, online activities such as blogging present novel scenarios, given that the instantaneous and widespread nature of online discussion may itself generate conclusions and eventualities not initially considered by those disseminating information.

The case is also noteworthy for another reason. Although not yet joined to the proceedings, Cole's lawyers have questioned Google in relation to these events. Shortly after this online discussion commenced, when 'Ashley Cole' was typed in to the Google search engine, the search engine would return the alternative suggested search, 'Ashley Cole gay'. Cole's lawyers were evidently keenly interested in whether this alternative search was a result of the Google search algorithm, or rather because of an editorial decision by Google, and accordingly asked Google to 'please explain'. The lawyers have indicated that a confirmation of the latter scenario by Google may entail their joinder to the proceedings.[17] This litigation continues.

Australia

In Australia, the legislature has afforded ISPs a limited shield in the form of s 91 to Sch 5 of the *Broadcasting Services Act 1992* (Cth). This provision protects ISPs from liability for third-party content hosted by them, in certain circumstances, where they are not aware of the nature of the content. This defence is likely to apply to actions in defamation.

However, the protection of this provision is not available where the ISP is on notice regarding any such content. Notice will generally be considered to have been provided where the ISP has received a complaint, since the ISP would then know of the existence and nature of such content. Where notice has been provided, the only defences to an action in defamation would then be on the basis of substantive defences such as truth.

Implications

Some important themes arise out of the case law above, which are of note for bloggers and in particular for ISPs who host blogs.

First, as *Gutnick* demonstrates, the nature of the internet means that traditional notions regarding jurisdiction and choice of law are becoming outmoded when it comes to online content. Because of the global reach of any such material, bloggers would do well to presume that material they publish online could realistically be read

and considered by courts to be the proper subject of defamation proceedings in numerous jurisdictions. Accordingly, individuals should evaluate the risks associated with blogging activities with due care.

Second, ISPs should consider the extent to which they may be liable for information contained on blogs hosted by them. Where ISPs clearly have no knowledge of defamatory content hosted by them, as noted above they may have a statutory defence, at least under Australian law. However, given the global nature of the internet, and the attendant possibility of liability in a variety of jurisdictions, ISPs may nonetheless be required to evaluate risks in multiple jurisdictions.

Third, although not currently reflected in judicial opinion, criticism of the decision in *Keith-Smith* alludes to a more contextualised consideration of the circumstances in which defamatory content is made. Notwithstanding that defamatory comments may be made in an online forum such as a blog, the number of people who may actually view those comments, and the extent to which credence is given to them, has been questioned.

Defamation concerning publication to a small number of readers, the so-called 'backyard' cases, is not novel. However, given the explosion of online content and the nature of online discussions, such cases may be heard with greater regularity. In Australian jurisdictions, defences to such cases may be available in the form of the statutory triviality defences under Australia's uniform defamation legislation.[18] It is entirely possible that the growing body of law in relation to online defamation may consider such arguments.

Finally, as stated above, in Cole's case against two UK newspapers, the UK courts are currently considering whether media organisations can be held liable for online comments that may have resulted from articles published by them. In *Webb v Bloch*,[19] the court held that:

> all who are in any degree accessory to the publication of a libel … are to be considered as *principals in the act of publication*: thus if one *suggests* illegal material in order that another may write it … [both] are equally amenable for the act of publication.[20]

It remains to be seen how far this accessorial liability for publication stretches.

The result of the *Cole* litigation will be watched with interest, and it is seems reasonable to consider that, given that blogging activities by their nature can foster instantaneous and widespread discussion, such arguments may become more common.

Intellectual property issues

Blogs created a myriad of complications for owners of intellectual property on the web. The ease of copying information, whether it be using content from a news item from a wire service or reproducing an image from another website, can make blogging a legal minefield both for the blogger themselves and for organisations that support their activities.

Copyright infringement

One of the most pertinent legal issues in the IP space for bloggers is potential infringement of copyright in material which is posted on blog sites. Principles relating to online copyright infringement have been developing in the context of peer-to-peer file sharing activities in recent years (*Napster*, *Grokster, Cooper* and *Kazaa)* although there has been no judicial consideration to date relating to copyright infringement specifically on a blog site.

The implication for bloggers is that permission is required from the copyright owner of materials in which copyright subsists to do any of the acts prescribed as exclusive rights under the *Copyright Act 1968* (Cth). The risk is greatest where large portions of material (or complete works, such as videos or audio files) are made available on a website which is accessible to the public for download. Apart from providing copyright material within blogs, bloggers need to take care to ensure that they do not provide links to other websites that infringe copyright. Where the blog is a commercial venture, and where profits are obtained through the provision of links to sites which provide access to infringing copies of copyright material, there is the potential for the owner of a

website, as well as the ISP, to be liable for authorisation of copyright infringement (*Universal Music v Cooper*).[21]

The proposed amendments to the *Copyright Act* may assist bloggers where material is placed online for the purpose of parody or satire. According to the current law, there is no exception to copyright infringement for this type of activity, and if a parody reproduces a substantial part of a work, it is likely that the blogger (and possibly the ISP) will be liable for infringement. Under the proposed amendments, there will be an exception to infringement where a work is reproduced for humorous or satirical imitation,[22] so long as the use 'does not unreasonably prejudice the legitimate interests of the owner of the copyright or a person licensed by the owner of the copyright'.[23]

A highly publicised and unique example of a large commercial video blog (or 'vlog') which presents a myriad of issues in the copyright space is the popular video-sharing site YouTube, which was recently purchased by Google for A$2.22 billion.

Moral Rights

Bloggers also need to ensure that they do not infringe the moral rights of a creator of a work. Moral rights include a creator's right of attribution, right against false attribution and right of integrity against derogatory treatment of a work.[24] Moral rights apply to all works and films (and works as included in films) that were in existence and still in copyright on 21 December 2000, and all works and films (but not sound recordings) created after that date.

From a practical perspective, this means that bloggers must (in addition to ensuring they don't infringe copyright) attribute the author or creator of copyright works correctly on their site and not make alterations to a work or engage in any conduct which is likely to be considered a derogatory treatment of a work.

Trade Mark Infringement, TPA and passing off issues

The nature of blogging and the subject matter which many blogs cover inevitably leads to the interaction of blogs with the brands and trade marks of corporations. Bloggers and the companies which support their activities need to consider the implications of trade mark and consumer protection laws which are likely to apply to their activities.

In developing a name for a new blog, care needs to be taken to ensure that the name does not incorporate someone else's trade mark and that it is not substantially identical with or deceptively similar to a registered trade mark. Use of another person's trade mark can also give rise to liability for misleading/deceptive conduct in contravention of s 52 of the *Trade Practices Act 1974* (Cth) if the conduct is in the commercial context and may constitute actionable passing off.

The content of a blog also needs to be carefully considered from a trade mark infringement perspective. Reproduction of logos or brand names can create trade mark infringement risks and also possibly copyright infringement risks where graphical logos are reproduced on a blogger's site. The risk of a trade mark infringement claim may be reduced where a mark is used in the context of criticism or discussions (where the mark is not used 'as a trade mark', as required to give rise to infringement under the *Trade Marks Act 1995* (Cth)).[25]

Blogs and companies: considerations for employees and employers

Blogging likewise presents novel considerations for employees and employers.

