The Digital Divide - International Enforcement of Digital Lockup

Michael D Pendleton, Professor of Law,
School of Law, Chinese University of Hong Kong, Hong Kong SAR, China
Murdoch University, Western Australia

ABSTRACT

Virtually all valuable information is digitised. Delivery, use and application require this. Software, blueprints, films, music, medical diagnostics, automobile diagnostics are all capable of delivery online in digital form. Copyright not only prohibits reproduction, copying, adaptation, communication but also, some have suggested, mere access. Hacking, cracking, P2P, Bit Torrent, and Monolith are all methods of accessing this information surreptitiously. In the case of popular media this is normally done from the privacy of the family home. It is civilly actionable in most jurisdictions but rarely litigated due to expense and the public outcry. In Hong Kong it is criminal and vigorously prosecuted by the Intellectual Property Department. Will the technology 'haves' demand criminal protection for digital information in coming rounds of bilateral and multilateral treaties? Should such demands be opposed? This paper surveys the issue of criminal penalty for unauthorised access of digital information in the context of technology transfer.

1. Intellectual Property (IP) Issues & Digital Subject Matter

Information in digital form may consist of intense clusters of traditional intellectual property and other rights for the IP lawyer. A ‘communication’ of a multimedia work on the Net consists, in IP terms, of layers of every IP right, except plant breeders/varieties rights[1]. These rights can have different owners, in different countries, and for different times. Further, different jurisdictions may provide different legal answers as to whether rights subsist, for what period, and who is the owner. This will continue to bedevil any single countries attempt to rationalise the law in this area. Another problem is that laws to protect IP, such as those against circumvention of ‘digital lockup’[2], are usually contained in IP laws but arguably protect information which is not IP or otherwise protected. For example a website containing the works of Shakespeare may be locked pending payment for access. To circumvent this may give rise to civil and criminal liability under a copyright statute even though the content, the works of Shakespeare, is not protected.

Nevertheless, the United States is vigorously pursuing a policy of attempting to require all nation states to follow US IP law and practice including outlawing attempts to circumvent ‘digital lockup’. This policy is being implemented using bilateral as well as multilateral agreements. However, the policy is creating a new divide in access to scarce resources, in this case access to valuable information, the life blood

of the information economy. It is a 'digital divide', between those countries which adequately, largely in the view of the US government, protect digital information and those who do not.

2. Enforcing Digital Lockup -Cyber Police in Hong Kong

This policy of the US Government to enforce digital lockup throughout the world is welcome in some quarters. The government of the Hong Kong SAR of the People's Republic of China, unlike the mother country, has a long history of aggressive enforcement of IP. It seems it was the first territory in the world to use the criminal law to enforce IP.

Recently, an individual was arrested in Hong Kong and a conviction secured for a downloading a Hollywood movie[3]. The man was jailed for six months and fined for down loading 'Miss Congeniality 2' on his home PC for personal viewing. He used BT (bit torrent) technology – the industry standard, to download the movie. The Intellectual Property Department (IPD) of the Hong Kong SAR government in collaboration with the Customs and Excise Department arranged for the police to raid his house at night. The IPD was responding to pressure from US film and music lobbyists. At the time of proofing this article news had just been received that the conviction was upheld on appeal.

2.1 Enforcing US IP Law as the World Standard in IP

Conforming to US intellectual property law in the digital area is true to its origins. The US demanded that the world treat computer programmes as literary copyright work. It is demanding the same of digital subject matter i.e., largely mosaics of computer software, multimedia works which form the content of the Internet. The author does not necessarily have a problem with the policy objective of the US government, though their method of achieving them is another thing. Indeed the nature of the Internet is such that only a nation with considerable hegemony can ensure the right to exclude others, which forms the incentive to create which is at the heart of intellectual property, and the access rights, the necessary balance to the exclusion right of IP. One major problem with the policy objective is that US IP law contains major provisions against abuse such as the fair use right and anti trust law which many other nations do not currently enjoy.

