

FOUR FOUR

Technological Protection Measures: South Africa Goes Overboard. Overboard.

Coenraad Visser¹

ABSTRACT: In the digital world, technological protection measures (TPMs) are increasingly used by authors to safeguard against copyright infringement. TPMs mainly control access to copyright works and/or the use of such works (for example, by limiting copying of these works). The international framework for protection against the circumvention of TPMs is found in the WIPO Copyright Treaty (WCT) of 1996. This article examines this framework, and how the international obligations have been discharged in the United States and Europe. In this context the extent of the protection, and possible exceptions and limitations, are considered. It is noted that overbroad protection would be particularly prejudicial to research and education in developing countries, and in this way would deny them the benefits of access to information and learning through global information networks. Finally, the position in South Africa is considered with reference to the Electronic Communications and Transactions (ECT) Act of 2002, which adopts a level of protection far stricter than that adopted in any of the developed countries surveyed.

INTRODUCTION

In a joint intervention of Electronic Information for Libraries (eIFL) and the International Federation of Library Associations (IFLA) at the General Assemblies of the World Intellectual Property Organisation (WIPO) in Geneva (from 25 September to 3 October 2006), Teresa Hackett of eIFL stated:

Access to knowledge is essential for the functioning of a healthy and democratic society. Access to knowledge is fundamental to education and research and the creation of human capital upon which the development of societies depend. This is especially true in the information society where economic progress depends on having a literate and educated population (eIFL & IFLA, 2006).

Although these comments were made in the context of the discussion of a proposed broadcasters' treaty, they are entirely appropriate to frame a consideration of technological protection measures (TPMs), mechanisms that are controversial and potentially destructive of users' rights (or privileges) in the context of copyright and related rights.

Many of the authors in this volume have referred in passing to TPMs, and so it is appropriate to consider their impact and regulation in more detail. In this article I shall canvass the international framework, the discharge of their international obligations by the United States and Europe, and the position in South Africa.

WHY TPMs?

In the analogue world, copyright infringement by unauthorised copying was curtailed by technological constraints - the available technology made copying rudimentary, cumbersome,

¹ Coenraad Visser is Professor of Intellectual Property Law and Head of the Department of Mercantile Law at the University of South Africa.

and expensive (Ginsburg, 2005: 2-3). Where unauthorised copying did occur on a large scale, the infringement provisions in copyright laws sufficed, as authors could enforce their rights against commercial enterprises that engaged in extensive copying and dissemination (Ginsburg, 2005: 3). Whatever copies individual end users made were unlikely to affect the author's market for her work.

The position changed, of course, with the advent of the digital world. The digitisation of works and the establishment of global information networks (like the Internet) opened up new opportunities for authors to distribute their works globally. At the same time, these technological advances increased the risk of copyright infringement. Also, digital media shift the analogue technological balance – now, economically significant infringing acts are no longer confined to entities earlier in the distribution chain. Instead, they can be committed by any end user with access to a computer and the Internet. In a nutshell, the challenge to copyright in this context is to protect copyright works in a world where:

- duplication is easy and inexpensive;
- every copy, whether from the original or another copy, is perfect; and
- distribution to users around the world can be achieved virtually cost-free and instantaneously over the Internet (Marks & Turnbull, 2000: 198).

It became clear to authors that the legal sanctions for copyright infringement had to be bolstered by TPMs that would disable end users from availing themselves of some of digital copying technology's potential for reproducing and redistributing copyright works (Ginsburg, 2005: 3). Pithily put, "the answer to the machine lies in the machine" (Clark, 1996: 139).

Examples of TPMs are:

- anti-copying devices that make copying of a work more difficult, or prevent copying altogether;
- devices that control access to copyright works (encryption, passwords, and the like);
- proprietary viewers (software that keeps a digital work always under its control, and so allows only uses authorised by the author); and
- watermarking or fingerprinting (techniques that add an invisible digital mark in the digital code of works to enable authors to identify and authenticate their works) (Dusollier, 1999: 285-286).

Yet any TPM provides only short-term relief – TPMs are always vulnerable to attack by hackers, especially as the processing capabilities of computer hardware and software continue to advance rapidly (Marks & Turnbull, 2000: 199). So authors concluded that the legal protection of copyright should be supplemented by technological protection, which, in turn, should be backed up by legal protection against the circumvention of such technological protection.