Employers

An employer is vicariously liable for the activities of its employees, where those activities are undertaken 'in the course of their employment'. The activities do not need to be specifically ratified, provided they are undertaken performing an authorised task. Blogging may classify as such an activity where ratified explicitly or tacitly. For example, if an employee (NSW-based) encourages an employee to post blogs on an industry blog site or company site, questions of vicarious liability are likely to arise.

An employer may also be liable for defamatory material as a party to publication in some circumstances, such as when an employee blog is hosted on an employer's website. A standard response to vicarious liability in relation to blogging has been to include appropriate sections for blogging activities in an employer's employee policies. This policy may forbid any blogging using work facilities, and provide notice to employees that an employer may exercise their rights under the *Workplace Surveillance Act 2005* (NSW) to monitor all blogging activities undertaken using work facilities.

Such policies enable employers to clearly specify which activities are authorised in the course of employment, and so minimise the possibility that any blogging undertaken by an employee is only undertaken in the course of employment to the extent that it complies with the policy.

Employees

Conversely, private blogging activity may have serious ramifications for an individual's tenure of employment. For example, recently a British citizen who wrote what she had thought to be an anonymous daily blog, entitled *Le Petit Anglais*, was fired over comments made in that blog, which her employer considered brought it into disrepute.[26] She had not named herself nor her employer, but had posted a photograph of herself on the blog.

This is but one example of a growing phenomenon that has developed its own name, 'dooced', an internet neologism for being fired for your blog.[27] The term itself refers to the blog of a US citizen, who was fired in 2002 for comments made on a blog regarding experiences while employed at an internet start-up.

In order to ensure that employees are fully informed about their obligations in relation to blogging, it is recommended that employers keep their staff fully informed about employer policies relevant to blogging activities. Equally, employees would do well to keep in mind the ramifications that their private blogging activities may have for their employers. It a lesson all too well forgotten that the vast size of the internet used as a 'cloak' for one's identity can often be illusory.

Conclusion

The analysis above has summarised some types of liability that may arise out of blogging activities for individuals and organisations in relation to defamation and IP issues. However, it is clear that the liability of organisations, whether through vicarious liability for employees or through the operation of Sch 5, s 91 of the *Broadcasting Services Act 1992* (Cth), liability is not limited to just defamation or IP issues. Accordingly, where notice has been provided, organisations may be held liable for disclosure of confidential information, as well as for deceptive and misleading conduct, discriminatory content, offensive or obscene material, or other kinds of legal liability.

Finally, as the dates of the cases considered make clear, a common theme which presents is that the law concerning liability in an online setting is very recent, and far from settled. Although no novel legal liabilities have arisen out of blogging activities, it has provided a novel setting for existing principles, which may have significant and unanticipated effects. These effects have only just begun to be tested before the courts.

It seems certain that, along with the explosion in privately produced online content in such forums as blogs, there will likewise be a growth in the amount of litigation, which further considers and refines these nascent principles, just as it seems likely that new factual scenarios will present new legal issues not yet considered in the few cases already decided.

In short, the message is 'watch this space' for further developments. ●

Arthur Artinian, Lawyer, and Jeremy Shirm, Lawyer, Blake Dawson Waldron, Sydney.

Endnotes

1. See <www.technorati.com>, accessed 15 October 2006.
2. See <www.dailykos.com>, accessed 17 October 2006.
3. See <http://wizbangblog.com/>, accessed 18 October 2006.
4. Faler B 'Add blog to the campaign lexicon' *The Washington Post* 15 November 2003.
5. O'Shea W '"New Economy"; the online journals known as web logs are finding favour as an efficient way to communicate within the workplace' *New York Times* 7 July 2003.
6. See <www.schwimmerlegal.com>.
7. McConvill J. (2006) 'Blog or you won't be read' *The Age* 3 April 2006 p 3.
8. (2002) 194 ALR 433.
9. (1990) 171 CLR 538 at 565.
10. See *Harrods v Down Jones* [2003] WEHC 1162, *Lewis v King* [2004] EWCA Civ 1329.
11. *Dow Jones v Jameel* [2005] EWCA 75.
12. [2006] EWHC 407 (10 March 2006).
13. Above at 5.
14. Above note 12 at 14.
15. [2006] EWHC 860.
16. See Bond C 'Can I sue Google if it says I'm gay? The tales of internet defamation in the UK' (2006) 64 *Computers & Law* at 1 for a detailed analysis of the Cole proceedings.
17. Nugent H 'Cole's lawyers trawl for libel witnesses on web' *The Times* (UK) 12 March 2006.
18. *Defamation Act 2005* (NSW), s 33; *Defamation Act 2005* (Vic), s 33; *Defamation Act 2005* (Qld), s 33; *Defamation Act 2005* (WA), s 33; *Defamation Act 2006* (NT), s 30; *Defamation Act 2005* (Tas), s 33; *Defamation Act 2005* (NT), s 33; *Defamation Act 2005* (SA), s 31; *Civil Wrongs Act* (ACT), s 139D.
19. (1928) 41 CLR 331.
20. Above note 19 at 364. Isaacs J was quoting Starkie T *The Law of Slander, Libel, Scandalum Magnatum, and False Rumours* (1832) with approval.
21. [2005] FCA 972; BC200505025.
22. Copyright Amendment Bill 2006 (Cth), new s 200AB(5).
23. Above, new s 200AB(1).
24. *Copyright Act 1968*, Pt IX.
25. *Trade Marks Act 1995* (Cth), s 120.
26. Frost V 'Dear diary, fed to the blogs today' *Sydney Morning Herald* 29 July 2006, article republished from the *Guardian*.
27. See 'Bridget Jones' blogger fire fury', <www.cnn.com> 19 July 2006.

Liability of ISPs for defamation in Australia: are things getting easier?

Mitchell Birks
NOOSA SHIRE COUNCIL

There has been much weeping and gnashing of teeth among ISPs worldwide over their potential liability for defamation. This is seen as particularly offensive where they host the defamatory material or, worse, where the ISP is a mere conduit for its transmission.

The laws of various jurisdictions have dealt with this liability in different ways. In Australia, the position has been updated by each state and territory recently passing largely identical legislation — the uniform defamation laws (UDL) — as well as recent case law from overseas. This article briefly touches on those developments.

Internet service providers (ISPs)

The position of publishers at common law was summarised in this pithy passage from *Godfrey v Demon Internet Ltd (Godfrey)*:[1]

> At Common Law liability for the publication of defamatory material was strict. There was still publication even if the publisher was ignorant of the defamatory material within the document. Once publication was established the publisher was guilty of publishing the libel unless he could establish, and the onus was upon him, that he was an innocent disseminator.

ISPs may host material, or they may be a conduit for it. After *Godfrey*, an ISP will be liable as a publisher of defamatory material that it hosts in its computer systems, and is also thought likely to be liable as a mere conduit.[2] The ISP may then raise the defence of innocent dissemination, showing that it was a subordinate distributor (it did not create material) which:

- did not know that the publication contained a libel;
- did not know that the publication was of such a character that it was likely to contain a libel; and
- was not negligent in their absence of knowledge.[3]

Before considering ISP liability in Australia, it is useful to trace the broader development of ISP liability, touching on issues of knowledge and control.

