

## **ENFORCEMENT OF COPYRIGHT AGAINST CYBERSPACE BANDITS**

*Christopher J. Whitelaw<sup>1</sup>*

### *Introduction*

A cyberspace bandit, for the purposes of this paper, is someone who infringes someone's copyright on the Internet. A cyberspace bandit is a tortfeasor and can be sued and/or prosecuted if he, she or it can be caught.

I have already published a paper last year called "Copyright and the Internet – An appraisal of the Government's Digital Agenda Reforms" which endeavored to review and appraise the federal government's digital agenda reforms contained in the *Copyright Amendment (Digital Agenda) Bill 1999*<sup>2</sup>. It attempts to evaluate whether and to what extent the reforms will, as the Attorney General claims they will, 'fill the gaps in copyright protection in the on-line environment'. That paper, first presented at the State Legal Conference last year, has also been serialized in the last three editions of the *Australian Intellectual Property Law Bulletin*, published by Prospect Publishing. In that paper I summarise the reforms contained in the Bill which relate to enforcement and remedies and provide some degree of analysis and commentary. This paper examines the issue of enforcement in more detail.

The reform bill was tabled in Parliament in September last year. It was then sent for review by the House of Representative's Standing Committee on Legal and Constitutional Affairs (the "Andrews Committee"). That Committee published an advisory report in November 1999 which was tabled in December. The Committee made 38 recommendations in its report. The government accepted 21 of them.

The Bill was re-presented and read a second time by the Attorney General on 27 June 2000. The Attorney indicated that the government, as a result of the Standing Committee's recommendations and its further consultation with key stakeholders, intended to make further amendments to the Bill. Further amendments were made and the Bill became law on 4 March 2001.

During the second reading speeches, Kevin Andrews, who chaired the review committee, highlighted the fact that once you digitize a book or sound recording, which practice is now commonplace, it can thereafter be copied thousands of times without reducing its quality. Even the one-millionth copy would still be a mint copy of the original. Anyone with a

---

<sup>1</sup> The author is a NSW Barrister.

<sup>2</sup> The *Copyright Amendment (Digital Agenda) Act, 2000* came into force on 4 March 2001.

computer and a modem, who gains access to one of those digitized copies, can, by the press of the button, email it as an attachment to hundreds or thousands of other people.

Mr Andrews gave this example to illustrate what was the central focus of his review committee – “Its concern was that the creator (of a work) should be able to have some say in what happens in the copying of that material. It is about a balance of interests. It is a balance between on the one hand the owner or creator of material, who, having a property interest in that material, is entitled to say whether they want it passed on, whether they want it passed on for a fee or whether they want it passed on freely to somebody else; and the other interest which is incumbent in this debate, and that is the way which we as a society..... say that there is an advantage in much information being available to as many people in the community as possible.”

As Mr Andrews observed – “We, as a Parliament, are for the first time deciding what the law should be in relation to copyright so far as digital material is concerned.” His committee recommended that the Bill be amended so as to give to copyright owners the ‘right of first digitization’. The government has accepted this recommendation and the Bill will be amended so as to convey that right to copyright owners as a subset of the right of reproduction. This amendment means that the owner of a copyright should have some say in whether or not the hard copy is transferred onto a floppy disk or reproduced into digital format – a format which will immediately place it at risk of unauthorized copying and dissemination to a vast audience without the copyright owner’s consent.

The government indicated that there would be a substantial increase in the criminal penalties for infringement, and that the Act would include an explicit power for the court to award *additional damages*<sup>3</sup> on a civil action where an infringement involves the first digitization of copyright material. In addition, in response to the Standing Committee’s report, the government has stated that the regulations will be amended to require that notices under the Copyright Act explicitly refer to the additional criminal penalties and civil damages that will apply. It will also make it clear that the fair dealing exception, which will permit the copying of a reasonable portion for purposes of research and study, will not include any communication of such material to other persons.

#### *The Key Issues for Enforcement against Cyberspace bandits*

The key issues are –

1. Make strategies for Protection and Prevention the first priority – technological protection measures/electronic rights management/community education/surveillance;
2. Identifying the infringement;
3. Identifying the bandit or entity to be sued/prosecuted;
4. Deciding on the most effective remedy to pursue –
  - i. jurisdiction;

---

<sup>3</sup> Section 115(4)(b) (ii) of the Act.

- ii. civil v criminal or both;
- iii. If civil –
  - Pre-emptive strike? Anton Piller/Mareva Injunction<sup>4</sup>;
  - Injunction? Damages? Or both?
- iv. cost/benefit/affordability;
- v. problems of evidence and proof – liability and damages.

It is not intended in this paper to set out or discuss the law concerning civil remedies for copyright infringement per se. There is literally no decided law in this country specifically dealing with infringements of copyright on the Internet. Most of the action is taking place in the American Courts. The purpose of this paper is to highlight the issues, the potential problems and to consider the utility of the digital agenda reforms in overcoming these problems.