In December 1996, the World Intellectual Property Organisation (WIPO) hosted a Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions. On 20 December 1996, the conference adopted two treaties, one of them the WIPO Copyright Treaty (WCT) (WIPO, 1996). The Treaty entered into force on 6 March 2002.

The question of the legal protection of TPMs against circumvention was one of the thorniest at the diplomatic conference. Much of the discussion focused on three issues:

- whether the prohibition should extend to circumvention devices as well as circumventing conduct;
- whether equipment should be required to respond to particular TPMs; and
- what were the appropriate exceptions to a circumvention prohibition (Marks & Turnbull, 2000: 200).

After protracted negotiations (Ficsor, 2002: 396-406), the diplomatic conference agreed on the following compromise wording for article 11 of the WCT:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law (WIPO, 1996).

Article 11 contains the following key elements:

- the subject matter protected – “effective technological measures”;
- the specification “used by authors” (and, by extension, their successors in title);
- the specification of the connection with authors’ rights under the WCT or the Berne Convention for the Protection of Literary and Artistic Works (their economic and moral rights);
- the prohibited act – “circumvention”;
- the restriction on the prohibition – only circumvention of TPMs that “restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law”.

I shall not here analyse article 11 in any detail but will make three brief comments.

First, “effective” does not connote that if a TPM can be circumvented, it is not “effective” (Ficsor, 2002: 545). Such an interpretation would be absurd. Also, “effective” introduces a knowledge requirement – a person inadvertently circumventing a TPM should not be liable.

Second, the prohibited act is stated to be the circumvention of a TPM. It was hotly debated whether the WCT should strike at both the act of circumvention and at circumvention devices. The argument against the inclusion of circumvention devices is that technology is neutral –

the same device can be used for lawful and unlawful purposes; to decrypt films in the public domain, or to decrypt films under copyright; to make limited copies for illustration in teaching; or to make unlimited copies for distribution over the Internet. The balance is delicate:

If the prohibition sweeps too broadly, it may bar the manufacture and dissemination of devices or services that have legitimate uses other than to circumvent controls on access to copyrighted works. Too extensive a prohibition may frustrate whatever legitimate activities the devices may permit. Equally importantly, too broad a definition may hamper the development of useful new technologies. On the other hand, if national law provided that a device may be distributed so long as it is capable of being put to use for non-infringing purposes, the prohibition would likely become meaningless (Ginsburg, 2005: 9).

The argument for a sweeping prohibition has been stated thus:

For several reasons a “conduct only” approach is insufficient. Circumvention conduct is generally not public; individuals usually undertake it in the privacy of their homes or workplaces. While the results of such activity, such as a software utility program that “hacks” a copy protection measure, may be made public, the conduct leading up to the cracking of the protection system is usually private. It is neither feasible nor desirable to undertake systematic monitoring of private conduct to deter circumvention activity. In any event, most people will not undertake the time and effort to crack a copy protection measure on their own. If, however, people can legally purchase (or receive for free) devices or services that defeat these measures, then it becomes more difficult to maintain the integrity and fulfill the purpose of protection technologies (Marks & Turnbull, 2000: 201).

It has been argued that, to constitute “adequate legal protection and effective legal remedies”, protection against the circumvention of TPMs should strike at both the actual act of circumvention and any preparatory act, including supplying a device that will enable circumvention (Ginsburg, 2005: 8).

Third, article 11 delegates to national legislation the designation of permissible acts, provided that these are in line with the exceptions and limitations in the Berne Convention and the WCT (Ginsburg, 2005: 8-9).

Article 11 has to be implemented in national legislation by each Contracting Party. By way of comparison, I shall refer to two pieces of implementing legislation – in the United States, the Digital Millennium Copyright Act (DMCA) which inserted section 1201 into the Copyright Act of 1976 (United States, 1998), and, in Europe, the Information Society Directive (European Commission, 2001).

THE UNITED STATES: THE DMCA

Section 1201 states three new violations:

- to circumvent TPMs that control access to copyright works;

- to manufacture, disseminate, or offer, and so on, devices or services that circumvent access controls; and
- to manufacture, disseminate, or offer, and so on, devices or services that circumvent a TPM that “effectively protects a right” of the author.