US position

The celebrated cases of *Cubby Inc v CompuServe (Cubby)*,[4] and *Stratton Oakmont v Prodigy Services Company (Stratton)*[5] combined to suggest that an ISP that takes steps to minimise the likelihood of publication of defamatory material will increase its risk, as they may be deemed to be exercising control over the material. This led to legislative action in the *Communications Decency Act* 1996 47 USC, s 230, the section saying, 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'.

The section was tested in *Zeran v America Online*.[6] Here, America Online (AOL) was told that it hosted defamatory material, and failed to remove it. The court gave AOL complete protection under s 230; the issues of editorial control and knowledge that had been relevant in *Cubby* and *Stratton* were not relevant.

UK position

The UK position is different. Knowledge and control are relevant to ISP liability.

The *Defamation Act 1996* (UK) contains 'the modern equivalent of the common law defence of innocent dissemination'.[7] Section 1(1) says:

> (1) In defamation proceedings a person has a defence if he shows that —
> a. he was not the author, editor or publisher of the statement complained of,
> b. he took reasonable care in relation to its publication, and
> c. he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

This was considered in the context of ISP liability in *Godfrey*.[8] Here, the defendant was an ISP operating Usenet newsgroups. Someone made a defamatory posting. The plaintiff told the defendant of the posting, asking them to remove it. The posting remained for a further 10 days.

The court noted that liability for the publication of defamatory material at common law was strict, applying even if the person did not know that the material was defamatory. The court quoted from *Byrne v Deane*,[9] where it was held that:

> … [t]he test it appears to me is this: having regard to all the facts of the case is the proper inference that by not removing the defamatory material the defendant really made himself responsible for its continued presence in the place where it had been put?

The court held that the ISP was liable, and said:

> In my judgment the defendants, whenever they transmit … from the storage of their news server a defamatory posting, publish that posting to any subscriber to their ISP who accesses the newsgroup containing that posting. Thus every time one of the Defendant's customers sees that posting defamatory of the plaintiff, there is a publication to that customer.[10]
>
> … The defendants chose to store [the].. postings within their computers. Such postings could be accessed on that newsgroup. The defendants could obliterate and indeed did so ...[11]

The ISP was liable for damages from the time that it was notified of the posting until the time of its removal.

However, the UK position is complicated by broader legal issues. The Court of Appeal seems to

acknowledge that the operation of the *Human Rights Act 1998* (UK) may affect defamation law.[12] Further, ISP liability was considered in a 2002 report by the UK Law Commission.[13] The Commission noted that the UK position had been potentially complicated by the adoption of the *Electronic Commerce (EC Directive) Regulations 2002* (UK),[14] which provides an immunity to ISPs arguably similar in effect to s 1(1) of the *Defamation Act 1996* (UK).[15]

The issue of ISP liability was recently addressed *Bunt v Tilley (Bunt)*.[16] Here, a claimant proceeded against three alleged defamers and their ISPs. The ISPs in question were mere conduits.

The ISPs did not know that they were involved in passing on defamatory material.[17] They secured orders that the claims against them be struck out summarily. Eady J said:

> … I am prepared to hold as a matter of law that an ISP which performs no more than a passive role in facilitating postings on the internet [sic] cannot be deemed to be a publisher at common law.
>
> … [P]ersons who truly fulfil no more than the role of a passive medium for communication cannot be characterised as publishers: thus they do not need a defence.[18]

The claimant here was self-acting, had poorly pleaded his case, and failed to lead salient evidence. Nevertheless the reasoning accords with leading opinion referred to therein,[19] notwithstanding that it may not mesh perfectly with passages from *Godfrey*.

Bunt involved an ISP acting as a conduit for the material, and not as a host. However the language of Eady J may be sufficiently wide to encompass a hosting of material. If so, then on the basis of *Byrne v Deane* and *Godfrey* where an ISP is told that it carries defamatory material, it is at risk of being a publisher of that material, thereby needing to rely on the defence.

Australian position

Before the UDL, the law of defamation in Australia varied between states. For an ISP, the common law defence of innocent dissemination may have been available, depending upon the circumstances and where proceedings were initiated. The defence as expressed in the state's law typically did not reflect changes in technology. For example, in Queensland the law was codified in the *Defamation Act 1889* (Qld), the common law defence of innocent dissemination being replaced by a statutory defence protecting sellers of periodicals or books.

The *Broadcasting Services Act 1992* (Cth) contains, in Sch 5, cl 91(1) the following:

> (1) A law of a State or Territory, or a rule of common law or equity, has no effect to the extent to which it:
>
> a. subjects, or would have the effect (whether direct or indirect) of subjecting, an Internet content host to liability (whether criminal or civil) in respect of hosting particular Internet content in a case where the host was not aware of the nature of the Internet content; or
>
> b. requires, or would have the effect (whether direct or indirect) of requiring, an Internet content host to monitor, make inquiries about, or keep records of, Internet content hosted by the host; or
>
> c. subjects, or would have the effect (whether direct or indirect) of subjecting, an Internet service provider to liability (whether criminal or civil) in respect of carrying particular Internet content in a case where the service provider was not aware of the nature of the Internet content; or
>
> d. requires, or would have the effect (whether direct or indirect) of requiring, an Internet service provider to monitor, make inquiries about, or keep records of, Internet content carried by the provider.

Although the clause was designed to protect ISPs that unwittingly host offensive (for example, pornographic) material,[20] Collins notes[21] its broader application (unlike the ISP code of conduct)[22] and that the clause effectively excludes from its application limited internet publications such as emails, information transmitted in the form of a broadcasting service, and data kept on a data storage device.

The clause excludes the operation of inconsistent state and territory laws and does not impose liability on an ISP if it knows that it carries defamatory material. That liability has to be found elsewhere. Liability will prima facie attach if an ISP is a publisher at common law, subject to any applicable defence — remembering that on the basis of *Bunt*, an ISP that is a mere conduit (or possibly a host) may not be a publisher and may not need a defence.

The uniform defamation laws

The UDL is not a code, but provides a framework that surrounds the common law. It uses common law understanding of 'publication' and 'defamatory matter'.

Section 32 of the UDL contains the defence of innocent dissemination. On the surface, it seeks to deal with liability of ISP's for publishing defamatory material that they did not create.

However, the treatment remains unsatisfactory. The defence, said to be 'expanded to take account of modern forms of communication',[23] says:

> *32 Defence of innocent dissemination*
>
> (1) It is a defence to the publication of defamatory matter if the defendant proves that —
>
> (a) the defendant published the matter merely in the capacity, or as an employee or agent, of a subordinate distributor; and
>
> (b) the defendant neither knew, nor ought reasonably to have known, that the matter was defamatory; and
>
> (c) the defendant's lack of knowledge was not due to any negligence on the part of the defendant.
>
> (2) For the purposes of subsection (1), a person is a subordinate distributor of defamatory matter if the person —
>
> (a) was not the first or primary distributor of the matter; and
>
> (b) was not the author or originator of the matter; and
>
> (c) did not have any capacity to exercise editorial control over the content of the matter (or over the publication of the matter) before it was first published.
>
> ….