As some of you may be aware, the House of Representatives Standing Committee on Legal and Constitutional Affairs received a reference from the Attorney General on 17 March 1999 to inquire into the state of copyright infringement in Australia and the appropriate mechanisms by which to respond to such infringement. The Committee held public hearings and received a wide range of written submissions. It suspended its inquiry in order to await the tabling of the government's *Copyright Amendment (Digital Agenda) Bill* and to consider the submissions presented during the government's consultative process on the draft Bill.

After reviewing that Bill the Standing Committee resumed the inquiry and published its report entitled "Cracking down on Copycats: enforcement of copyright law in Australia" in November 2000. The report contains 22 recommendations. Many of these recommendations have not yet been taken up by the government and included in the *Copyright Amendment (Digital Agenda) Act, 2000*. It may well be that the government needs further time to evaluate some of these recommendations.

I will be summarizing some of the main points presented in the written submissions prepared by some of the major stakeholders later in the paper. Those submissions addressed, inter alia, the following issues –

- i. options for copyright owners to protect their copyright against infringement, including use of the existing provisions of the *Copyright Act*, use of other legislative provisions apart from the *Copyright Act*, and technological or other non-legislative measures for copyright protection.

---

<sup>4</sup> Note that the House of Representatives Standing Committee on Legal and Constitutional Affairs, in its "Cracking Down on Copycats: enforcement of copyright in Australia" report presented in November 2000 recommended (Rec. 12) that "a provision be introduced into the *Copyright Act 1968*, similar to section 100 of the *Copyright, Designs and Patents Act 1988 (UK)*, which authorises a copyright owner or his agent to seize a copy of their work (or other subject matter) that is offered for sale or hire from a place other than a regular or permanent place of business." This amendment, if made, would grant to a copyright owner a civil power of seizure.

- ii. the adequacy of criminal sanctions against copyright infringement;
- iii. the adequacy of civil actions in protecting the interests of plaintiffs and defendants in actions for copyright infringement;
- iv. the desirability or otherwise of amending the law to provide further procedural, evidential or other assistance to copyright owners in civil actions for copyright infringement.

I will be considering these submissions in the light of the amendments to the *Copyright Act* contained in the *Copyright Amendment (Digital Agenda) Act, 2000*, which came into effect on 4 March 2001. I will try to evaluate to what extent the Act, addresses the concerns raised in the submissions to the Standing Committee. The focus of this paper is on copyright infringement in cyberspace.

#### *An Illustration of the Problem*

The factors listed above could be applicable to any alleged infringement of copyright, whether in hard copy format or on the Internet. The only difference is that in cyberspace the decision making process facing the copyright owner may be far more complicated and confusing.

As you all know, the Internet is a global environment, and therefore potential infringers of a copyright subsisting in Australia may be located anywhere in the world. Anyone with a PC anywhere in the world could be the cyberbandit. Before the copyright owner can say "Jack Robinson" infringement on a massive scale may already have taken place. And yet, it may prove impossible for the copyright owner to identify a suitable entity to take enforcement action against, and even if an infringer is found, action taken against that infringer may have little impact in stopping an ongoing infringement of the copyright. Because of the ease and speed of reproduction on the Internet, once the first infringement takes place it is very difficult to quarantine it. Unfortunately there is, as yet, no Norton Anti-Virus type remedy which can be utilised.

This is why the emphasis of the digital agenda reforms is focused on Prevention and Criminal Sanctions and on Website owners and Internet Service Providers, as opposed the millions of Internet users worldwide. This emphasis, and the rationale for it, is explained in detail in my earlier paper.

Copyright violation is easy and widespread on the World Wide Web. Some would say that it is part and parcel of the Internet and therefore anyone who places copyright material on the Internet does so with this understanding. If they fail to make use of rights management protocols and effective technological protection measures then anyone accessing their material is likely to have an implied license to reproduce it. It is a self-help environment. The onus is on copyright owners to make use of all available measures and devices to protect their copyright. If they do not, then they should not be heard to complain.

Today, software exists that will “watermark” images with copyright information, embedding proof of ownership and making it easier to identify violations. Software is being developed with will embed digital files with Java applets that prevent downloading and sending as email attachments. Companies have come into existence that will search the Web for copyright violations on behalf of clients.

So, the real concern should be how to protect the rights of copyright owners who either do not authorise their work to be published or disseminated or made available on the Internet; or who choose to do so protected by rights management protocols and effective technological protection measures. How can they best enforce their rights if they are infringed by cyberspace bandits?

The real threat tends to come from the following sources –

- Piracy;
- Hackers;
- Web site Proprietors;
- Irresponsible Internet Service Provides;
- PC end users as a global collective entity or phenomenon impacting upon copyright owners’ commercial interests.