2.2 Multimedia – Digital Subject Matter & Intellectual Property

Although even in the US, when it comes to digital subject matter and the Internet, there are very difficult question of balance between exclusion and access rights. The complexity of peer to peer (P2P) technology and the law as articulated in the US Supreme Court decision in *MGM v Grokster*[4] can sometimes mask the rather simple question of balancing user and provider interests. This process of balancing is not easy, but the issue, as opposed to its resolution, is often masked by the muddled and misunderstood law as well as the technology. In order to understand the P2P cases it is important to survey the liability of third parties internet service providers (ISPs) or

carrier service providers (CSPs)[5] and others who facilitate access to media which may infringe copyright or facilitate its infringement. This facilitation is referred to as 'authorising infringement in Anglo-Commonwealth copyright law and the functional equivalent appears to be 'vicarious liability' in US copyright law. A few words of introduction are in order as to the concept of authorizing infringement or vicarious liability.

2.3 The Anglo-Commonwealth Concept of Authorizing Infringement of Copyright

Applying the law as to authorisation of infringement of copyright derived from *UNSW v Moorhouse*[6], (sanctioning, countenancing or approving), the High Court of Australia held in *Telstra v APRA*[7] that Telstra was liable when one of its subscribers played music, for which they held no license, to callers who were "on hold". The decision was the cause of considerable concern to ISPs and CSPs. In Australia as elsewhere amendments were introduce to provide that CSPs are not to be taken to authorise infringements merely because such infringers used the facilities provided by the CSP[8]. A finding of authorisation of infringement must take into account the following factors, under Section 36(1A) and 101(1A) of the Australian Copyright Act, 1968, to cite but one example of this type of legislation: the CSPs power to prevent the infringing acts;

'…the relationship between the CSP and the infringer; and whether the CSP took reasonable steps to prevent the infringement including compliance with industry codes'

2.3.1 Litigation Relevant to S 101(1A)

In *Universal Studios v Cooper*[9] (currently awaiting decision by the Australian Federal Court) the issue is whether a CSP whose subscriber's website contains hyperlinks to a external website containing MP3 files constitutes authorisation of infringement, having regard to s.101 (1A) *Copyright Act.* Similarly in *Sony v University of Tasmania* [10](also currently awaiting decision by the Federal Court), the issue this time is whether the provision of search engines on university computers for students and staff constitutes authorisation of storage and communication of infringing music files

3. Carrier Service Provider Liability Pre Digital Millennium Copyright Act (DMCA 17 USC) United States Law

It seems there was no direct copyright liability for passive CSPs due to the activities of their subscribers[11]. Vicarious liability was treated leniently in *Netcom* [12] but the decision was effectively undermined in *Fonovisa*[13], where the 9th Circuit overruled on the basis of vicarious liability replied upon in *Netcom.*

3.1 DMCA Safe Harbour Provisions

Under s. 512(a-d) *17 USC*, safe harbour is provided for CSPs from infringement where copyright material receives:

A. basic routing & transmission
B. passive caching (subject to expeditious removal of access to infringing material upon notification);
C. data storage & web hosting (subject to removal of access on becoming aware of material or notified of it ('Take Down Notice' procedure) ;
D. is subjected to information location tools or technology (subject to similar conditions to C).

Conditions of Safe Harbour for the CSP
Acquiring safe harbour under the statute is subject to the CSP: not initiating the communication of the infringing material; not selecting the material or its recipients; policing and terminating accounts of repeat infringers; and complying with any relevant industry codes.

Recently Australia concluded a bilateral trade treaty with the US, the US Free Trade Agreement (USFTA)[14]. As is the case with other US bilateral trade treaties the treatment of digital subject matter according to the norms of US copyright law was a condition precedent to conclusion of the agreement[15].

The *US Free Trade Agreement Implementation Act, 2004 (USFTI Act*), Schedule 9 contains 11 parts dealing with copyright[16]. Most provisions take effect on 1January, 2005 except those expressed as dependent on the coming into force of the WIPO Performers & Phonograms, Treaty.

We are here concerned with the provisions as to carrier service liability (CSLs) and technological protection measures.

3.2 Carrier service Provider Safe Harbours in Australia

The *USFTAI Act, 2004* follows the *DMCA* "Safe Harbors' (same categories) but with some differences.