In *Godfrey*, a defence based on this section would not have been available because of the effects of s 32(1)(b). This defence, ultimately, may not bring ISPs

the level of protection that they are after.[24]

Section 32(3) then provides extensive examples of when an ISP is acting as a subordinate distributor. For example, an ISP acting as a mere conduit may be compared to a mail service,[25] thereby being a subordinate distributor under s 32(3)(d). However, for an ISP, whether acting as a conduit or a host, the crux of the s 32 defence seems to be the phrase in s 32(2)(c), 'any capacity to exercise editorial control'.

This summarises the problems seen in the US cases without providing any real help in understanding when this aspect of the defence will apply. The Explanatory Notes are unhelpful, rather blandly rehashing the text of the section.[26]

Collins draws an analogy from cases to the effect that parties that procure the commission of torts may attract liability, but those that facilitate the tort may not.[27] This was picked up by the court in *Bunt* and essentially followed to allow conduit ISPs to escape being described as publishers. If *Bunt* were followed in Australia (which seems probable), an ISP would not be liable for defamation where it acted as a mere conduit without knowledge.

But what of the ISP that hosts material? *Bunt* may or may not apply. The extent of control required is 'any capacity', which suggests a low standard. Does an ISP that considers whether to set up its affairs so that it can exercise control, but then decline to do so and adopt another technological model, have the capacity to exercise editorial control? And what exactly is editorial control? Does it connote the active poring over material to edit, proofread, and consider it — or does it merely mean that the ISP has an ability to block an offensive site? Or could the answer lie somewhere in between? Under s 32, a hosting or caching ISP remains at risk of a *Godfrey* outcome, and the application of this section will be determined by litigation rather than perceptive drafting.

Conclusion

The knowledge that it publishes defamatory material will prevent an ISP from raising the s 32 defence. If an ISP merely facilitates communication, as in *Bunt*, it may not be regarded as being a publisher, as that term is known in the common law. Accordingly, the ISP may escape liability. If the ISP is a publisher (perhaps it is not a 'passive medium' for communication), and it did not know that it publishing the offending material, the important test in the s 32 defence relates to exercising editorial control. If there is 'any capacity' to exercise editorial control, the s 32 defence is not available to an ISP. The knowledge that an ISP may have is relevant to both cl 91(1) of the *Broadcasting Services Act 1992* (Cth), and the operation of the s 32 defence, and how these to sections will intersect on this issue is unclear.

The result of the UDL for ISPs is that their position is set out in a patchwork of laws consisting of the common law, federal legislation and the UDL. Participants will find this unhelpful and more complex than it needs to be.

The UDL is, broadly, a welcome evolution in the law and yet there was an opportunity for reform in this area that might have been missed. While there seems to be no general call for the 'blanket' immunity offered to an ISP that is enjoyed in the US, as far as ISPs are concerned the defence of innocent dissemination would be well served by codification, thereby covering the various issues raised in the common law, the UDL and the provisions of the *Broadcasting Services Act*. ●

Mitchell Birks, Solicitor,
Noosa Shire Council.

Endnotes

1. [2001] QB 201 per Morland J at 26.
2. Collins M *The Law of Defamation and the Internet* Oxford University Press, Oxford 2001.
3. Above p 177. For a slightly different summary of the authorities, see Gillooly M *The Third Man, Reform of Australasian Defamation Defences* Federation Press, Sydney 2004 p 204.
4. 776 F Supp 135 (SDNY 1991).
5. (1995) 195 NY Misc LEXIS 229.
6. 129 F3d 327 (4th Cir).
7. Lord Mackay LC *House of Lords Hansard* Col 214 Defamation Bill 2 April 1996.
8. [2001] QB 201.
9. [1937] 1 KB 818 at 837 per Greene LJ.
10. Above at 33.
11. Above note 9 at 35.
12. *Dow Jones & Co Inc v Jameel* [2005] EWCA Civ 75.
13. Law Commission (UK) *Defamation and the Internet: A Preliminary Investigation* Scoping Study No 2 (December 2002), pp 5–21.
14. For a useful summary of this issue, see above pp 7–10.
15. Above note 13, p 9.
16. [2006] EWHC 407 (QB).
17. Strangely, the court noted, at 27, that the comments were posted on the claimant's own website, and it was within the claimant's power to remove them if he so chose.
18. At 36 and 37.
19. His Honour quoted extensively Collins M *The law of Defamation and the Internet* (2nd edn) Oxford University Press, Oxford 2005.
20. See generally Coroneos P 'Internet content control in Australia: attempting the impossible?' [2000] *UNSWLJ* 6.
21. Above note 2. Compare with Heitman, who describes the protection as illusory: Heitman K 'Free speech online: still shooting the messenger' (2005) 28(3) *UNSWLJ* 928 at 929.
22. Which does not seem to affect defamation — see the May 2005 version at <www.aba.gov.au/internet/codes.shtml>.
23. Queensland, *Parliamentary Debates* Legislative Assembly 9 November 2005 p 3891, and 25 October 2005 p 3427 (Mrs LD Lavarch, Minister for Justice and Attorney-General).
24. As to one view about appropriate protection for ISPs, see Heitman above note 21.
25. *Bunt v Tilley* [2006] EWHC 407 (QB), where Eady J quotes Collins above note 2 at para 15.43.
26. For example, see Explanatory Notes to Defamation Bill 2005 (Qld) at p 20.
27. Collins above note 2 at para 15.38.

Internet jurisdiction in the People's Republic of China

Dan Svantesson
BOND UNIVERSITY

While private international law in China is becoming increasingly important, the sporadically released jurisprudence shows that the Chinese practice leaves much to be desired. As the strength of private international law is dependent on the extent to which it is upheld by People's Courts, these problems are crucial not only for foreigners and Chinese alike in the enforcement of rights involving foreign elements, but central to the future development of private international law.[1]

The People's Republic of China (PRC) has more citizens than any other state in the world. That fact, combined with the PRC Government's encouragement of internet use, makes it reasonable to suggest that the PRC is emerging as a major participant in the global use of the internet. The potential of the PRC as a future market is augmented by the increasing strength of the PRC's economy. Currently, the PRC is the fastest growing economy in Asia.[2] Indeed, the rapid development of the Chinese economy is unprecedented in modern history. With this in mind, it is not surprising that an increasing number of Australian businesses, including web-based businesses, are considering entering the massive PRC market.

Against this background, this article examines the circumstances under which the PRC courts may claim jurisdiction over a foreign website in relation to contracts.

