LexisNexis™ Butterworths

Volume 11 Number 4

Print Post Approved 24437100049

Internet Law Bulletin

Contents

Information contained in this newsletter is current as at July 2008

LexisNexis™ Butterworths

Global perspectives on peer-to-peer file sharing

Cheng Lim, Elizabeth Campetti and **John Eden**
MALLESONS STEPHEN JAQUES

The unauthorised sharing of copyright-protected works over peer-to-peer (P2P) networks is widely regarded by the music and movie industries (rights holders) as the single biggest threat to their respective business models. According to the International Federation of the Phonographic Industry (IFPI), at least 80 per cent of all internet traffic comprises the transfer of copyright works on P2P networks.[1]

In the face of this digital revolution, rights holders have explored a range of models — including both legislative and non-legislative initiatives — to persuade internet service providers (ISPs) to take steps to prevent P2P file sharing. These proposals range from the introduction of voluntary 'notice and disconnect' regimes to the imposition by ISPs of mandatory filtering.

This article explores several proposals that have been put forward by rights holders, each of which asks the key intermediary in the digital world — the ISP — to play a proactive role in the fight against piracy. We begin by providing an overview of the economics of P2P file sharing, noting the scale of the problem and disagreement over its financial implications for rights holders. We then consider each of the major regulatory proposals in turn.

Economics of P2P file sharing

As P2P networks have become ubiquitous, a great deal of controversy has erupted over whether file sharing has either hurt or helped the rights holders' traditional revenue streams. Some economic studies have concluded that file sharing reduces record sales. For instance, three papers published in the *Journal of Law and Economics* in April 2006 each found some kind of harm to rights holders from file sharing.[2] Other studies suggest that file sharing has had no negative impact on CD sales, including a widely cited paper in the *Journal of Political Economy* in February 2007, which analysed actual downloads on file sharing networks.[3]

Rights holders have consistently argued that P2P causes substantial economic harm. Consistent with this position, IFPI has referred to the growth of P2P as prompting a crisis in recorded music that it argues has wide implications for the whole digital marketplace and all those businesses to which music is an important ingredient.[4]

Regulatory proposals

'Notice and Disconnect'

Globally, rights holders and other stakeholders have explored a variety of different ways to regulate file sharing. One of the preferred solutions put forward by rights holders is a notice and disconnect scheme where, after a predetermined number of warnings, the subscriber account of an alleged file sharer is disconnected by their ISP.[5] This type of proposal has also been referred to as a three strikes regime,[6] because the proposals include a graduated system of written warnings followed by a suspension notice and, on the third occurrence of suspected infringement, disconnection.

While the fine details of these schemes differ, they all share similar elements, including that a user can be disconnected without the intervention of a court or a legal finding that the user has actually infringed copyright. The rights holders favour such schemes because they say that the evidence shows that a single warning is adequate to cause users to cease engaging in P2P file sharing.[7] ISPs consider that this mechanism requires them to, in effect, perform a judicial role in assessing infringement of third-party rights, and to enforce them on behalf of rights owners.

Australia is one of the countries in which rights holders have been vocal in their lobbying for the adoption of a 'notice and disconnect' system. The

proposal is that a warning email would be sent for the first infringement, followed by a limited suspension from the service for a second infringement, and termination for a third infringement. However, the proposal does not address a number of practical issues. For example, it provides no details about how ISP customers engaging in P2P would be identified, contains an underlying presumption of guilt, and does not answer the question of what would happen to those whose accounts have been terminated. Would, for example, ISPs be required to create a blacklist of offenders, or could terminated users simply resubscribe to another ISP's services?

A similar scheme has been proposed in the UK. While not adopting a position on the 'three strikes' proposal, the UK government has recently published a strategic paper threatening to introduce legislation to address the issue of P2P file sharing if a voluntary solution is not reached by April 2009.[8]

The 'three strikes' model has been most influential in France, where, in November 2007, President Nicholas Sarkozy announced that ISPs and stakeholders had signed a memorandum of understanding (MOU) relating to a notice and disconnect scheme.[9] The French version of the scheme bears some significant differences to those proposed in the UK and Australia. Most importantly, according to the MOU, the regime will be administered by an independent government body under the supervision of a judge. This body will send warnings to file-sharers and act as an appeal tribunal.

In Japan, it appears that steps have also been taken to implement a form of notice and disconnect. It has been reported that the four largest Japanese internet providers have entered into an agreement that requires ISPs to disconnect internet access for users of Winny, a P2P technology that is often used to distribute pirated films, music and software.[10] Under this approach, copyright holders give an ISP a list of IP addresses of alleged infringers using Winny. After a warning, flagrant violators are be subject to disconnection by their ISPs.[11]

But not all government responses to notice and disconnect have been positive. In Sweden, the *Renfors Report*, released in September 2007, proposed a change in the law to oblige ISPs to block the subscriptions of users who repeatedly engage in copyright infringement on a large scale. However, in March 2008, the Swedish Minister of Justice, Beatrice Ask, and Minster of Culture, Lena Adelsohn Liljeroth, announced that the government had rejected the report's recommendations.[12] This was due to widespread criticism of the disconnection proposal and the serious repercussions of such a scheme in a society where access to the internet is considered an imperative welfare issue.

Further, the European Parliament has also passed a resolution expressly rejecting the adoption of 'three strikes' style regimes.[13] This resolution of 10 April 2008 called on the Commission and member states to:

> recognise that the internet is a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society [and] to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access.[14]

As we have seen, notice and disconnect schemes are not all cut from the same cloth. Some proposals give rights holders the ability to disconnect file-sharers irrespective of the scale of the alleged infringement. Other schemes — like Japan's — only require the disconnection of large-scale infringers. However, in each case the sanctions countenanced under notice and disconnect or 'three strikes' schemes are serious.

Many ISPs have been reluctant to adopt any form of notice and disconnect. In particular, ISPs in some countries are wary of relying on allegations of infringement given to them by rights holders. Such allegations have had neither the benefit of public examination nor been tested in court. Furthermore, they typically rely on IP address data to link infringements with individual subscribers, which can pose difficult issues of proof and technical reliability.[15] There are also temporal issues arising out of the linking of IP address data to end users, particularly where ISPs use dynamic IP address allocation techniques to maximise their efficient use of IP addresses.

... allegations [of infringement] have had neither the benefit of public examinations nor been tested in court.

Some ISPs regard notice and disconnect as requiring providers of commercial services (internet connectivity) to make what are essentially judicial determinations such as:

- is the file subject to copyright?
- has there been an infringement? and
- is there a fair dealing or fair use defence?