Category A (routing & transmission)
Any remedy against the CSP is limited to terminating the account and disabling access to online locations outside Australia. In ordering such a remedy the court must have regard to: harm to copyright owner; the burden of the order on the CSP; technical feasibility of the order; effectiveness of the order; and whether another form of order would be less burdensome.

Category B (passive caching)
To enjoy protection the CSP must ensure site access conditions are met, eg. access to site only to subscribers. The CSP must not make substantive modifications to cached material. The CSP must have policy of suspending repeat infringers and follow industry code. Caching must be an automatic process but manually selecting criteria for caching does not disqualify CSP from category B.

A CSP must disable access to material if notified on prescribed form that material on original site has been removed. If an industry code is in force the CSP must comply by updating material and not interfering with any technology monitoring 'hits' to website or material. If the above is complied with, remedy against CSP limited to removing or disabling access to infringing material; terminating an account; or a less burdensome but comparable order.

Category C (data storage & web hosting)
The CSP must have a policy of terminating repeat infringers accounts, complying with industry codes and not interfering with standard technical measures. The CSP must also, not receive a financial benefit directly attributable to the infringing activity if the CSP has the right and ability to control the activity. "Financial benefit' was defined in the *USFTAI Act*, and repealed and replaced in the *CLA Act* by s116AH(3) which seems to tie the immunity in with what the industry as a whole is doing.

Unlike the DMCA, and seemingly contrary to Art. 17.11.29(b)(v)(B) of the *USFTA*, the *USFTIA*, provides that CSPs in category C & D situations do not have to take action on receipt of a 'Take Down' notice, of itself. The CSP only had to act when infringement has been found by a court, and is referred to in the notice.
However, *Copyright Legislation Amendment Act*, 2004 passed in controversial circumstances in December, 2004, effectively reverses that. New Notice provisions are now applicable.

The CSP must now comply with two different sets of notice and take down procedures. The CSP must appoint a 'designated representative' to claim limited liability under the 'notice and take down' procedure.

First Notice & Take Down Procedure
This applies where notice from copyright owner or agent. The actual procedure is set out in the Copyright Regulations, 2004.

Second Notice & Take Down Procedure
This applies where CSP itself becomes aware of stored infringing material or aware of facts or circumstances indicating infringement. Where the above is complied with, the remedy to the copyright owner in these circumstances is as in category A, limited to terminating the account and disabling access to online material.

Category D (information location tools)
While it is clear these include hyperlinks, online directories and search engines provided by the CSP, where these are not provided by the CSP, it is a moot point as to whether they are covered. The two sets of conditions applicable to Category C apply here, as do the limitations on remedies against the CSP, and the notice and 'take down' procedure, but there is no counter notice or notification procedure.

Essential Action for a CSP
It is essential for a CSP to designate a representative (*Copyright Regs 20C*) and have protocols for action by time limits. The CSP must also be prudent in taking down material on its own initiative. If an employees come across what is clearly infringing material on a site they should be required to report it and the CSP should act [17].

4. P2P Cases in the US & Elsewhere

4.1 1st Generation Cases - where Liability Was Found

This is a complex area well surveyed in an article by Akester P, Copyright & the P2P Challenge[18]. The author draws a distinction between first and second generation P2P (peer to peer) technology and thus genre of cases, though this was before the United States Supreme Court decision in *MGM v Grokster*[19], which appears to conflate the genres back to the first where liability was found for contributory infringement (read authorisation of infringement in functionally equivalent Australian terminology). In the now famous *A&M V Napster*[20], and in *UMG v MP3.Com*[21], and *Re Aimster* [22] liability was found for contributory infringement. In these cases it seems clear the CSP has a degree of control over what subscribers do.

4.2 2nd Generation Cases – No Liability Found

In what appeared to be a second genre of P2P technology where the CSPs control over what subscribers do online was far more nebulous the Dutch Court of Appeals in *Buma v KaZa A* [23] and the United States Ninth Circuit Court of Appeals held in MGM v Grokster[24] that 'morpheus' and like software allowing unauthorised down loading of music did not constitute contributory infringement by the CSP. A significant part of the reasoning in both courts decisions was that the technology did not allow any real control by the CSP and was capable of lawful uses.