The internet in the PRC

The internet in the PRC is structured according to a four-tier system not dissimilar to that of many other states. Starting from the bottom, we have the individual internet users (tier four). They connect to the internet through internet service providers (ISPs) (tier three). The ISPs connect to an internet access provider (IAP). The IAPs, representing the second tier, are the ones that actually own the physical networks, which are leased by ISPs. Finally, the IAPs connect to the government's gateway (tier one) and can thereby access the global internet. What makes this system different to that of many other states is the fact that this is not merely the system normally used, but the one prescribed by law.[3] Thus, for example, an internet user may not connect to the internet via a foreign ISP in order to circumvent the system, and any such attempts will be punished.[4]

The consequence of this structure is that the PRC Government can control the internet traffic that enters and leaves the PRC part of the internet, and the Government of the PRC has been known to block a range of foreign websites in order to limit the amount of foreign content available to its citizens. Examples of websites that have been blocked include CNN, the BBC, the *Washington Post*, the *New York Times*, Yahoo!, Amnesty International, the Voice of America and foreign Falun Gong websites. However, the blocking of foreign websites is not static. Rather, it goes on and off, seemingly unpredictably, and may not always affect the whole country. Similar structures can be found, for example, in Saudi Arabia and Singapore, but they are otherwise relatively rare.

If taken to the extreme (for example, blocking access to all foreign websites), this method can be seen, arguably, as an alternative to aggressive extraterritorial claims of jurisdiction — foreign material that is effectively blocked simply cannot cause direct local harm in the PRC. In other words, if blocking were taken to its extreme, there would be no need, or indeed any ground, for claims of extraterritorial jurisdiction. It is noteworthy that, so far, the PRC has not made any wide internet-related jurisdictional claims, while, for example, the US, France, Australia, Italy, Germany, Canada and the UK have all made such claims.

Jurisdiction: an overview

The fundamental jurisdictional rule in Chinese conflicts is that a civil suit against a Chinese citizen comes under the jurisdiction of the court at the place where the defendant is *domiciled*,[5] or if not, under the jurisdiction of the people's court at the place of his regular abode or residence.[6] However, the law of the PRC provides for separate jurisdictional rules in foreign-related, or so-called *shewai,* cases.

A judicial interpretation of the Supreme People's Court from 1992[7] provides rather clear guidelines as to when a case is a *shewai* case. A case is classed as a *shewai* case if one or both parties are foreigners (including stateless persons, foreign enterprises or foreign organisations). Further, a case is classed as a *shewai* case if the legal fact that the civil legal relationship between the parties establishes, changes, suspends or occurs outside the territorial sphere of the PRC. Finally, with some exceptions, a case is classed as a *shewai* case if the civil case concerns subject-matter located outside the territorial sphere of the PRC.

Although fairly clear, the definition of *shewai* gives rise to the following questions in relation to the internet. First, can an e-commerce website located on a server within the territory of the PRC fall within the *shewai* category? Second, can an e-commerce website located on a server outside the territory of the PRC, but aimed at doing business in the PRC, fall within the *shewai* category?

The first question is easy to answer. Since all e-commerce operations (that is, profit-making internet information services) located on servers within the PRC must have a business licence issued by the PRC and must meet certain requirements,[8] such operations could not fit within the *shewai* category; they are Chinese by their very nature.

The second question is slightly more complex and will presumably depend on

the ownership of the e-commerce operation. If the website is operated by foreign owners, a potential dispute would be between the foreign operator and the Chinese party, and would thus fall within the *shewai* category. However, it is also possible for a dispute arising out of a Chinese contact with a website located on a server outside the territory of the PRC to fall within the *shewai* category, even if the website is operated by a Chinese business. This can, for example, be the case if the contract was formed at the location of the foreign server.

Finally, two more rules are to be observed. The foreign party to a *shewai* case enjoys 'the same equal litigant rights and obligations as the citizens, legal persons and other organizations of the PRC'[9] and the *Law of Civil Procedure of the People's Republic of China* further provides that, where there are no special rules provided in relation to *shewai* procedures, other relevant provisions of the law will apply.[10]

Different rules apply in relation to jurisdictional claims over contractual relations and jurisdictional claims over situations involving defamation.

Jurisdiction in contracts cases

Part 4, ch XXV of the *Law of Civil Procedure of the People's Republic of China* supplies the rules of jurisdiction, specific for civil actions over contractual disputes involving foreigners, or disputes over property rights against a defendant who does not reside within the territory of the PRC. Article 243 states that, if the defendant has a representative organisation within the territory of the PRC, or has detainable property within the territory of the PRC, or the contract is signed or carried out within the territory of the PRC, or the object of litigation is within the territory of the PRC, a civil action against a defendant not residing within the territory of the PRC is under the jurisdiction of the court of the place where:

- the contract was signed;
- the contract was carried out;
  the object of the litigation is located;
- the defendant has property that can be detained;
- the infringements of rights have taken place; and
- the representative organisation of the defendant is located.

Most of these jurisdictional grounds are familiar to Australian conflict of laws lawyers. Further, somewhat similarly to in Australia, the parties to a foreign-related contract in the PRC have, with some limitations, the right to agree in writing to place the case under the jurisdiction of a court that has 'an actual connection with the dispute'.[11] If no forum is selected the rules outlined in art 243 of the *Law of Civil Procedure of the People's Republic of China* apply.

In addition to the requirement of 'an actual connection with the dispute', mentioned above, there are also other limitations placed on contractual stipulations of the forum to have jurisdiction. Several articles of the *Contract Law of the People's Republic of China* make the validity of unfair contractual terms, such as some jurisdictional clauses in contracts of adhesion (for example, click-wrap agreements and disclaimers), questionable. For example, art 3 states that 'neither party may impose its will on the other party'.[12] Further, the *Law of the People's Republic of China on Protecting Consumers' Rights and Interests* makes the validity of contracts of adhesion even more questionable.[13] For example, art 24 states that:

> … [b]usiness operators must not set unfair and unreasonable regulations against consumers by the use of format contract, circular, statement, shop or store notice and other means, or try to alleviate or avoid their civil responsibility they must bear for harming the legitimate rights and interests of consumers by resorting to the above means.[14]

In light of these very general rules, it could be argued that what otherwise would have been a valid contract is not even considered a contract if there is an unreasonably unequal division of power between the parties. However, it seems rather far-fetched to assume that the very existence of a power imbalance between the parties would invalidate the contract, and there are no court decisions indicating that such a strict interpretation is correct. A more reasonable approach is to assume that the focus is not on the power imbalance as such, but rather on the misuse of a power imbalance. If this is correct, the practical difference between the PRC rules and the Australian rules found, for example, in the *Trade Practices Act 1974* (Cth) is not that great.

Contracts of adhesion may also be governed by the provisions of the *Contract Law of the People's Republic of China* regulating standard contracts. Article 39 ensures the following.

> Where a contract is concluded by way of standard terms, the party supplying the standard terms shall abide by the principle of fairness in prescribing the rights and obligations of the parties and shall, in a reasonable manner, call the other party's attention to the provision(s) whereby such party's liabilities are excluded or limited, and shall explain such provision(s) upon request by the other party.
>
> Standard terms are contract provisions which were prepared in advance by a party for repeated use, and which are not negotiated with the other party in the course of concluding the contract.[15]

Furthermore, a standard term of a contract is deemed to be invalid 'if it excludes the liabilities of the party supplying such term, increases the liabilities of the other party, or deprives the other party of any of its material rights',[16] all of which can obviously be the consequence of a forum, or law, selection clause.