There is also concern among ISPs that disconnection could penalise the wrong person where an internet connection is shared among multiple users. Acting on unproven allegations to disconnect customers' internet access could give rise to liability on the part of ISPs to their customers or, equally importantly, could damage their brands. These concerns, together with those set out here about practical implementation of the proposed notice and disconnect schemes, reinforce ISPs' reluctance to adopt them.

Content filtering

Notice and disconnect schemes are designed to discourage file sharing through the threat of termination. According to rights holders, most internet users would cease sharing files on receiving their first warning, and only persistent infringers would risk having their accounts terminated.[16] However, there are a number of alternatives to making threats against file-sharers. For example, infringements could be reduced by making infringing content *less*

available. Rights holders have explored this avenue in at least two jurisdictions, suing ISPs to obtain court orders that should, in theory, reduce the availability of copyright materials online.

In Belgium, the Society of Authors, Composers and Publishers (SABAM) recently sued Scarlet (formerly Tiscali), an ISP, for secondary copyright infringement. SABAM successfully argued that Scarlet, as a provider of internet services, was responsible for enabling the file sharing activities of its customers. The remedy awarded by the court was unprecedented: Scarlet was required to implement filtering technologies within six months to stop illegal file sharing from occurring on its network. If Scarlet does not comply with the court's order, it will have to pay 2500 Euros per day in damages. The case is currently being appealed.[17]

A number of large content owners have also issued proceedings in Ireland against Eircom, Ireland's largest ISP. The Irish divisions of EMI, Sony BMG, Universal and Warner Music have joined forces in arguing that Eircom is violating the *Copyright and Related Rights Act 2000* (IE) by making copyright works available without authorisation at the direction of internet users.[18] Interestingly, the plaintiffs appear not to have alleged any actual infringements of copyright in the pleadings, but have taken the action based on a presumption that Eircom is infringing copyright works owned by the plaintiffs. The remedy sought is a wide-ranging injunction that would restrain Eircom from infringing copyright in sound recordings owned or licensed to the plaintiffs by making copies of those sound recordings available to the public through its internet service. The injunction does not specifically seek installation of filtering technologies, but the installation of Audible Magic fingerprinting software or a commercially available equivalent was put forward by the plaintiffs as one method of removing infringing content from Eircom's network.[19]

Co-operation between ISPs and rights holders is not as rare as the *Scarlet* and *Eircom* cases might suggest. For example, in the US, rights holders have opted to co-operate with ISPs to develop anti-piracy technologies. Cary Sharman, head of the Recording Industry Association of America (RIAA), has said that the RIAA does not endorse mandatory filtering by ISPs but instead prefers a 'marketplace solution' to address illegal file sharing.[20]

In the UK, the British Phonographic Industry (BPI) and Virgin Media recently announced a two-month trial of such a marketplace solution. The scheme, which has been branded as an educational campaign, is centred on the provision to Virgin by the BPI of the IP addresses of customers identified as sharing copyright material. Identified customers will be sent two letters, one from Virgin and one from the BPI. However, no personal information is intended to be disclosed to the BPI, and the scheme makes no mention of disconnection of customers who continue to share files.[21]

AT&T is also working with the RIAA and the Motion Picture Association of America (MPAA) on new filtering technology that may reduce unauthorised copying of movies and music.[22] The specific technology that AT&T plans to use has not been made public. Since P2P traffic is notoriously difficult to detect and control, and P2P traffic is increasingly encrypted to prevent determination of the nature of the content being distributed, only time will tell if AT&T's filtering technology will be effective to deter illegal file sharing over P2P networks. What is clear, however, is that filtering technology is sometimes adopted as a result of voluntary arrangements, not by way of a court order.

Disclosure of alleged file-sharers' identities

While filtering technologies attempt to reduce the availability of copyright materials, disclosure seeks to discourage access to those materials by disclosing file-sharers' identities to rights holders, typically through legislative initiatives and lawsuits. For example, the Swedish government is considering legislation giving courts the authority to compel ISPs to hand over the personal details of suspected file-sharers.[23] This could be beneficial to some Swedish ISPs that do not want to take action against customers unless the law requires it. As a spokesman for Swedish ISP Com Hem

put it, regulation of copyright infringement should be treated as a judicial matter so that ISPs do not have to 'act as police'.[24]

This approach is also favoured in countries such as Australia, where the Federal Court Rules already provide that an order for preliminary discovery can be made to identify the respondent in proceedings.[25] The advantage of this approach is that any action taken by an ISP is on the basis of an order made by a court, so the ISP is not exercising a quasi-judicial function in its own right.

In the litigation context, rights holders in Europe have not had an easy time obtaining information about alleged file-sharers. One example of these difficulties is provided by the *Telefónica* decision,[26] where the ECJ held that European Union law does not require ISPs to disclose the names of those sharing files across their networks in a civil lawsuit. The plaintiff in the case, Promusicae, filed a civil petition in a Spanish court to compel Telefónica, a Spanish ISP, to reveal the identities and physical addresses of users whom Promusicae believed were using P2P networks to infringe copyright works. Telefónica argued that Spanish law only required disclosure of such information in a criminal case, so that it could avoid disclosure for purposes of civil copyright infringement proceedings. The ECJ agreed to hear a reference from the Spanish court, and decided that the Spanish legislation was valid and consistent with the various European directives on the issue.

The *Telefónica* decision, along with the Swedish government's proposed legislation, highlights the tension between protecting the legitimate interests of copyright owners and protecting the personal information of end users. Indeed, some see the *Telefónica* decision as a missed opportunity to articulate proper guidance to member state legislatures in dealing with the competing interests of rights holders, privacy advocates and end users.[27] Whatever one's position on how to balance these two competing values, it seems likely that rights holders will continue to lobby for legislation enabling more streamlined access to the identities of alleged file-sharers.

Denying access to file-sharing websites

Courts in Denmark have on at least two occasions ordered ISPs to block access to file-sharing websites. First, in February 2008, the IFPI secured a judgment requiring Denmark-based ISP Tele2 to shut down access to the popular file sharing site The Pirate Bay. The court found that Tele2 infringed the plaintiff's copyrights by giving its customers access to its website.[28] The second blocking order, also made against Tele2, required it to block access to AllofMP3.com[29], a popular Russian music download website.

While the rights owners see denying access to specific sites as one way of addressing the issue of copyright infringement without suing individual file-sharers or asking ISPs to implement new filtering technologies, some internet activists argue that file sharing sites should not be shut down, even if they are used for piracy, on the basis that file sharing sites also help people share legal content.

Conclusion

The IFPI stated in its 2008 *Digital Music Report* that:

> 2007 was the year ISP responsibility started to become an accepted principle. 2008 must be the year it becomes reality.[30]

While the IFPI, other industry bodies and rights holders are adamant that ISPs have a role to play in reducing global file sharing, the IFPI principle of ISP responsibility appears to be far from accepted by ISPs (who regard themselves as mere conduits) and other stakeholders. This discussion illustrates that governments and public bodies have started to recognise that rights holders' proposals raise several practical and legal issues, including concerns over privacy, liability and consumer interests.