4.3 United States Supreme Court in *MGM v Grokster* [25]

In July 2005 the United States Supreme Court overruled the Ninth Circuit and held the CSP was guilty of contributory infringement. It disapproved of the citation of *Sony v Universal Studios*[26] and the fair use concept of "time shifting' as apposite to this case. While this article in no way purports to comment on the over 400 pages of unanimous decision of the court given by the separate opinions of Ginsburg and Bryer JJ (between whom other members of the court divided), it does seem on a cursory reading that the Ginsburg J's decision downplays the significance of the CSPs technological inability to effectively control the conduct of subscribers. Her decision seems to find liability on the basis that the CSP knew illegal conduct would occur and something has to be done to contain infringement on such a massive scale.

4.4 Provisions Relating to Anti-Circumvention of Technological Protection Measures (TPMs)

A TPM is a measure designed in the ordinary course of its operation, to prevent or inhibit copyright infringement by controlling access to the work or a copy control mechanism[27]. Importation, manufacture, and commercial dealing with devices that have limited commercial use other than to circumvent a TPM, are civilly and criminally actionable in many jurisdictions. Mere use of a TPM is not presently actionable in Australia but is actionable under the US *DMCA*..

In Australia, the High Court's impending decision in *Sony* v *Stevens* [28] would seem to have to take a position on either the trail judge's insistence that Sony's Play Station chip was not a TPM because it did not 'directly prevent or inhibit infringement during its operation'. Note that Sackville J, had held that transfer of data from CD to RAM & screen display was not reproduction. Note that this position is now reversed by Pt.10 Sch. 9 *USFTAI Ac.* Or it will have to endorse the Full Federal Court's unanimous position that provided the chip 'inhibited infringements occurring somewhere else and a different time by way of deterrence', Sony's chip was thus still a TPM. Either way, the decision will be largely irrelevant because of the new legislative provisions.

Impending Changes to TPM Definition
The definition of TPM under the *DCMA*, EU Directive and *AUSFTA* are not qualified by the present Australian *Copyright Act* requirement that the TPM act to "prevent or inhibit copyright infringement". Mere control of access to a work may be enough.

The USFTA gives Australia a two year grace period to legislate new TPM provisions. In doing so, Parliament should be mindful of evidence of attempted abuse of this right highlighted in the US courts decisions.

5. Using 'Digital Lockup' or Anti-Circumvention Provisions to Protect Non Copyright Content or for Extraneous Purposes

Examples of 'digital lockup' or anti-circumvention provisions being used to protect Non Copyright Content or for extraneous purposes are readily available from the US case law. In *Lexmark v Static Control* [29] **t**he defendant supplied generic print cartridges for Lexmark printers with code embedded in their chips to answer challenges from software in the Lexmark printer. The US appeal court rejected this was circumventing a TPM and characterised the software as preventing non Lexmark components functioning in the printer. The court effectively read into the *DCMA* a requirement that the function of the TPM must have a connection to copyright protection. The court was clearly worried about monopolies in spare parts.

Similarly in *Chamberlain v Skylink*[30] *t*he issue was similar to *Lexmark* and concerned remote controls for garage doors not of the plaintiff's manufacture. The remotes carried codes to access the security software embodied in the garage door opening mechanism. The court again asserted the *DMC*A provisions were to combat digital piracy not "protect non-copyright controls to access as such". Gajarsa J, opined that a different construction of anti circumvention in the *DMCA* provisions "would repeal the fair use doctrine".

S.116A of the Australian *Copyright Act, 1968*, permits circumvention for purposes including: reverse engineering for purposes of interoperability, error correction, security testing; copying from a library for research or study, and certain other uses. Art. 117.4.7(e)(I) – (viii) of *USFTA* allows certain new purposes including preventing children viewing content, encryption research, protecting personal information and law enforcement, but does not mention, error correction, study and research , Part VB, & others. There is no mention of the type of use in *Lexmark* or *Chamberlain.*

Art 17.4.7(e)(viii) of the *USFTA* allows classes of exceptions to be designated for non infringing uses of circumvention devices where a legislative or formal review finds credible evidence of adverse impact. No factors or guidelines as to what is an adverse impact are provided. Owners and consumers groups can both be expected to quarrel over attempts to designate non infringing use of circumvention devices by lobbying for formal or legislative review for these purposes.