Effective remedies, civil and/or criminal, can be sought against all of these categories of offenders except the last one unless the end user can also be shown to be engaging in the infringing activity for commercial gain. The digital agenda reforms implemented in the *Copyright Amendment (Digital Agenda) Act* recognise the futility of trying to control the millions of end users on a global Internet. This is simply recognising the essential nature of the Internet.

There is no doubt that end users can seriously damage the commercial interests of a copyright owner. Individually and collectively, they can be responsible for a massive amount of unauthorized copying and dissemination of material. It is now easy and inexpensive for anyone to use a scanner to scan someone’s written work onto a hard-drive and then post it on some website or bulletin board. It is easy to upload music from a CD on to a server in order to permit someone else to download it and listen to it – free of charge.

Three recent examples of cyberspace infringement will serve as a useful illustration of the problems potentially faced by copyright owners in this country.

1. Recording Industry Association of America(RIAA) and Metallica v Napster Inc. ;
2. Gnutella – decentralized “freeware” technology.
3. The ‘mousetrapping’ phenomenon.

Napster is a web site in the US that allows PC users to access the website, choose digital music files stored on the website server and then download them for their personal use. They call it "swapping" songs. There is no charge. A Napster customer can use the facility to swap musical files with other customers. It is a form of trading music online. It is done without seeking any prior authorization or license from the copyright owners of the sound-recordings or the musical works.

The technology that permits users to do this is called MP3 – a digital compression format that turns music on compact discs into small computer files that can be easily sent back and forth over the Internet. Once a music file is downloaded from Napster to the user's PC, if the user also has a portable music player called the "RIO", he or she can then easily and quickly download the music file from the PC to the RIO. This will then permit the user to listen to the music file using digital technology, which will ensure that there is no degeneration in the sound quality. MP3 is a standard non-proprietary compression algorithm freely available for use by anyone. Once downloaded, it can be sent to any number of other users without any loss of quality in the sound.

The proponents of MP3 and Napster argue that all it does is to facilitate private, non-commercial use of copyrighted recordings. This is permitted in the US by the Audio Home Recordings Act 1992. However, there is no such right in Australia.

On 26 July a federal judge in San Francisco granted a temporary injunction restraining Napster Inc. from trading music online, pending a trial. The decision has been hailed by the US Recording Industry as a major victory. The Industry has viewed Napster as a dangerous Internet rival that could short-circuit traditional music sales.

During the hearing of the injunction application, the judge, Marilyn Hall Patel, said that the online company was encouraging wholesale infringing against the music industry. She said, "when the infringing activity is of such a wholesale magnitude, the plaintiffs are entitled to enforce their copyrights."

The judge ordered the Recording Industry Association of America (RIAA) to post a \$5 million bond against any financial losses Napster could suffer from being shut down temporarily. RIAA's lawyer claimed that the decision "establishes that the rules of the road are the same online as they are offline, and that it sends a strong message to others that they cannot build a business based on others copyrighted work without permission."

Napster's lead lawyer is David Boies, who headed up the US Justice Departments legal team that did combat recently with Microsoft. He immediately lodged an appeal against the temporary injunction. He had argued during the injunction hearing that the personal copying of music online was protected by federal 'fair use' laws, and that it encouraged the sampling of new music and promotion of new artists. He argued that the service should be

considered a non-infringing use as defined by the precedent-setting *Sony Betamax case*. The judge, rejecting that argument, said that it was hard to envision applying the fair use principle to a world-wide service of 20 million users. Napster users are able to trade song files through more than 100 central computer servers at Napster.

RIAA has claimed that this "song-swapping" via Napster has cost the music industry more than \$300 million in lost sales. The opposing camp disagrees and counter-claims that users of Napster and other music sharing programs are 45 percent more likely to increase their music purchasing than fans who are not trading digital bootlegs online.

On 28 July a federal appeals court granted Napster's request for an emergency stay to keep the music swapping service operating. The two appeal judges said that 'substantial questions' had been raised about the 'merits and form of the injunction.' The appeals court wanted further time to consider the matter. It may take up to several months for it to make a final decision as to whether an injunction should be granted or not, and on what terms. Napster's Motion before the appeals court stated that Judge Patel had erred by attempting to 'adapt existing copyright provisions to the new realities of Internet technology.'

The final trial between Napster and the Music Recording Industry is being cast as a David v. Goliath battle between a Silicon Valley upstart and the giants of the recording industry. Its outcome may well determine the future of music and copyright law.<sup>5</sup> The second skirmish between Napster and the Recording Industry was played out in the US Court of Appeals hearing of the Appeal against Judge Patel's preliminary injunctions. On 12 February 2001 the U.S. Court of Appeals for the ninth Circuit handed down a decision adverse to Napster. A full transcript of that judgment can be located on the Internet.<sup>6</sup> [The key points of the judgment and its ramifications to be discussed as part of the seminar presentation]

In essence, the Court of Appeals found that the preliminary injunction granted by the District Court was both warranted and required but its breadth and scope needed modification. It gave direction to the District Court as to how the injunction had to be modified. The matter was then remitted back to the District Court.