The debate between rights holders, ISPs and consumer groups over how best to address illegal file sharing via P2P networks will in all likelihood continue for some time. The question for the stakeholders appears to be whether there are alternatives to the types of strategies discussed in this article to curb unauthorised file sharing, such as the development of compelling alternative business models for the legal distribution of content. ●

Cheng Lim, Elizabeth Campetti and John Eden,
Intellectual Property and Technology Group, Mallesons Stephen Jaques.

Endnotes

1. IFPI, *IFPI Digital Music Report 2008* (2008) 3.

2. See Liebowitz S 'File Sharing: Creative Destruction or Just Plain Destruction' (2006) 49 *Journal of Law and Economics,* 1; Rob R and Waldfogel J 'Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students' (2006) 49 *Journal of Law and Economics, 29*; Zentner A 'Measuring the Effect of File Sharing on Music Purchases' (2006) 49 *Journal of Law and Economics,* 63. All three papers are available at <http://econpapers.repec.org/article/ucpjlawec/>.

3. Oberholzer-Gee F and Strumpf K *The Effect of File Sharing on Record Sales: An Empirical Analysis* (2006) <www.utdallas.edu/~liebowit/intprop/OS%202006-12-12.pdf>.

4. IFPI, above n 1.

5. See Eliott F 'Internet Users Could Be Banned over Illegal Downloads' The *Times* 12 February 2008 <http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article3353387.ece>; Gilmore H and Armstrong K 'War on Music Piracy' *Sydney Morning Herald* 17 February 2008 <www.smh.com.au/articles/2008/02/16/1202760662778.html>.

6. See, for example, Ozimek J 'France Gets Closer to "Three Strikes" Downloader Web Ban' *The Register* 12 June 2008 < www.theregister.co.uk/2008/06/12/france_music_law/>.

7. Stephen Peach, CEO of Aria, in the television programme MiTunes, SBS 3 June 2008 as part of the Insight series.

8. Department for Culture, Media and Sport, *Creative Britain, New Talents for the New Economy* February 2008 <www.innovateuk.org/_assets/pdf/other-publications/creative%20britain%20-%20new%20talents%20for%20the%20economy_feb2008.pdf>.

9. See Fenton B 'French Plan E-mail Warnings for Illegal Downloads' *Financial Times* 28 January 2000

<www.ft.com/cms/s/0/d5fe255a-cd41-11dc-9b2b-000077b07658.html>.

10. See Williams C 'Japanese ISPs Agree Three Strikes-style Anti-piracy Regime' *The Register* 16 March 2008 <www.theregister.co.uk/2008/03/17/japan_three_strikes/>.

11. See Ou G 'Japan's ISPs Agree to Ban P2P Pirates' *ZDNet* 16 March 2008 <http://blogs.zdnet.com/Ou/?p=1063>.

12. Ask B and Adelsohn Liljeroth L 'Kulturarbetare får stöd av domstol' *Svenska Dagbladet* 14 March 2008 <www.svd.se/opinion/brannpunkt/artikel_972903.svd>.

13. European Parliament Resolution of 10 April 2008 on Cultural Industries in Europe 2007/2153(INI) (2008) PE 405.408.

14. Ibid [23].

15. See, for example, Piatek M, Kohno T and Krishnamurthy A 'Challenges and Directions for Monitoring P2P File Sharing Networks: or Why My Printer Received a DMCA Takedown Notice' (2008) University of Washington Technical Report UW-CSE-08-06-01 <http://dmca.cs.washington.edu/>.

16. IFPI, above n 1, 19.

17. The Scarlet case did not consider Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive), which provides immunity to ISPs for activities they undertake as providers of internet services. At issue in the appeal will be whether the E-commerce Directive provides wide immunity for ISPs that have no direct involvement in the infringing activities of their customers. In addition, the appeal will also likely consider whether the E-commerce Directive prevents a judge from granting injunctive relief at a rights holder's request.

18. Whelan J and Cullen C 'Ireland: Irish ISP Sued by Music Industry' *Managing Intellectual Property* June 2008 <www.managingip.com/Article/1940955/Irish-ISP-sued-by-music-industry.html>.

19. Audible Magic is the leading provider of content filtering software. Its customers include Microsoft, Grouper, YouTube, Nokia, videoegg, Dailymotion and a number of other well-known internet companies. See Audible Magic, *Content Identification Services Customers* (2008) <http://www.audiblemagic.com/clients-partners/contentsvcs.asp>.

20. Anderson N 'RIAA Chief: We Don't See a Need for Mandatory ISP Filtering' *Ars Technica* 30 January 2008 <http://arstechnica.com/news.ars/post/20080130-riaa-chief-we-dont-see-a-need-for-mandatory-isp-filtering.html>.

21. See Williams C 'Virgin Media and BPI Join Forces to Attack Illegal File-sharing' *The Register* 6 June 2008 <www.theregister.co.uk/2008/06/06/virgin_media_bpi_deal/>.

22. Stone B 'AT&T and Other ISPs May Be Getting Ready to Filter' *New York Times Weblog: Bits* 8 January 2008 <http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/>.

23. See Associated Press, 'Sweden Pursues Illegal File Sharers' (14 March 2008) <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20080314/Sweden_files_080314>.

24. Above.

25. See *Federal Court Rules 1979* (Cth) O 15A.

26. *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] EUECJ C-275/06 <www.bailii.org/eu/cases/EUECJ/2008/C27506.html> ('*Telefónica*'). See also European Digital Rights, 'ECJ Decision on Handling Traffic Information in Civil Cases' 30 January 2008 <http://www.edri.org/edrigram/number6.2/ecj-traffic-copyright>.

27. Tielemans H and Van Quathem K 'Privacy Rules do not Trump IP Protection' (May 2008) 180 *Copyright World* 12, 12–13.

28. Cheng J 'Pirate Bay to IFPI: Danish Ban Has Led to Even More Traffic' *Ars Technica* 12 February 2008 <http://arstechnica.com/news.ars/post/20080212-pirate-bay-to-ifpi-danish-ban-has-led-to-even-more-traffic.html>.

29. Smaran-Torrentfreak and Gjerding S 'Danish ISP Forced to Block Allofmp3.com' *European Digital Rights* 8 November 2006 <www.edri.org/edrigram/number4.21/allmp3_denmark>.

30. Above.

Business as usual: a review of the report *Copyright Exceptions for Private Copying of Photographs and Films*

Peter Knight and **Rebecca Wakeling** CLAYTON UTZ

It will come as a great shock to the Attorney-General's Department to learn that ordinary people all over Australia are copying films and other copyright material — not just songs — legitimately obtained by them, onto their iPods and other MP3 and MP4 players. And nothing is going to make this stop.