In summary, it could be said that the PRC's approach towards jurisdictional claims over contractual situations is rather similar to that of many other states; the parties' choice is ordinarily upheld except in some circumstances where protection is provided for a weaker party, and where no choice is made, the court searches for a forum with a close connection to the dispute.

Discretion to decline jurisdiction

In contrast to the laws of Australia and other common law countries, PRC law does not really recognise the doctrine of *forum non conveniens*. This does not mean, however, that there are no instances where a people's court may choose to decline exercising jurisdiction. For example, a prior foreign judgment may prevent the same matter from being heard in a people's court.[17]

While Chinese law does not expressly address *lis alibi pendens*, the doctrine is recognised in the practice of the people's

courts. In this context, it is interesting to note Kong and Hu's assertion that:

> … [i]t is not difficult to observe that People's Courts choose to accept or reject the doctrine of *lis alibi pendens* depending on whether the treatment would be favourable to the Chinese party.[18]

Concluding remarks

Should a PRC court claim jurisdiction over a foreign website, the website operator may find some comfort in the fact that the PRC's choice of law rules may point to the application of foreign law. Further, Australian courts will only recognise and enforce PRC judgments in rather limited circumstances. Both these factors impact on the severity of a PRC court claiming jurisdiction over an Australian website operator.

To summarise, while important differences exist, the relevant PRC rules are not fundamentally different to the law of many other countries, and indeed, at least so far the PRC has not made wide jurisdictional claims over foreign website operators. ●

Dan Svantesson, Assistant Professor, Faculty of Law, Bond University, Queensland.

This article is drawn from Svantesson D Private International Law and the Internet, *Kluwer Law International, The Hague/London/NY January 2007, forthcoming, which addresses the relevant laws of Australia, England, Germany, Hong Kong SAR, the PRC, Sweden and the US.*

Endnotes

1. Kong Q J and Hu M F 'The Chinese practice of private international law' (2002) 3 *Melbourne Journal of International Law* 435.
2. Paglee C D 'Contract law in China: drafting a uniform contract law' (Chinalaw Web; on file with author).
3. See *Provisional Regulations of the People's Republic of China for the Administration of International Connections to Computer Information Networks* (1997). I have been unable to ascertain whether this Provisional Regulation is still in force. However, the key point, that the PRC exercises a relatively strict control over what crosses the border to the PRC part of the internet, is beyond doubt. See, further, OpenNet Initiative 'Internet filtering in China in 2004–2005: a country study' <www.opennetinitiative.net/studies/china/>.
4. See, for example, 'Official reply of the Supreme People's Procuratorate on the application of laws to acts of illegally operating international, Hong Kong, Macao, or Taiwan telecommunication services', The Supreme People's Procuratorate, 6 February 2002 <www.isinolaw.com>.
5. *Law of Civil Procedure of the People's Republic of China 1991*, art 22.
6. Above.
7. The Supreme People's Court *Opinions (I–VII) of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China* 14 July 1992 para 304 <www.isinolaw.com>.
8. See, for example, *Measures on Internet Information Services 2000*, art 6.
9. Above note 5, art 5(1).
10. Above, art 237.
11. Above, art 244.
12. *Contract Law of the People's Republic of China 1999*, art 3.
13. That is, in relation to consumers.
14. *Law of the People's Republic of China on Protecting Consumers' Rights and Interests*, art 24.
15. Above note 12, art 39.
16. Above, art 40.
17. H K Yang's analysis attached to *Huigao Yuntong Co Ltd v Uchida Electronics Co Ltd and the Uchida Electric Appliances Manufacturing (Xiamen) Co Ltd for Joint Fraud and Act of Tort* 5 August 1995 Fujian Provincial Higher People's Court <www.isinolaw.com>.
18. Above note 1, pp 421–22.

Regulation of online banking Part 2: the application of APRA standards to online banking

Liong Lim and **Howard Cheung**
FREEHILLS

Part 1 of this article, which appeared in the last issue of the *Internet Law Bulletin*, (2006) 9(6) & (7) *INTLB* 78 introduced some of the regulatory challenges raised by the growth of online banking in Australia. The potential application of certain Australian Prudential Regulation Authority (APRA) standards to online banking activity was discussed, and two standards were highlighted: APS 231 (the 2002 Outsourcing Standard) and APS 232 (the BCM Standard).

Part 1 outlined the key provisions contained in each of the above standards. Part 2 will move beyond a discussion of the content of the standards and will analyse:

- the rules for determining when the 2002 Outsourcing Standard and the BCM Standard that will apply;
- the potential for those standards to apply to online banking activities; and
- the legal status of the standards and what this means for businesses which might need to comply with their provisions.

This article will conclude that, while the 2002 Outsourcing Standard and BCM Standard are not specifically expressed to target online banking

activities, the potential breadth of their application and the nature of modern day banking would mean that both standards will almost certainly apply to contracts for online banking activities. This article will observe, however, that there remain some areas where further clarity or guidance from APRA would be welcome.

Outsourcing

When does the 2002 Outsourcing Standard apply?

There are three general conditions that must be met for the 2002 Outsourcing Standard to apply to a particular contract.

Does the contract in question relate to an authorised deposit-taking institution (ADI)? APRA maintains a list of ADIs which includes Australian-owned banks, foreign subsidiary banks, branches of foreign banks, building societies, credit unions, specialist credit card institutions and authorised non-operating holding companies.[1] Contracts, by their nature, involve multiple parties. Consequently, any compliance obligations which attach to an ADI will affect the counterparty to the contract.

Does the contract relate to outsourcing? Paragraph 1 of the 2002 Outsourcing Standard defines outsourcing as 'an ADI entering into an agreement with another party (including a related company) to perform a business activity which currently is, or could be, undertaken by the ADI itself'.

The definition is intentionally broad. Paragraph 3 of the 2002 Outsourcing Standard makes it clear that the outsourcing concept is meant to cover joint ventures, strategic alliances or partnering arrangements:

- whether between ADIs and related companies or third-party entities;
- whether the service provider is located either within and outside Australia; and
- whether the outsourced functions are performed inside or outside Australia.

Does the outsourcing relate to business activities of a material nature? This requirement is somewhat misleading. At first glance, the condition appears to reduce the broad scope of the 2002 Outsourcing Standard created by the definition of outsourcing. Paragraph 5 defines a material business activity as 'one that has the potential, if disrupted, to impact significantly on the ADI's business operations, reputation or profitability'.

However, the 2002 Outsourcing Standard goes on to provide that, '[h]owever, in the normal course, APRA would expect ADIs to apply the practices set out in the Standard and Guidance Note to all outsourcing arrangements'.

APRA's attempt to clarify the operation of the standard in fact creates uncertainty and appears to cut across the requirement of materiality. The safer view for ADIs, therefore, would be to apply the 2002 Outsourcing Standard to all types of outsourcing.

If all three conditions set out above are met — that is, the contract in question involves an ADI, the contract relates to outsourcing, and the outsourcing is of a material business activity — then the 2002 Outsourcing Standard will need to be considered. Given the potential breadth of the wording in the standard, most outsourcing arrangements involving ADIs are likely to be affected.

How does the 2002 Outsourcing Standard apply to online banking?