#### *Gnutella – Decentralized "freeware" technology*

Online music-swappers/traders say that if Napster loses its battle and is closed down, that will have no effect on Gnutella and other decentralized 'freeware' technologies which have been spawned by Napster. With Gnutella there is no central website and servers to enable the swapping of music. The song files can be traded directly between a constantly changing collection of computer users. It works on a distributed network system. Instead

---

<sup>5</sup> Since this paper was written the case between Napster and one of the complainant record companies has been settled. The settlement involved Napster agreeing to enter into a license agreement with that company.

<sup>6</sup> <http://www.ce9.uscourts.gov/web/newopi>.

of having central servers maintain a list of available files, each user's computer is in effect a server.

Both Napster fans and technology experts are saying this is only the beginning of the battle over copyrights on the Internet. They say that the number of file-swapping software programs will be impossible to police and close down.

*The Mousetrapping Phenomenon on the Net*

This occurs where a cyberspace bandit, located anywhere in the world, makes copies pages off web sites belonging to others, by stealing them off some central server where the web sites are posted (in some other part of the world) and then re-posts them on some other server on the world wide web. When search engines like Yahoo or Alta Vista are requested by an internet user to locate one of those web sites they are unable to distinguish between the original and the copied web page. This results in thousands of person logging in to the stolen site only to find that they have been hijacked. On arriving at the hijacked site they are then redirected to a hard-core porn site (gambling site or whatever) where they become 'mousetrapped'. This means that they are bounced through a maze of interconnected sites across vast geographical boundaries.

What can a copyright owner do in such a situation? The copyright is being violated in the most brazen and blatant way. The copyright owner's commercial interests are at serious risk. If the violation continues without check it may even spell financial disaster for that owner's Internet business. And at the owner's expense the cyberspace bandit is possibly making a very good profit. It is literally impossible to locate the perpetrator of the violation. He or she could be anywhere in the world. What remedy could the owner obtain from his or her own domestic courts? The quick answer is that civil remedies would not provide any solution. The solution, if any, would have to come via law enforcement and criminal sanctions. But even that is problematic as such things as page-jacking, mousetrapping and disabling user's browsers have not yet been identified as criminal offences. In this sense, the statement that the Internet is the "wild west" rings true.

*What Solutions might there be to these sorts of Copyright Infringements in Australia once the digital agenda reforms have become part of Australian Copyright law?*

In the Napster scenario, provided the Courts could exercise jurisdiction over the offender, the activity of Napster would be a clear infringement of copyright in the sound-recordings. Napster would not find any refuge or comfort in the Australian fair-dealing laws. Therefore jurisdiction would be the only potential impediment to obtaining a civil remedy. The target defendant would be Napster and not any of the Internet users down-loading the MP3 music files. Pursuing them could be like swatting flies.

The Gnutella scenario is more problematic as there is no web site proprietor or Internet service provider to target. It would seem that either civil remedies would have to be sought against individuals who can be proved to be infringing the copyright in sound

recordings by making unauthorised copies. The hurdles facing the copyright owners would be identifying the offenders and the likely lack of jurisdiction to obtain remedies against offenders who do not reside in Australia.

Relying on criminal sanctions<sup>7</sup> provided under Part V Division 5 of the Act might also prove difficult because the activity is all happening in private, between the participants PCs, and does not involve any sale or letting for hire. There is no violation of electronic rights management information or technological protection measures involved in the activity. However, with the proposed digital agenda amendments to Section 132 (5A) of the Act a participant in the Gnutella music file swapping could be found guilty of *distributing* an infringing copy of a sound recording if it can be proved that he or she *transmitted* it after receiving it or recording it "so as to result in the creation of an infringing copy". In such a case the transmission would be deemed to be a distribution of the infringing copy.

In the Mousetrapping scenario no civil remedy would be available unless the offender was located within the jurisdiction and was in a position to put a stop to the infringing activity, and no criminal remedy would be available until such time as web-page hijacking and mousetrapping are made criminal offences. An offence would be committed under the digital agenda amendments if the hijacking involved some circumvention of an '*effective technological protection measure*' aimed at stopping a cyberspace bandit from gaining access to the web page and/or making any copy of it.<sup>8</sup>

*The Remedies and Enforcement Scheme under the federal Copyright Act incorporating the proposed digital agenda amendments*

The scheme is contained in Part V of the Act. Division 1-4 covers *civil remedies* and Division 5 covers *criminal offences and penalties* and Division 6 contains miscellaneous provisions that apply to both civil and criminal proceedings.

As previously stated, it is not the purpose of this paper to talk about remedies per se, but to identify and discuss particular issues of enforcement of copyright of particular relevance to the Internet and the digital environment in which infringement may occur.