With its report *Copyright Exceptions for Private Copying of Photographs and Films: Review of sections 47J and 110AA Copyright Act 1968*,[1] the Attorney-General's Department (the Department), responding to pressure from copyright owners who argued that the fabric of copyright — and their economic interests — would be harmed by a change to the law that simply recognised the facts of consumer behaviour, decided to do nothing. We must remember that this response relates only to non-pirated film and other copyright material which has been properly purchased (not rented or downloaded) by consumers.

In its report, the Department made the following recommendations.

Recommendation 1

> The Department recommends a re-examination of public awareness material and consumer information on the meaning of the format-shifting exceptions to assist people to understand their rights and obligations under the *Copyright Act 1968*.[2]

This recommendation arose from submissions that supported widening ss 47J and 110AA in order to bring those sections into line with s 109A.[3]

S 109A (the 'iPod exception') was introduced into the Act by the *Copyright Amendment Act 2006* and recognised as a reasonable use of a sound recording that it may be copied by its owner for his or her private and domestic use only — and hence this would no longer be an infringement of the copyright in the sound recording or the underlying literary and/or musical works. In the same amending legislation, however, s 110AA was introduced, which arbitrarily limited such a 'format-shifting' defence to copying 'videotapes ... in analog form'. Why so narrow?

It was argued by the copyright owners that the situation with video files is entirely different from that of sound recordings. It was argued that there are proposed new formats for video files, including special formats which permit limited copying. Notwithstanding that exactly the same issues with respect to new forms of distribution of copyright material were advanced by copyright owners in respect of sound recordings prior to the introduction of s 109A, the Department agreed that these future possibilities were such as to make all too difficult an amendment to s 110AA so that it would work the same way in respect of films as s 109A works in respect of sound recordings. The Department was persuaded that the market for films and photographs is so different from the market for digital music that a re-examination of public awareness and consumer information was the appropriate response.[4]

What is happening in the real world makes this an almost incomprehensible conclusion. Furthermore, it is difficult to educate the public about the value of a copyright law that makes unlawful what they do every day and regard as a normal and reasonable exploitation of what they buy, or of the value of an exception to infringement based on technology so outdated (that is, videotapes) as to be regarded by consumers as irrelevant. This makes it even more likely that consumers will regard all of copyright law as ridiculous, including the prohibition of unauthorised downloads. Amendments that make copyright law relevant to today's technology, and a public awareness campaign to encourage consumers to acquire content legitimately — including by the possible new formats hinted at by the copyright owners — would be of greater use.

Recommendation 2

> The Department recommends that no change be made to section 47J at this time. However it would be beneficial to provide further public information in relation to copyright in photographs taken professionally for a family or private occasion.[5]

The Department was critical both of views supporting reasonable consumer expectations and views supporting creator's rights. It stated that neither side provided information concerning the likely market effect of change. Consequently, neither side met the onus for establishing the justification for, and consequences of, legislative change.[6]

The Department failed to address why the exception was limited to photographs, and did not offer any form of support or policy justification for why photographs received different treatment from artistic works generally.

Recommendation 3

> The Department recommends that no change be made to section 110AA at this time. However, the Department will continue to monitor the evolution of relevant markets to determine if new products are introduced as anticipated by the film industry.[7]

Despite acknowledging that increasing numbers of consumers are likely to value the ability to format-shift film material to different playing devices, and that film content-owners want to adapt their business models to meet market demand and changing consumer wishes, the Department was of the view that a change to s 110AA was not necessary to assist markets to adapt.[8]

The Department thought the importance of the home entertainment market for film-rights holders made it imprudent to embark on legislative change affecting the home entertainment market without clear indications that intervention is appropriate and likely to be effective.[9]

Similarly, the Department concluded that it would be premature to extend s 110AA to allow permanent copies of film material recorded from television broadcasts to be made without reliable information as to the likely market impact. It took the view that any link between ss 110AA and 111 would allow consumers to make permanent 'library' copies of feature films and television programs, potentially causing financial harm to copyright owners.[10]

It is difficult to see how facilitating greater flexibility in legitimate copying of films will adversely affect the market. The Department's conclusion is indicative of a reluctance to acknowledge the reality of consumer behaviour and ignores the advent of personal MP4 players and wireless home networks and the consequent consumer expectation that they should be able to view video material on a number of devices.

Where to from here?

The Department's recommendations effectively enshrine a 'business as usual' approach, which is likely to lessen the credibility of copyright law in the eyes of reasonable consumers. The present-day situation is reminiscent of that so aptly described by Lord Templeman in the late 1980s, in the case of *CBS Songs Limited v Amstrad Consumer Electronics plc*,[11] where his Lordship commented as follows:

> From the point of view of society the present position [domestic copying of audio tapes] is lamentable. Millions of breaches of the law must be committed by home copiers every year. ...
>
> Whatever the reason for home copying, the beat of Sergeant Pepper and the soaring sounds of the Miserere from unlawful copies are more powerful than law-abiding instincts or twinges of conscience. A law which is treated with such contempt should be amended or repealed.

Though directed to UK consumers in the context of UK copyright law, Lord Templeman's comments remain equally applicable in the context of newer technologies today.

Regrettably, the reality of modern technology and day-to-day consumer behaviour does not appear to have been given any weight by the Department against a range of possibilities and hypotheses presented by copyright owners. This is surprising, given the comment made by the then Attorney-General, Philip Ruddock, when the format-shifting exceptions were introduced in 2006: 'Copyright is important and should be respected… That is why the government is updating our laws to keep pace with technology'.[12] ●

Peter Knight,
Partner, and
Rebecca Wakeling,
Lawyer,
Clayton Utz, Sydney.

Endnotes

1. Attorney-General's Department *Copyright Exceptions for Private Copying of Photographs and Films: Review of sections 47J and 110AA Copyright Act 1968* (Report), tabled in Parliament 18 June 2008. Available at <www.ag.gov.au>.
2. Above, n 1, p 3.
3. Above, n 1, para 3.16, p 10.
4. Above, n 1, para 3.19, p 11.
5. Above, n 1, p 3.
6. Above, n 1, para 4.6, p 12.
7. Above, n 1, p 3.
8. Above, n 1, para 5.12, p 17.
9. Above, n 1, para 5.13, p 17.
10. Above, n 1 para 5.17, p 18.
11. [1988] AC 1013.
12. 'Copyright changes set to make downloads legal', *Sydney Morning Herald*, 15 May 2006. Available at <www.smh.com.au>.