The 2002 Outsourcing Standard is drafted in general, technology-neutral terms, without any express reference to online banking. However, given the potential breadth of its application, there is a possibility that the 2002 Outsourcing Standard would cover a range of activities that relate to online banking.

Any contract for the procurement of a business service for an ADI's online operations which either is, or could be, undertaken by the ADI itself, is an outsourcing arrangement under the terms of the 2002 Outsourcing Standard. Accordingly, the development of new website interfaces, the provision of website support services, even the creation of software code for a consumer website, are all activities which could be undertaken inhouse by an ADI. If any of those were to be subject to an outsourcing arrangement, there would be the potential for the 2002 Outsourcing Standard to apply.

Furthermore, given the confusion discussed above in relation to what kinds of outsourcing activities are material, it would be prudent for ADIs and their suppliers to take the 2002 Outsourcing Standard into consideration for most of their contracts.

What are a party's obligations if the 2002 Outsourcing Standard does apply?

As discussed in Part 1 of this article, the 2002 Outsourcing Standard imposes several obligations on ADIs entering into outsourcing arrangements which fall within the scope of the standard. These include, in brief, requirements that:

- a legally binding agreement must be in place to cover the outsourcing arrangements;
- APRA must be consulted prior to the contract being entered into for outsourcing to a service provider outside Australia, and APRA must be notified after the contract is entered into for outsourcing to a service provider within Australia;
- monitoring processes must be employed, including ensuring APRA has appropriate access rights to supervise and monitor; and
- the ADI must undertake appropriate due diligence and provide for contingency plans to bring services back inhouse.

These are general requirements that would apply to outsourcing of services relating to online banking in the same way as any other outsourcing contract. There are, however, certain obligations in the 2002 Outsourcing Standard which could give rise to additional considerations where the outsourcing relates to an online banking function.

In particular, para 16 of the 2002 Outsourcing Standard requires an ADI to monitor the outsourcing relationship. Specifically, the paragraph requires ADIs to ensure that they employ a process for regular monitoring of performance under the agreement, including meeting criteria

set out in the service level agreements. In a contract to outsource online banking functions, the service level agreement may be very detailed and is likely to cover areas such as the speed of transactions, online availability, conduct of helpdesk calls, data recovery and security. The monitoring of these areas of activity will need to be carefully conducted to satisfy the requirements of the 2002 Outsourcing Standard. IT law practitioners will be aware that monitoring of service levels is often an area of extensive negotiation. By making monitoring of service levels not just a commercially prudent practice, but one required by regulation, the 2002 Outsourcing Standard, arguably, adds an additional layer of complexity.

Business continuity management

The application of the BCM Standard

The scope of the BCM Standard is easier to determine than the 2002 Outsourcing Standard. Paragraph 5 of the BCM Standard simply provides as follows:

> APRA requires all ADIs to identify, assess and manage potential business continuity risks to ensure each ADI is able to meet its financial and service obligations to its depositors and other creditors.

Like the 2002 Outsourcing Standard, the BCM Standard does not expressly refer to online banking. The obligations contained in the standard, which are discussed below, refer to all the functions of the ADI. However, given that most ADIs engage in some form of online activity, ranging from the provision of information via a website to more complicated online transaction services, one would expect that managing business continuity risks would almost certainly include management of online risks.

Obligations under the BCM Standard

The BCM Standard outlines several specific obligations which ADIs must fulfil in order to meet their general obligation to manage potential business continuity risks. These were set out in detail in Part 1 of this article and included requirements that:

- an ADI must determine the potential financial, legal, reputational and other material consequences if the critical business functions, resources and infrastructure are unavailable;
- a written Business Continuity Plan (BCP) must be developed and implemented;
- if an ADI experiences a major disruption, it must notify APRA; and
- an ADI should have insurance arrangements in place to cover the costs suffered due to a business disruption.

Additional considerations for online banking

As with the 2002 Outsourcing Standard, the obligations under the BCM Standard are framed in technology-neutral language. However, additional considerations need to be taken into account when applied to online activities. There are two provisions which warrant particular comment.

First, the BCM Standard contains a requirement that ADIs put in place a BCP. Paragraph 25 defines a BCP as 'the documented procedures and information which enable the ADI to respond to a disruption, recover and resume critical business functions'. Paragraph 27 goes on to set out what is required in a BCP, including:

- the procedures to be followed in response to a material disruption to normal business operations, which should enable the ADI to manage the initial business disruption and recover and resume critical business functions, resources and infrastructure;
- a list of all resources needed to run operations in the event the primary operational site is unavailable;
- a communication plan for notifying key internal and external stakeholders if the BCP is invoked; and
- information about an ADI's alternative site(s) for the recovery of business and/or IT operations.

In an online banking context, special regard would need to be paid to internet issues. For instance, the communication plan would typically need to include lines of communication with the host provider for web-servers, and the identification of 'alternative sites' might include mirror servers instead of, or as well as, redundant office locations.

Second, the matter of how the BCP deals with security issues takes on greater significance in an online context. The BCM Standard does not specifically address the issue of breakdowns or outages caused by unauthorised access to computer systems or malicious hacking. For online activities, however, these are likely to rank among some of the most common risks.

In the authors' view, APRA could have avoided some uncertainty by mandating specific standards for online activities. In August 2004, APRA contacted all affected ADIs in relation to 'emerging threats to internet banking'[2] and recommended that ADIs undertake various actions to guarantee personal identification number (PIN) and password security for consumers, and also implement measures to minimise the risk of online fraud and identity theft. It would have resolved some uncertainty if APRA made it clear that those recommendations were covered in the BCM Standard or some other applicable standard.

Legal status of APRA standards

The 2002 Outsourcing Standard and BCM Standard were made under s 11AF of the *Banking Act 1959* (Cth). In particular, s 11CA of the *Banking Act* provides APRA with the power to direct an ADI to comply with a particular standard. Failure to comply with an APRA direction is a criminal offence. It is not clear, though, whether an APRA standard is merely a prudential recommendation or a compulsory standard.

It is the experience of the authors that APRA will generally commence the compliance process by discussing any potential non-compliance with the ADI, and undertaking appropriate information-gathering and monitoring activities, before issuing a notice under the *Banking Act*. At the point that APRA issues a direction, the status of the standard becomes clear, and

compliance with APRA's direction is compulsory. There is an argument that up until that point, however, the standards are merely guidelines as opposed to regulatory requirements. The issue has yet to be specifically tested by the courts. Accordingly, the safer view for parties engaging in a contract for outsourcing or business continuity services is that the contract should specifically refer to those standards, as opposed to merely requiring compliance with applicable law.

Conclusion: more regulation

The financial services sector has been subject to increasing regulation in recent years.

Both the 2002 Outsourcing Standard and the BCM Standard were implemented after 2002 and APRA intends to expand the scope of the obligations under each standard. While both standards, it is argued, are broad enough to cover online banking activities, the failure by APRA to specifically refer to internet banking means that ADIs and their suppliers must interpret general principles in an online context. As discussed, this can raise challenges.