The key issues thrown up by the digital environment would include –

1. Identifying the relevant breach of copyright;
2. Identifying and locating the culprit;
3. Deciding on which culprit to pursue;
4. Deciding on choice of remedy – civil or criminal or both – which would be most effective<sup>9</sup> in the circumstances? ;

---

<sup>7</sup> The Act provides for jail terms for up to 5 years for guilty offenders.

<sup>8</sup> Section 132 (6) of the Act provides that the section (Offences) only applies to acts done in Australia.

<sup>9</sup> Both from a time perspective and a cost of enforcement perspective.

5. Determining whether a domestic court would be able to exercise jurisdiction over the culprit and the offending conduct;
6. If jurisdiction was available, the ability to enforce any judgment.

I have to some extent already addressed these issues in my earlier paper<sup>10</sup> mentioned at the start of this paper. I do not intend to repeat what contained in that earlier paper. I simply want to add to it. However, one thing that I want to emphasize again – any owner of copyright who chooses to place their works on or make their works available via the Internet must avail themselves of whatever self-help measures are available to them to protect their copyright. Otherwise they should not really be heard to complain if infringement occurs. To choose not to make use of available self-help protection measures is simply an open invitation to those who are minded to infringe.

What I wish to address are the breaches of copyright that are more deserving of sympathy and attention. I wish to address three types of infringement -

- i. Infringement activity that involves digitizing, copying and distributing and making available copyrighted material on the internet (whether or not for profit or commercial gain) without the permission of the owner of the copyright;
- ii. Infringement activity which involves deliberately violating a copyright owners self help measures to protect and control use of their material placed on the Internet;
- iii. Infringement activity that in some way violates a copyright owner's legitimate use of the Internet to conduct business or to carry on some lawful interaction with members of the public from their web site.

The Napster and Gnutella activities discussed above are examples of the first type of infringement. The 'mousetrapping' activity is certainly an example of the third type of infringement and might also involve the second type of infringement.

## CIVIL REMEDIES

### *Identifying the relevant actionable breach of copyright and a viable defendant*

This is also discussed at length in my earlier paper. If the culprit is an individual, within the court's jurisdiction, and if the remedy sought against the individual will bring a stop to the infringement, then by all means go for the individual. However, if such an individual exists as the obvious defendant, that individual is most likely going to be a web site proprietor or some kind of distributor or facilitator of the infringing activity, rather than PC end user who is simply benefiting from the activity. Such an end user is likely to be amongst a thousand or a million other such end users.

---

<sup>10</sup> Copyright and the Internet – an appraisal of the federal government's digital agenda reforms", 1999.

If the statutory requirements for an authorized infringement<sup>11</sup> under the proposed amendments to s39 of the Act can be made out, then action brought against an Internet service provider (ISP) whose server or servers are facilitating the continuation of the infringing activity may be the preferable target of any demand or litigation. It may be that the ISP is not yet aware of the infringing activity and hence it may not become at risk of liability under s.39 until being notified of the activity and its infringing nature by the copyright owner. The new s.39B makes it clear that it will not be held liable simply because its facilities are being used by the person or persons engaged in the infringement. When it possesses the necessary knowledge and awareness of the activity, then whether or not it is later found to be liable for 'authorising' it will depend on findings made as to its power to prevent the activity and whether any steps it has taken to prevent or avoid the continuation of the activity can be judged as 'reasonable'.

If the infringing activity is being hosted on or facilitated by servers located outside of Australia, accessible to PC Internet users in Australia, the situation becomes even more complicated for the owner. In this situation the domestic servers being utilized by the domestic Internet users may not be in a position to do anything about it to prevent or avoid the continuation of the infringement. The infringing activity is not emanating from any web site or bulletin board hosted by its own servers. The issue would firstly be whether it could block the use of its own servers from being used to transmit infringing transmissions from the source to the end users; and the second issue would be that if it could do so, could it be done in a way and at a cost to the ISP that would satisfy the 'reasonable steps' criterion of the new s.39(1A) of the Act. If it would place an undue burden on the ISP to prevent or avoid the offending activity, it might not be obliged to do it because it exceeds what would be considered 'reasonable'.

The digital agenda act introduces new civil remedies in Division 2A to permit copyright owners to bring actions in relation to circumvention devices and electronic rights management information. These amendments are found in sections 116A – 116C. The potential relief that a court may grant is that contained in s.115 and s.116 of the Act.

The new civil remedy is directed at a person who, without the permission of the owner or licensee of the copyright in a work or other subject matter that is protected by an effective technological protection measure (ETPM), does any of the following acts –

- i. makes a circumvention device (CD) capable of circumventing, or facilitating the circumvention of the ETPM;
- ii. sells, lets for hire or offers or exposes for sale or hire such a CD;
- iii. distributes such a CD for the purpose of trade, or for any other purpose that will affect prejudicially the owner of the copyright;
- iv. exhibits the CD in public by way of trade;
- v. imports such a CD into Australia for any of the above purposes;

---

<sup>11</sup> The principles are discussed in my earlier paper.