Business-to-consumer e-commerce: the EU and Australia compared

Dr Dan Jerker B Svantesson FACULTY OF LAW, BOND UNIVERSITY

Consumer transactions account for a large part of e-commerce worldwide, and one of the most important e-commerce markets in the world is the European Union (EU). Focusing on e-commerce, this article analyses the EU's regulation of consumer transactions, and compares it to the regulatory approach taken in Australia.

The article starts by highlighting the significant difference between how Australia and the EU define 'consumers'. It then examines the most relevant EU instruments and points to similarities and differences with Australian law.

Definition of 'consumers'

Similar to several international instruments, and contrary to the Australian approach, the EU instruments give rather brief definitions of the term 'consumer'. While the exact wording varies somewhat amongst the EU instruments, typically a consumer is defined to include any natural person who is acting for purposes which are outside his or her trade, business or profession.[1] Leaving aside the fact that Australia uses a very lengthy and complex definition of who is a 'consumer'[2], the most significant difference is that the EU's definition excludes what can be termed 'business consumers': businesses acting as consumers in purchasing goods or services.

Under the *Trade Practices Act 1974* (Cth), businesses are classed as consumers, and provided the same protection as other consumers, where they contract for goods or services, and:

(1) the purchase is not for re-supply or otherwise for being used up or transformed in trade or commerce, and
(2) the purchase is either
  (a) for goods/services of a kind ordinarily acquired for personal, domestic or household use, or
  (b) for an amount lower than the prescribed amount (currently AUD 40,000).

Unfortunately, no similar arrangement is made under the EU approach. While rare,[3] the wide definition of 'consumers' used in Australia is superior to that used in EU instruments. After all, a corporation acting outside its main field of business may be in as weak a bargaining position as a consumer typically is. Imagine, for example, a one-man bakery contracting with a major electronics company for a computer. The baker may have as little knowledge of computers as an average consumer, and is certainly the weaker party in the transaction. It seems odd that the baker would be classed as a consumer if purchasing the computer for personal use, but not classed as a consumer if buying the computer to keep track of production in the bakery.

Unfair terms

While not specifically targeted at e-commerce, the EU's Unfair Terms Directive[4] is highly relevant. It came into force in 1993, and it regulates unfair contractual terms in business-to-consumer (B2C) contracts.

The types of contractual terms that fall within the scope of the directive are defined in two different ways. First, general provisions are laid down, and second, specific examples of unfair terms are described in the annex to the Directive.

As far as e-commerce is concerned, it is particularly interesting to note that Art 3(1) of the directive regards contractual terms which have not been individually negotiated, such as most click-wrap agreements and disclaimers, as unfair provided that they:

(1) cause a significant imbalance in the parties' rights and obligations arising under the contract;
(2) are to the detriment of the consumer; and
(3) are contrary to the requirement of good faith.

Interestingly, drawing on the *Unfair Terms in Consumer Contracts Regulations 1999* (UK), which represents the UK's implementation of the Unfair Terms Directive, the *Fair Trading Act 1999* (Vic) was amended in 2003 to include a part (Pt 2B) regulating unfair terms in consumer contracts in much the same manner as promoted in the Unfair Terms Directive. By taking this step, Victoria is leading the way in Australia, and there are strong reasons to believe (and hope!) that similar amendments will be made in other Australian states' Fair Trading Acts, or alternatively at federal level.

Misleading conduct

If a legal rule's success is measured by reference to how often it is relied on in litigation, one of the most successful rules in Australian law is found in s 52 of the *Trade Practices Act 1974* (Cth). In essence, this unusually short section makes clear that, 'A corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive'.

This provision has been relied on in several e-commerce cases. For example, it has been used to take action against a US-based person operating a website selling invalid and over-priced tickets to the Sydney Opera House.[5] It has been used in an attempt to prevent one TV network from displaying a picture of the Olympic torch on its website, as another TV network had the broadcasting rights to the Olympics in Australia.[6] And, it has been relied on in an action relating to the similarity of the domain names used by two businesses in related industries.[7]

A similar approach has been taken by the EU. The relatively recent Directive on Unfair Business-to-Consumer Commercial Practices[8] regulates business practices that are misleading, aggressive and/or coercive. The structure of this directive is rather similar to the structure of the Council Directive on Unfair Terms in that both directives contain broad rules complemented by an annexed list of practices/terms that always are contrary to the directive in question.

The most central provision of the Directive on Unfair Business-to-Consumer Commercial Practices is Art 5. It states that a commercial practice is unfair and therefore prohibited if it:

(a) 'is contrary to the requirements of professional diligence',[9] and
(b) materially distorts or is likely to materially distort the economic behaviour of an average consumer whom it reaches or is addressed to.[10]

As far as misleading commercial practices are concerned, the directive draws a distinction between misleading actions and misleading omissions. In assessing whether a business has made a misleading omission, regard is had to all the features and circumstances of the practice and to the limitations of the communication medium.[11] This may have huge implications in relation to e-commerce where, depending on the circumstances, it may be argued that the method of communication in question did not allow for the communication of particularly detailed information. However, in most forms of e-commerce, businesses can be expected to provide sufficiently detailed information.

Several types of unfair, and thereby prohibited, commercial practices outlined in the annex are of particular relevance in the context of e-commerce. For example, the annex declares as unfair practices such as pyramid schemes,[12] 'claiming in a commercial practice to offer a competition or prize promotion without awarding the prizes described or a reasonable equivalent'[13] and:

> creating the false impression that the consumer has already won, will win, or will on doing a particular act win, a prize or other equivalent benefit, when in fact either: there is no prize or other equivalent benefit, or taking any action in relation to claiming the prize or other equivalent benefit is subject to the consumer paying money or incurring a cost.'[14]

Information requirements

Both the E-commerce Directive[15] and the Distance-selling Directive[16] contain provisions regulating the type of information that e-commerce providers must supply. Under the E-commerce Directive, any natural or legal person providing an information society service (such as a person operating a website) must provide information, such as its name, e-mail address and geographical address.[17] Further, where the information society service is commercial in its nature:

(a) the commercial communication shall be clearly identifiable as such;
(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously; and
(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.[18]

While the above is applicable to both B2B and B2C transactions, Art 10 is specifically aimed at consumer protection. It requires that, unless the contract is concluded via e-mail or a similar form of individual communication, consumers must have access to the following information prior to placing an order: 'the different technical steps to follow to conclude the contract';[19] 'whether or not the concluded contract will be filed by the service provider and whether it will be accessible';[20] 'the technical means for identifying and correcting input errors prior to the placing of the order';[21] and 'the languages offered for the conclusion of the contract'.[22] This information must be provided comprehensibly and unambiguously. Further, Art 10(3) states that '[c]ontract terms and general conditions provided to the recipient must be made available in a way that allows him [or her] to store and reproduce them'. This is important as in many cases, pop-up boxes with terms and conditions lack easy printing options.