Giving effect to the good sense evident in the US case law is difficult in Anglo Commonwealth jurisdictions due to the absence of a 'fair use' defence. These jurisdictions copyright legislation feature fair dealing, a much more limited defence.

5.1 The Absence of Fair Use in Anglo-Commonwealth Copyright Law

Last year the Australian Attorney General announced an internal inquiry into the need for a 'Fair Use' defence in Australia. It is to be hoped the Copyright Law Review Committee (CLRC) **Simplification of Copyright Report**[31] will be consulted, as it recommended a fair use defence to replace the present law's limited fair dealing defence quite some years ago. Many copyright lawyers representing both owner and user interests, I suspect, would agree on the need for a flexible fair use defence.

5.2 Securing Fair Dealing Rights

Even the limited defence of fair dealing can arguably be defeated under Anglo-Commonwealth law by contracting out of the right. In its '**Copyright & Contract'**[32] report the CLRC recommended that provided lawful access was obtained to online material, circumventing a TPM should be able to be used in certain circumstances to ensure the user benefited from the limited fair dealing & other rights under the *Copyright Act*. There has been no response from government on this report.

6. Conform to US Copyright Law or be Locked Out

The push by the US government through multilateral forums and bilateral agreements such as free trade agreements,confirm that access to technological and cultural products of US origin or dissemination is dependent upon trade partners enforcing provisions akin to US IP law, including criminal enforcement. Failure to do so will result in 'digital lock up'. The 'have nots' are yet again in jeopardy!

---

[1] Even that may change if research to find biological forms of computer memory, such as algae, succeed. Such algae varieties may give rise to patent and plant breeder's rights.
[2] A computer programme which requires a password, or payment or both, before 'unlocking' the content of the device, website or other repository.
[3] HKSAR v Chan, Mags. Ct. 20 Dec, 2005.
[4] 545 US, 125 SCt 2764 (2005)
[5] A slightly wider term than ISPs as the term may even comprehend provision of a search engine on a website.
[6] (1975) 133 CLR 1
[7] (1997) 38 IPR 294
[8] S.39B & 112E *of Digital Agenda Amendments to* Copyright Act
[9] [2004] FCA 78
[10] [2003] FCA 724

[11] *Sega v Maphia* 857 F.Supp 679 (N.D. Cal 1994), *Religious Technology v Netcom* 907 F.Supp 1361 (N.D. Cal *1995); contra* Playboy v Freda (839 F.Supp 1552 (MD Fla 1993

[12] Fn 5

[13] (76 F.3d 259 (9th Cir. 1996)

[14] The *Australia – US Free Trade Agreement (USFTA)* took effect on 1 January, 2005.

[15] See generally, Varghese J, 'Guide to Copyright and Patent Changes in the US Free Trade Agreement Implementation Bill 2004' (Aug 2004) Parliamentary Library – Current Issues Brief No.3, 2004-5.

[16] The copyright provisions related to Performer's Rights in Sound Recordings; Performer's Moral Rights; Performer's Protection; Copying & Communicating Broadcasts of Performances; Duration of Copyright in Photographs; Duration of Copyright in works and other subject matter; Carrier Service Providers; Technological Protection Measures (the required provisions as to Technological Protection Measures (TPM) have a two year grace period for their introduction); Electronic Rights management Information ; Criminal Offences; and Encoded Broadcasts.

17 With thanks to my colleague Warwick Rothnie, of the Melbourne Bar for sight of the unpublished paper 'Update on Copyright Law –2005'.

18 [2005] EIPR 106

19 See Fn 1.

[20] 114 F.Supp. 2d 896 (N.D. Cal 2000)

[21] 92 Fed. Supp. 2d. 349 (S,D.N.Y. 2000)

[22] 334 F. 3d 643 (7th Cir. 2003)

[23] Court of Appeals (1370/01 SKG)

[24] 259 F.Supp 1029 (C.D. Cal 2003

[25] Fn 4 above

[26] 464 US 417

[27] TPMs are so defined in (s.10(1) *C Act*).

28 [2000] FCA 906

29 387 f.d522 96th Cir. 2004)

30 381 F.3d 1178 (Fed.Cir. 2004)

[31] Report No. 112

[32] Report No 116