- vi. makes such a CD available online to an extent that will affect prejudicially the owner of the copyright;
- vii. provides a circumvention service (CS) capable of circumventing, or facilitating the circumvention of the ETPM.

To escape liability under this section a person who does any of these acts will carry the onus of satisfying a court that at the time of doing the act he, she or it did not possess the requisite mental state to attract liability. The requisite mental state is that the offender “knew or ought reasonably to have known, that the device or service would be used to circumvent, or facilitate the circumvention of the ETPM.” In other words civil liability can be established on the basis of constructive knowledge as well as actual knowledge. This obviously favours copyright owners. The requisite knowledge will be presumed if the defendant is not able to prove the contrary. In other words it is a rebuttable presumption.

However a complete exemption is given to the maker or importer of a CD if it is made or imported –

- a. for use only for a “permitted purpose”; or
- b. for the purpose of enabling a person to supply the CD, or to supply the CS, for use only for a “permitted purpose”.

The supplier of a CD or CS is let off the hook completely if the recipient gives the supplier before, or at the time of, supply a declaration signed by him stating that the device or service is to be used only for a “permitted purpose” and identifies the purpose.

S.116A (7) of the Act provides that a CD or a CS is taken to be used for a “permitted purpose” only if:

- a. the device or service is used for the purpose of doing an act comprised in the copyright in a work or other subject matter; and
- b. the doing of the act is not an infringement of the copyright in the work or other subject matter under section 47D, 47E, 47F, 49,50,183 or Part VB.

This is another victory for copyright owners and licensees. Following its considerations of submissions on its draft exposure Bill the government has decided to limit the scope of “permitted purpose”. As earlier drafted the section would have included the fair dealing exceptions within the scope of permitted purpose. The re-drafting limits it to the new exceptions permitting the reproduction of computer programs to make interoperable products, to correct errors and for security testing, the exceptions for libraries and archives and the remunerated exceptions for educational institutions and the Crown.

Copyright user groups had strenuously argued against such a restriction being introduced. They wanted to ensure that the amendments did not limit the operation of the limitations or exceptions to copyright contained in the Act. They argued against the copyright owners that it was quite proper that the law would permit users access to circumvention devices for ‘legitimate non-infringing purposes’, such as the fair dealing purposes. They argued,

contrary to the copyright owners, that this was striking the right balance between the interests and that it was consistent with the international standards set by the WIPO Treaties.

Article 11 of WIPO Copyright Treaty requires adequate legal protection and effective legal remedies against the circumvention of technological measures used by owners "in connection with the exercise of their rights under the WIPO treaties....and used to restrict acts which are *not authorized or permitted by law.*" Hence, the user groups argued that the treaties did not require protection and remedies against circumvention where the circumvention is done in order to facilitate a use of copyright material that is permitted by law, for example in reliance on the fair dealing exceptions.

The Parliamentary Standing Committee, which reviewed the digital agenda Bill, considered the changes that the government introduced to the Bill concerning exceptions to the rule against circumvention. It noted that the "permitted purposes" exceptions did not represent all the exceptions to infringement under the Copyright Act. It concluded that there was a need to allow copyright users to use circumvention devices in pursuit of legitimate purposes, but felt that the government had struck an appropriate balance between copyright owners and users by introducing the section on "permitted purposes" which was not previously included in the exposure draft of the Bill.

#### *Jurisdiction*

"When courts attempt to apply traditional territorial based jurisdictional rules to cyberspace, the situation becomes even more complicated, due to lack of geographical or physical boundaries. The Internet permits users to keep both their identity and location anonymous, so there may be no correlation between a person's Internet identity and address and their actual identity and address."<sup>12</sup>

This paper is not going to include a treatise on jurisdiction. I am simply highlighting some issues peculiarly relevant to copyright and the Internet. The Internet, as another author<sup>13</sup> has recently pointed out, complicates the application of complex territorially based jurisdictional principles because:

- i. material posted on the internet has a worldwide audience;
- ii. there is an enormous and growing number of internet users internationally;
- iii. it is easy to move a website from one jurisdiction to another;
- iv. a website can be hosted in one jurisdiction, while other parts of the website are hosted in another jurisdiction; and
- v. it is not always possible to determine where a website or a user is located.

---

<sup>12</sup> Jew, B, 'Cyber jurisdiction – emerging issues and conflicts of law when overseas courts challenge your web', (1998) *Computers & Law* 24 at 25.

<sup>13</sup> Gaye L Middleton and Jocelyn Aboud – 'Jurisdiction and the Internet', a paper included in 'Going digital 2000 – Legal issues for e-commerce, software and the internet' published by Prospect Media Pty Ltd.