The ambition, structure and content of Art 11 changed considerably throughout the drafting of the directive. In its final form, it reads as follows:

(1) Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:
   — the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,
   — the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.
(2) Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.
(3) Paragraph 1, first indent, and paragraph 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

The Distance-selling Directive

contains somewhat overlapping provisions. They will not be discussed here.

Leaving aside the particular rules aimed at regulating spam,[23] Australian law does not contain any similar provisions. This is problematic and ought to be addressed.

Jurisdictional issues

One of the main advantages e-commerce has over traditional commerce is its ability to facilitate contracts over distances. As a result, it is frequently the case that the parties to an e-commerce contract are located in different countries. Where a dispute arises in such a situation, it is necessary to consider the following questions:

- in which country can litigation be carried out (jurisdiction)?
- which country's law should govern the dispute? and
- where can a judgment rendered in the dispute be recognised and enforced?

Taken together, these questions form an area of law referred to as conflict of laws, or private international law. The EU's approach to conflict of laws is currently undergoing some changes. Consequently, it is necessary to highlight no less than four different instruments. However, only two of them need to be discussed in detail.

As far as jurisdiction (and recognition and enforcement) is concerned, the key instrument is the Brussels I Regulation.[24] It is a closed double convention, meaning that the regulation deals with jurisdiction as well as recognition and enforcement, and that only the jurisdictional grounds provided in the regulation are viewed as valid. It is only intended to regulate the jurisdictional question among member states of the EU. However, as some states have extended the rules of the Brussels I Regulation into their domestic private international law rules,[25] the rules of the regulation will also affect claims against persons not domiciled in an EU member state in some cases.

When combined, Arts 15, 16 and 17 have the effect of ensuring that an e-commerce consumer typically can chose whether to take action against a business at the consumer's place of domicile or at the business's location, and the business is prevented from taking action against the consumer at any place other than the consumer's place of domicile. Further, the consumer cannot contract out of these privileges, at least not prior to the dispute arises.

Turning to the issue of choice of law, a distinction must be drawn between contractual and non-contractual situations. The choice of law question in non-contractual situations is dealt with in the Rome II Regulation.[26] As we focus here on e-commerce, it is however contractual choice of law issues that interest us. Such issues are currently regulated through the Rome Convention.[27] While it is likely that the Rome Convention will be replaced by the proposed Rome I Regulation,[28] it is uncertain when that change will take place. Consequently, the discussion below is focused on the Rome Convention.

One important aspect of the Rome Convention is that it is applicable regardless of the origins of the contractual parties. That means that, provided that the court in question has jurisdiction, it must apply the rules of the Rome Convention in determining the applicable law (provided that the contract falls within the scope of the Convention). Further, the law specified by the rules of the Rome Convention is to be applied whether or not it is the law of a member state.[29]

The starting point of the Rome Convention (Rome I Convention) is that the parties' choice of law should be respected and upheld.[30] Where no choice is made, attention is placed on connecting factors, such as the habitual residence of one or the other of the parties. Interestingly, like the Brussels I Regulation discussed above, the Rome Convention contains rules aimed specifically at protecting consumers. In effect, it invalidates choices of law that would deprive consumers of protection afforded to them through mandatory rules of the state in which they have their habitual residence.[31] Where no choice has been made, the contract is to 'be governed by the law of the country in which the consumer has his habitual residence'.[32]

While this may seem like a rather generous approach, a consumer will only enjoy this protection in limited circumstances. For the purpose of e-commerce, it is particularly interesting to note that one situation where the consumer would enjoy the mentioned protection is where:

> …the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract'.[33]

This provision is associated with at least two problems in the e-commerce setting. First, when is a web advertisement to be viewed as meeting the requirement of being a specific invitation or advertising of the kind mentioned? Second, the requirement that the consumer has taken the steps necessary for the conclusion of the contract in her or his home country, is unreasonable in relation to e-commerce. As noted by a learned author:

> …it should make no difference whether a consumer living in Brno [Czech Republic] has placed his order from home or from an Internet café while on a half-day shopping visit in Bratislava [Slovak Republic]'.[34]

While the *Trade Practices Act 1974* (Cth) contains some consumer protection provisions that a consumer cannot contract out of,[35] Australian law does not otherwise have any provisions similar to this.

Concluding remarks

This article has highlighted that the EU's approach to consumer protection in e-commerce bears great similarities to that taken in Australia. It should also have been made clear that the EU's e-commerce regulation consists of a number of partly overlapping instruments, creating a patchwork approach that is inaccessible to the uninitiated.

In comparing Australia's approach to that taken by the EU, three major differences have been identified. First, Australia has given a much wider definition to the term 'consumer' than has the EU. Indeed, Australia's wide definition is at odds with the definition of 'consumers' in most, if not all

international instruments. Typically, when one jurisdiction has taken a significantly different approach to the rest of the international community, that state has opted for an inappropriate approach. However, for the reason expressed above, it is nevertheless submitted that in this particular case, the Australian approach is superior to that taken elsewhere.

The second major difference between Australia's and the EU's approach to consumer protection in e-commerce is the information requirements that exist in EU law, but not under Australian law. Where such information is provided, consumers are empowered as they are put in a better position to make informed decisions. Therefore requiring that such information is made available to the consumer is an important step in ensuring effective consumer protection. It is consequently submitted that Australian law would benefit from adopting the same approach as the EU.

Finally, Australia's conflict of law rules ought to be amended so as to provide extra protection for consumers, as the EU's conflict of law rules do. It is acknowledged that most consumer disputes involve low values and will not be settled through cross-border litigation. However, it is nevertheless of crucial importance that such litigation is available as a means for consumers to exercise their rights. ●

Dr Dan Jerker B Svantesson,
Associate Professor,
Faculty of Law,
Bond University.

Endnotes

1. See, for example, Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Art 2(e).

2. *Trade Practices Act 1974* (Cth) s 4B.

3. The only similar approach I have come across is found in Art 1(4) *lit*(a) of the Greek Consumer Protection Act (Law No. 2251/1994), which defines a consumer as 'any natural or legal person, for whom products or services offered in the marketplace, are destined, or who makes use of such products or services, provided that he/she is the final recipient of them'. See further: Iglezakis I *e-Commerce directive — The Greek response* CLSR (2005) 21, 38–45, at 40.

4. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

5. *Australian Competition and Consumer Commission v Chen* [2003] FCA 897; BC200304783.

6. *Seven Network Ltd v News Interactive Pty Ltd* [2004] FCA 1047; BC200405090.

7. *Sydney Markets Ltd v Sydney Flower Market Pty Ltd* [2002] FCA 124; BC200200932.

8. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'). Hereinafter referred to as 'Council Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market' in footnotes.

9. Council Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, Art 5(2)(a).

10. Above, n 7, Art 5(2)(b).

11. Above, n 7, Arts 7(1).

12. Above, n 7, Annex I point 14. Compare to ss 65AAA-65AAE of the *Trade Practices Act 1974* (Cth).

13. Council Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, Annex I point 19.

14. Above, n 13, Annex I point 31.

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

16. Council Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts aims at providing consumers purchasing goods or services via distance communication.

17. Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Art 5.

18. Above, Art 6.

19. Above, Art 10(1)(a).

20. Above, Art 10(1)(b).

21. Above, Art 10(1)(c).

22. Above, Art 10(1)(d).

23. *Spam Act 2003* (Cth).

24. Council Regulation (EC) No. 44/2001, 22 December 2000, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [Official Journal L 12 of 16.01.2001].

25. See, for example, the private international law rules of Italy.

26. Council Regulation (EC) No. 864/2007, 11 July 2007, on the law applicable to non-contractual obligations [Official Journal L 199 of 31.07.2007].

27. Convention on the law applicable to contractual obligations, opened for signature in Rome on 19 June 1980 [Official Journal C 27, 26 January 1998].

28. *Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I)*, 15 December 2005, COM (2005) 650 final, p. 20 <europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0650en01.pdf>, 20 March 2006.

29. Rome Convention, Art 2.

30. Above, Art 3(1).

31. Above, Art 5.

32. Above, Art 5(3).

33. Above, Art 5(2).

34. Michael Bogdan, *Internet and Private International Law*, in R. Pol_ák (ed) Introduction to ICT law — selected issues (July 2007), at 34.

35. Refer to the effect of *Trade Practices Act 1974* (Cth) s 67.

Illegal file sharing threatens growth of music

Sabiene Heindl MUSIC INDUSTRY PIRACY INVESTIGATIONS PTY LTD

In the last issue of the Internet Law Bulletin we ran an article by Adam Sauer in which he argued that P2P sharing technologies help disseminate culture. In this issue, the author argues the opposite point of view.

The argument that illegal file sharing is, on balance, beneficial, is fundamentally flawed as it is based on a number of misconceptions about the music industry and the impact of illegal file sharing. In short, illegal file sharing is the single biggest obstacle to the growth of new legitimate business models for online music distribution and more broadly the continued growth of music, both essential for the 'continuation of culture' that Adam Sauer endorses in his article 'Legitimising Web-based Music Piracy'.[1]

Five years after the emergence of a market for legal online music downloads, the digital music industry is continuing to grow. As Sauer himself notes, ARIA figures demonstrate that in 2007, Australian digital wholesale sales in total increased significantly and were up 126 per cent in unit sales and 43 per cent in dollar value.[2] Worldwide, there are over 500 legitimate digital music services offering over six million tracks — over four times the stock of a music mega-store. There is also a plethora of sites, including label and artist sites, where music can be obtained or streamed legally for free. Sauer suggests that there has been 'reluctance on behalf of record companies' to release music digitally. In fact, record labels are continuing to invest significant resources into digitalising the tens of millions of tracks in their respective catalogues, an exercise that often also requires a renegotiation of longstanding agreements with the artists to obtain appropriate digital rights.

However, unfortunately the rise in digital music sales has not been enough to offset the decreases in physical sales and therefore, in Australia, there continues to be a steep decline in revenues year-on-year. This is in part because it is extremely difficult, if not impossible, to compete with services that are illegally offering music for free without investing in or compensating the creators of that music.

Sauer suggests that illegal file sharing has no 'effect on profit' because 'most people are not making a profit in sharing music'. Unfortunately, this is not borne out by the results of numerous studies. In Australia, independent research suggests that 2.8 million people, or 18 per cent of the population, are actively involved in illegal downloading of music files, equating to 1 billion illegal files being shared per year by Australians alone. Fifty-seven per cent of illegal file sharers do not go on to purchase that music legitimately. Further, research in the US suggests that at least 20 per cent of illegal downloads would have otherwise been purchased legitimately.[3] On this basis, illegal file sharing causes staggering lost sales of at least 200 million digital tracks each year in Australia. This dwarfs the legitimate market, which was only 19 million tracks in 2007. The point is not that illegal file sharers are not making a profit from their activities but rather that the activity is negatively impacting on legitimate music sales.

Many people, including Sauer, attempt to justify illegal file sharing on the basis that it allows people to get tracks that they may not be able to access from legitimate digital sources. In short, stealing is okay if you can't get the product legitimately on the internet or because it is too difficult to source the legitimate physical product and use the recent format shifting exceptions under the *Copyright Act* to convert it to a digital format. This argument goes to the very heart of our moral and societal values. Does this mean that it is okay to break into a house and steal a limited edition painting because you can't simply buy it from a store? In any case, this is for the large part a moot point as the vast majority of illegal file sharing is of popular new-release music that can be easily and cost-effectively purchased legitimately online.[4]

The Australian music industry has made it clear that it has no intention at present to sue individuals. This is because litigation is a second-best option in our jurisdiction, not because 'the impact (of illegal file sharing) is not sufficient enough to bother [with litigation]'.[5] The Gower Report in the UK notes that P2P use had doubled in the US in the two years after the music industry commenced lawsuits against individuals and concluded that 'such lawsuits have not led to a significant reduction in P2P users.'[6] Therefore, litigating against individuals in Australia would not have the broader affect of systematically discouraging illegal file sharers from engaging in the activity. Nor will it achieve the objective of creating a consumer culture that respects creativity.

Therefore, the music industry in parts of the world, including Australia, is requesting that ISPs take a role in protecting intellectual property rather than letting copyright theft run rampant on their networks. A recent iPoque study in Europe suggests that the illegal file sharing traffic is producing *more traffic on the internet than all other applications combined* and therefore is substantially negatively impacting on the speed and cost of the network. In Australia, the 20 per cent of the population engaged in file sharing use close to 60 per cent of bandwidth. The Australian music industry believes that ISPs should implement a commonsense graduated

warning process, leading to disconnection of the internet connection as a last resort for persistent illegal file sharers. Governments in France, the UK, Japan and Hong Kong have recently supported this approach.

In conclusion, suggesting that 'the benefits of illegal peer-to-peer sharing outweigh the detriments' does not take account of the multifaceted situation at hand, nor does it look to the future. The reality is that the music industry is a highly speculative one, with record labels investing over 20 per cent of their revenues into finding and nurturing new talent, the majority of which do not even break even. Illegal file sharing undermines the ability of the music industry to obtain returns on investment so that it can fairly compensate the creators of the music. The sad reality is that the 'growth of culture' that Sauer argues for will be significantly diluted if songwriters and artists are no longer rewarded for creating music. ●

Sabiene Heindl,
General Manager,
Music Industry Piracy Investigations Pty Ltd (MIPI).