Further regulation is also planned. At the time of writing, there has been extensive discussion of a draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2005 (Cth) (the AML/CTF Bill) which, if passed, would require various entities (including ADIs) to carry out customer identification procedures in relation to individuals, companies, trustees, partners in a partnership, associations, registered cooperatives and government entities.[3] Given the growth of online banking services, it must be the case that any identification process must be implemented for both online and offline application. Once again, though, the Bill seems to contemplate general principles, leaving it to ADIs and their IT suppliers to interpret the legislative requirements in an online context.

Call to action

Given the importance of online services to modern day banking, it is suggested that a more proactive approach is warranted. Especially with more regulations being passed either in the form of APRA standards or as legislation such as the Bill, specific guidelines for online activities would be a welcome clarification of existing principles.

The 2002 Outsourcing Standard and BCM Standard already go some way by laying down general themes that apply to financial services technology contracts as a whole. However, online banking is only a subset of financial services, with its own particular commercial risks. Applying general standards to particular types of services runs the risk of confusion. Guidelines as to how these standards would apply in the online environment would assist both banks and their suppliers. ●

Liong Lim, Senior Associate, and Howard Cheung, Solicitor, with Freehills TMT Group, Sydney.

Endnotes

1. Full list available at <www.apra.gov.au/adi/ADIList.cfm>.
2. See <www.apra.gov.au/ADI/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=7589>.
3. AML/CTF Bill 2006, s 29.

Casenote

An EU domain name dispute with 'the lot'

ARBITRATION CENTER FOR EU DISPUTES
CASE NO 01959

Top level domains (TLDs) for the EU, with the .eu suffix, became available on 7 December 2005. The European Registry of Internet Domain Names introduced a phased registration process to protect organisations from cyber-squatters. Until 7 April 2006, there was a four-month period known as the 'sunrise period', where only holders of prior rights to a name, for example, trade mark owners, could apply. The rules concerning the implementation and registration of .eu TLDs are set out under the Commission of European Communities Regulation (EC) No 874/2004 of 28 April 2004 (the Regulation). Disputes are governed by the *.eu Alternative Dispute Resolution [(ADR)] Rules* (the Rules). The ADR procedure is provided by the Arbitration Court attached to the Economic Chamber of the Czech Republic and Agricultural Chamber of the Czech Republic (the court).

Facts

A German citizen, Alexander Schubert, (the Respondent), applied to register '.lot.eu' (the disputed domain name) on the first day .eu TLDs became available. On 23 June 2006, Lot Polish Airlines (the Complainant) filed a complaint with the court. The Complainant had been the Polish national airline operator since 1929 and owned a number of registered trade marks and domain names featuring the word 'Lot'.

The Arbitration Centre Panel (the panel) will revoke or transfer a disputed domain name, where the domain name is identical or confusingly similar to a name in respect of which a right is recognised or established by the national law of a member state and/or EC law and either:

- the respondent has no rights or legitimate interest in the name; or
- the domain name has been registered or is being used in bad faith.[1]

According to the panel, however, the Complainant was required to prove the existence of each of the above. Fortunately for the Complainant, the panel's interpretation had no impact and the panel ordered that the disputed domain name be transferred to the Complainant. The panel's reasoning is discussed below.

Identical or confusingly similar

According to the Rules and the Regulation, the Complainant must:

- hold a name in respect of which a right of the complainant is recognised or established by national and/or EU law; and

- show evidence that the said name is identical or confusingly similar to the disputed domain name.

The panel concluded that the evidence of the complainant's ownership of its registered trade marks satisfied the first requirement and that the inclusion of the '.eu' suffix was irrelevant.

Right or legitimate interest

The Respondent submitted that it owned the German trade mark, LOT,[2] but failed to provide evidence of its use of that mark. The panel had to decide whether this ownership was enough of a 'right or legitimate interest'.[3] Although the panel conducted its own research, it was unable to find any evidence of the Respondent's use of its trade mark or that the Respondent had ever been commonly known as 'Lot' or of any legitimate, non-commercial or fair use of the term 'Lot'. According to the panel, trade mark registration does not automatically provide a 'legitimate right or interest'. In the panel's opinion, a genuine legitimate right should be based on clear evidence demonstrating that the trade mark registration was obtained in good faith and for the purpose of making a good faith use of that mark. The panel found that the lack of use, combined with the respondent's behaviour in connection with the registration of other trade marks and domain names corresponding to third parties' trade marks, enabled it to conclude that the registration of the trade mark was not a genuine or legitimate right or interest.

Bad faith

Under the Rules and the Regulation, examples of 'bad faith' include:

- where a domain name was acquired primarily for the purpose of selling it to the holder of an earlier right in the name; or
- the respondent has a pattern of registering domain names so as to prevent earlier rights-holders from doing so.[4]

The complainant submitted that the respondent was the CEO of a Californian company specialising in 'internet domain strategy consulting services'. According to the complainant, in many (if not all) cases, the trade marks and domain names were registered with a view to claiming compensation from the owners. The panel noted that many of the websites connected with third-parties' trade marks were 'inactive'.[5] It therefore concluded that the Respondent was not 'developing bona fide activities' with these domain names.

According to the Complainant, the registration was also made in bad faith based on the Respondent's involvement in other UDRP proceedings.[6] The panel agreed that there was a pattern of cyber-squatting conduct, finding it 'obvious' that the registration of the disputed domain name followed the same bad faith purposes in the other Uniform Dispute Resolution Policy (UDRP) proceedings.

Finally, although the Respondent did not ask to be paid for the transfer of the disputed domain name, there was some suggestion that if the Respondent did agree to a transfer, the Complainant would also be required to 'take' his LOT trade mark, which may have required compensation. The panel found this proposal surprising if the assets were essential to the development of the respondent's commercial activities. In the panel's view, the respondent's proposal 'diluted any presumption of fairness' and there was an element of 'bad faith'.

Comment

The decision is of interest as it shows that the court may look 'behind' any rights respondents may seek to rely on, even if those rights are registered trade marks dating before the domain name existed. It also serves as reminder of the importance of keeping records, for example, business plans, demonstrating a bona fide intention of using a domain name given that, unlike trade mark law, there is no formal grace-period for non-use. ●

Andrew Jaworski, Solicitor (Australian Qualified), Field Fisher Waterhouse, London.

Endnotes

1. Article 11(d)(1) Rules; art 21.1 Regulation.
2. Trade mark No 30124140 (13 April 2001) for pharmaceutical and veterinary products and substances to cure firework burns.
3. Article 11(e) Rules; art 21.2 Regulations.
4. Article 11(f) Rules; art 21.3 Regulation.
5. For example, CLUBMED.INFO or NBC.DE.
6. See Case No D2001–1274 *Koninklijke Luchtvaart Maatschappij NV v Excelsa Czop*.

PUBLISHING EDITOR: Bridget Brooklyn BA (Hons) PhD **MANAGING EDITOR: Anupama Bhattacharya PRODUCTION: Christian Harimanow**
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
TELEPHONE: (02) 9422 2222 FACSIMILE: (02) 9422 2404 DX 29590 Chatswood www.lexisnexis.com.au bridget.brooklyn@lexisnexis.com.au
ISSN 1329-9735 Print Post Approved PP 244371/00049 Cite as (2006) 9(8) *INTLB*