As the same author pointed out in her paper, "As territorial based principles of jurisdiction are difficult to translate to the internet, which defies territorial boundaries, the law regarding jurisdiction in cyberspace remains unsettled. There appears to have only been one case so far, decided in Australia, dealing with jurisdiction in relation to the internet. This is the case of *Macquarie Bank v Berg* [1999] NSW SC 526.<sup>14</sup> This single decision is hardly enough to have produced any settled principles to apply in this area. Hopefully this will emerge in due course from further litigation.

For an Australian Court to be able to exercise jurisdiction the following elements have to be satisfied –

- i. The defendant has to have been validly served with process, or else have voluntarily submitted to the jurisdiction;
- ii. The Court has to be satisfied that the local jurisdiction is the appropriate one. It has discretion to decline jurisdiction if it forms the view that the jurisdiction is clearly inappropriate.<sup>15</sup>

In the recent case of *Macquarie Bank v Berg*, the Plaintiff sought an injunction to restrain the defendant from publishing defamatory material on the internet. The defendant was not resident in NSW or in Australia. The acts done by him were most likely done in the United States. His action was to post the alleged defamatory statements on a foreign website. Persons residing in NSW could access that website and read the material.

The judge refused the injunction. Although she found that the court was empowered to restrain conduct occurring or expected to occur outside of the jurisdiction, she declined to exercise that jurisdiction in this instance because 'it would exceed the proper limits of the use of the injunctive power of the court.' She also noted that any order she made would only be able to be enforced if the defendant were to return to NSW. The unenforceability of the order was another factor against granting the order sought by the plaintiff.

During the argument in the case the special problems posed by the internet were discussed. It became clear that there was no means by which the transmission of material on the internet could be restricted to a certain geographic area. The judge explained that she could not impose NSW law 'throughout the world'. An injunction granted by a NSW court was designed only to ensure compliance with NSW law. It is not intended to operate in other jurisdictions.

It remains to be seen whether in cases which arise in the future the Australian courts will develop a set of principles to establish jurisdiction over foreign defendants similar to those

---

<sup>14</sup> A decision of Simpson J.

<sup>15</sup> As to the factors relevant to considering whether the forum is appropriate see *Oceanic Sun Line Special Shipping Co Inc v Fay* (1988) 165 CLR 197; *Spiliada Maritime Corporation v Cansulex* [1987] AC 460; *Voth v Manildra Flour Mills Ltd* (1990) 171 CLR 538.

which have emerged in the US. The US courts have distinguished between general jurisdiction and special jurisdiction.<sup>16</sup> The criteria that must be established to found special jurisdiction over a foreign defendant includes –

- i. the defendant purposefully availed itself of the privilege of doing business within the forum state;
- ii. the relevant cause of action arises from the defendant's activities within the forum state; and
- iii. the exercise of jurisdiction would be fair and reasonable.

Naturally, wealthy plaintiffs may possess greater options than financially weaker ones in that if they can identify and locate the culprit in another country they may be able to move swiftly to restrain that defendant using the laws of the foreign country. This will naturally depend on whether the laws of the foreign country will favour the plaintiff and provide it with the remedy sought. Most copyright owners will be financially deterred from taking such action.

#### PROTECTION VIA CRIMINAL SANCTIONS AND LAW ENFORCEMENT AGENCIES

The general scheme contained in the Digital Agenda Act is covered in my earlier paper. Once again, the purpose of this paper is simply to carry the discussion a bit further.

The key issues raised in this area by the Internet and the digital agenda reforms are –

1. The adequacy of the laws to address the known and perceived threats to copyright owners;
2. The capacity, skill and resources of law enforcement agencies to effectively utilize the criminal laws to halt and deter infringing activity.
3. The likely impact of the new criminal sanctions.

#### *The adequacy of the laws*

This remains to be seen. The digital agenda reform amendments have only just come into effect. The House of Representatives Standing Committee on Legal and Constitutional Affairs Inquiry into Copyright Enforcement during its hearings in 1999 and from the many submissions it received elicited a fairly widespread consensus that the criminal sanctions provided by the Act as they presently exist (ie. without the proposed amendments contained in the digital agenda Bill) were of little use in assisting copyright owners safeguard their interests. High amongst the complaints were firstly that the onus of proof

---

<sup>16</sup> For a full discussion of the US cases and the criteria applied to establish jurisdiction over foreign defendants whose relevant activity occurred on the internet, see the paper by Gaye Middleton and Jocelyn About cited above in footnote 13. The authors point out that the manner in which the courts have applied the criteria to similar facts has been inconsistent leading to inconsistent decisions.

cast upon the prosecution in relation to subsistence and ownership of copyright was too onerous and too costly to discharge<sup>17</sup>, and secondly, that the law enforcement agencies lacked sufficient resources and expertise in this area.