Endnotes

1. (2008) 11(3) INTLB p 45.
2. See <www.aria.com.au/pages/ARIAreleases2007wholesalemusicsalesfigures.htm>.
3. Institute for Policy Innovation, 'The True Cost of Sound Recording Piracy to the US Economy', *Policy Report 188*, August 2007 p 7.
4. A review of BigChampagne shows that 'Top Swaps' on illegal file sharing networks are popular music: <www.bigchampagne.com/>.
5. Above n 1.
6. HM Treasury *Gowers Review of Intellectual Property*, December 2006, p 102, available at <www.hm-treasury.gov.uk/media/6/E/pbr06_gowers_report_755.pdf>.

bytes

Consultative working group to improve cyber-safety

The members of the Cyber-Safety Consultative Working Group (working group) were announced on 15 May 2008 by the Minister for Broadband, Communications and the Digital Economy, Senator Stephen Conroy.

The working group has been formed as part of the government's program to improve online safety for children. It will:

- consider issues relating to cyber-safety that are faced by children in Australia;
- report to the government on the measures required to operate and maintain world's best practice safeguards for children engaging in the digital economy; and
- advise the government on priorities for the implementation of such measures by government and industry.

The working group will focus on issues such as cyber-bullying, identity theft, breaches of privacy, promotion of inappropriate social and health behaviours and exposure to inappropriate content. While doing so, the working group will take into consideration the online environment in which Australian children currently engage, Australian and international responses to cyber-safety issues and the potential for cooperation between Australian and international stakeholders in dealing with such issues.

The working group is made up of representatives from community groups, ISPs, industry associations, business and government organisations.

The government has also announced that it will establish a joint parliamentary standing committee to investigate and report on similar cyber-safety issues.

The working group was scheduled to first meet in late May 2008.

Marcus Fleming,
Blake Dawson.

Internet addresses to run out by 2011

The Organisation for Economic Co-operation and Development (OECD) published a report titled *Internet Address Space: Economic Considerations in the Management of IPv4 and in the deployment of IPv6* for the Seoul Conference The Future of the Internet Economy, which took place in June 2008.

The OECD report warns that 85 per cent of all available internet addresses are already in use and that at this rate, addresses will run out by 2011. The organisation is calling on governments and businesses to work together to meet the growing demand for internet addresses. They contend that this issue affects businesses throughout the world, as the future of the internet economy is at stake.

The internet protocol currently in use is IPv4. According to the report, there are three available options which can be considered to address the growing need for internet addresses:

- extend the current IPv4 Network Address Translation (NAT);
- make available for use all previously allocated but presently unused IPv4 addresses; or
- adopt IPv6 protocol worldwide.

The OECD is in favour of adopting the IPv6 protocol worldwide, as it sees it as the only long-term solution to the problem.

The US government and the European Commission are working on deploying IPv6 networks in the near future and the Chinese government has already started rolling out IPv6 in preparation for the 2008 Beijing Olympics, which is considered to be an ideal testing ground for mobile devices and transport systems running on the new internet protocol.

Florence Riviere,
Blake Dawson.

What's new in e-security?

Recently, the federal government has shown particular interest on issues of individual, business and government e-security.

On 13 June, the Minister for Broadband, Communications and the Digital Economy, Senator Stephen Conroy, and the federal Attorney-General, Robert McClelland MP, met with industry and community organisations in Sydney to 'discuss emerging e-security challenges'. According to the ministers, discussions at the forum, called Over the Horizon, will inform the government's future e-security policy deliberations.

The Over the Horizon forum officially concluded National E-security Awareness Week, which was launched by Senator Conroy on 6 June 2008 with the intention of highlighting steps that Australians could take to protect their data, computer and internet connection.

Senator Conroy then went to Seoul as vice-chair of the OECD Ministerial Meeting on the Future of the Internet Economy on 17 and 18 June. While at the meeting, Senator Conroy joined with other ministers from around the world in adopting the Seoul Declaration.

According to the minister, a key element of the Seoul Declaration is greater international collaboration on e-security and cyber safety. Conroy said that the declaration is intended to 'highlight a need for increased cross-border co-operation of governments

and enforcement authorities in the areas of improving cyber-security, combating spam, as well as protecting privacy, consumers and minors'.

Finally, on 3 July, the federal Attorney-General and Senator Conroy announced a whole of government review of e-security. According to Robert McClelland MP, 'the e-security review is an opportunity to look at what help the government can provide to develop a more secure and trusted electronic operating environment for both the public and private sectors'.

Ryan Grant, Associate,
Baker & McKenzie

ICANN frees up top level domains

In June, the International Corporation for Assigned Names and Numbers (ICANN) announced in principle support for removing restrictions on the generic top level domains which can be assigned. At present there are only 21 generic top level domains which are available for use (that is, domains in the form .com, .org, and .net etc). Under the new proposal, any string of letters can be applied for, although applications will be subject to an approval process. Examples of generic top level domains which will become available under the new scheme include .paris and .brandname. The new scheme will also permit gTLDs which use non-roman characters.

The application process does not require that existing trade marks will be automatically reserved to the relevant trade mark holder, but such holders will have an objection process that they can rely upon. The application process includes an auction to resolve any contention between multiple applicants for a given gTLD.

The new scheme is subject to finalisation of the proposed implementation and approval by the ICANN Board. This review is expected to occur in early 2009 with the scheme operational for applications by the second quarter of 2009.

The ICANN announcement is available at <www.icann.org/en/announcements/announcement-4–26jun08-en.htm>. ●

Brendan Scott,
Principal, Open Source Law.

contributions

Contributions to the *Internet Law Bulletin* are welcome.
Please submit notes (between 800 and 1500 words) for publication to:

EDITOR: Alison Hartman
LexisNexis Butterworths
Locked Bag 2222
Chatswood Delivery Centre NSW 2067
Ph: (02) 9422 2222 Fax: (02) 9422 2404
alison.hartman@lexisnexis.com.au

Copy should preferably be presented as an email with an electronic copy of the submission attached.

PUBLISHING EDITOR: Alison Hartman PUBLISHING OPERATIONS MANAGER: Anupama Bhattacharya PRODUCTION: Alexandra Berthold
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
For further information on this or other LexisNexis products, call Customer Relations: 1800 772 772 Monday to Friday 8.00am-6.00pm EST; email: customer.relations@lexisnexis.com.au; or visit www.lexisnexis.com.au for information on our product catalogue.
Editorial enquiries: alison.hartman@lexisnexis.com.au

ISSN 1329-9735 Print Post Approved PP 244371/00049 Cite as (2008) 11(4) *INTLB*