Time will only tell whether the introduction of new digital agenda amendments to the Act, designed to prevent the infringement of copyright in the digital domain, will help deter copyright infringement on the internet, and whether law enforcement agencies will be quick to bring prosecutions if the new laws are broken. Music Industry Piracy Investigations (MIPI) had this to say in its submission to the House of Representatives Standing Committee concerning the Internet – “ The Internet by its very nature adds another dimension or jurisdiction to law enforcement. It is both a vehicle for traditional illicit behaviour and the breeding ground for a new class of criminal. These criminals will be fully-fledged ‘netizens’, limited by imagination who will spawn illicit enterprises hitherto unknown. This class of offender will be, for many reasons, better trained, better resourced and more imaginative than either his predecessors or law enforcement professionals.”

Further on, MIPI stated, “It is relatively easy to conceal one’s true identity and location on the Internet. Further there are few Internet specific offences or legislative facilitations that overcome the jurisdictional issues. At present, the only effective means of preventing infringements is obliging the ISP to remove an infringing site. It may be that, even in the future, the most effective means of dealing with Internet crime will be neutralization or disruption rather than use of traditional enforcement/prosecution methods. This area of enforcement merits urgent multi-disciplinary review and research.”

The centerpiece of the digital agenda amendments in the area of law enforcement and criminal sanctions is the new offences relating to interference with rights management information (RMI) and circumvention of effective technological protection measures. These new offences may prove to be a great benefit to those few copyright owners who have the resources and capacity to develop or pay for the development and installation of very sophisticated and expensive technological devices to safeguard their copyright and commercial interests. It will be of less or not use to copyright owners who lack such resources.

The requisite mental element required for the criminal offences is knowledge or recklessness.<sup>18</sup> Although copyright owners submitted to the Andrews Committee reviewing the Bill that constructive knowledge should suffice to establish liability, as is the case with civil remedies, the Committee took the view that it was appropriate that civil offences require a lesser degree of knowledge than criminal offences.

The same exception for “permitted purposes” as is allowed for the new civil remedies applies to the criminal sanctions.

---

<sup>17</sup> See for instance the submission of Music Industry Piracy Investigations.

An attack leveled at the proposed new laws is that they do not prohibit the use of circumvention devices that are intended to defeat or overcome the encryption or works or other technological safeguards utilized by copyright owners. The offences are directed at preventing commercial dealings in circumvention devices. People who actually use them for infringing copyright will not commit any offence. The critics therefore complain that such an omission undermines the copyright owner's legitimate right to decide whether to grant access to and use of copyright material.

In its submission to the Standing Committee inquiring into the enforcement of copyright, CAL (Copyright Agency Ltd) said due to this omission the digital agenda Bill may not be sufficient to ensure Australia's compliance with its international obligations, specifically under Article 11 of the World Intellectual Property Organisation (WIPO) Copyright Treaty which provides as follows:

*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."*

That submission was repeated to the Standing Committee during its review of the digital agenda Bill. In its Advisory Report published in November 1999 the Committee stated at paragraph 4.44 "The Committee supports the existence of a civil remedy for the use of a circumvention device for the purposes of infringing copyright." It also supported the inclusion of a civil remedy where a person uses a circumvention device in an attempt to infringe copyright.<sup>19</sup>

MIPI, in its submission to the Committee inquiring into copyright enforcement, pointed out that the most common forms of infringing material posted on the internet was the posting of sound recordings, music and lyrics. In relation to music and lyrics it said that the difficulty was exacerbated by the available means of detection which amounted to no more than manual surveillance conducted in real time. Effective and efficient identification was therefore impractical.

In relation to sound recordings, MIPI said that the most common form of infringement was committed by use of the 'MP3' format, the format used by Napster and Gnutella discussed earlier in this paper. MIPI said that using automated search technology, together with a global surveillance project, a substantial proportion of such activity could be identified. It estimated that at any given time in excess of 300,000 infringing MP3 files were being posted on the internet. Each contained sound recordings posted without the consent of the copyright owner. Given the nature of servers containing infringing files it said that it would

---

<sup>18</sup> Sections 132(5B) –(5E).

be possible for more than 3 million pirate sound recordings to be downloaded, world-wide, every 24 hours. It said that it appeared at that time that approximately 70,000 new infringing MP3 files were being posted on the internet by approximately 500 new infringers each month.

Neither the Copyright Act as it was before being amended or with the added digital agenda amendments is suited to dealing with this kind of phenomenon. Short of closing down the servers that facilitate such infringing activity, if they exist within the reach of the court's jurisdiction, what else can be done? Maybe the penalties that might attach to a caught "user" who is trading in such MP3 files has to be pegged at such a high level that knowledge alone of the possible penalty might act as an effective deterrent.

Chalfont Chambers

March 2001

---

<sup>19</sup> See Recommendation 14.