This provision extends the scope of copyright in four ways:

- it creates a claim for unauthorised access to copyright works;
- it makes distributors of circumvention devices directly liable for the dissemination of the means to gain unauthorised access;
- it makes distributors of circumvention devices directly liable for the dissemination of the means to make copies or to engage in communications to the public; and
- it makes the distributors of both kinds of devices liable even if some of the end users to whom the devices are distributed would use them for non-infringing purposes (Ginsburg, 2005: 12).

The courts have ruled that “effective” protection does not connote protection that is especially difficult to crack.²

Note that section 1201 prohibits the act of circumventing an access control, and the trafficking in devices that circumvent access controls or rights controls. It does not prohibit the act of circumventing a rights control, as such act will either be an act of direct copyright infringement, or be legitimised by an exception such as fair use.

Device and services manufacture and trafficking are statutorily prohibited in three instances:

- where the device was “primarily designed or produced for the purpose of circumventing” a TPM that “effectively controls access” to a copyright work, or “effectively protects a right” of the author;
- where the device was not primarily designed to circumvent but actually “has only [a] limited commercially significant purpose or use other than to circumvent”; and
- where the device is “marketed” as a device to be used to circumvent access or rights controls.

The statute provides for a variety of exceptions, including for reverse engineering, encryption research, and security testing. It has been argued that these exceptions are “overly narrow and shortsighted” and that they should be supplemented by “a more general ‘other legitimate purposes’ exception” (Samuelson, 1999: 25-28).

In bilateral free trade agreements (FTAs), the United States Trade Representative almost invariably insists on imposing an obligation on its contracting partner to enact protection of TPMs along American lines.³

² *321 Studios v MGM* 307 F Supp 2d 1085 (ND Cal 2004); also *Universal Studios v Reimerdes* 111 F Supp 2d 346 (SDNY 2000), *aff'd sub nom Universal City Studios Inc v Reimerdes* 273 F 3d 429 (2d Cir 2001).

³ For example, in the FTAs with Australia (http://wwwustr.gov/Trade_Agreements/Bilateral/Australia_FTA/Final_Text/Section_Index.html, accessed 1 October 2006), and Bahrain (http://wwwustr.gov/assets/Trade_Agreements/Bilateral/Bahrain_FTA/final_texts/asset_upload_file211_6293.pdf, accessed 1 October 2006).

EUROPE: THE INFORMATION SOCIETY DIRECTIVE

Articles 6.1 and 6.2 of the Directive oblige Member States to protect authors against the circumvention of any effective TPM, and against the trafficking in circumvention devices and services. Unlike the DMCA, the Directive does not distinguish between access control and copy (rights) control.

Article 6.4 relates to the dilemma facing an end user who wants to exercise a copyright exception or limitation but who is constrained from doing so by a TPM (Braun, 2003: 499). This provision states:

in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law ... the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned...(European Commission, 2001).

The implementation of this provision in various Member States has been tortuous and varied (Braun, 2003: 501-502). It is clear that the Directive prefers authors and end users to strike their own bargain, and that Member States should intervene only in the absence of such a bargain (Dusollier, 2003: 63).

LESSONS FROM THE UNITED STATES AND EUROPE

The ways in which the United States and Europe implemented the prohibition against the circumvention of TPMs threaten legitimate use: in the United States and Europe, because the devices necessary to circumvent for non-infringing purposes are prohibited; and in Europe, because the implementation by Member States of the exceptions to the prohibition on circumvention is not mandatory. This can have the following far-reaching consequences for users of digital works protected by copyright and TPMs:

THE UNAVAILABILITY OF TRADITIONAL COPYRIGHT DEFENCES: the circumvention of TPMs constitutes a violation separate of copyright infringement (Singer, 2002: 128). Liability arises not for copyright infringement but for the circumvention of a TPM (Lunney, 2001: 839). Since the circumvention of a TPM is a violation distinct from copyright infringement, the same exceptions and limitations that serve as defences against actions for copyright infringement would not be available in cases of the circumvention of TPMs (Besek, 2004: 394). So end users will not be entitled to circumvent TPMs in order to exercise their traditional privileges.

THE DIGITAL LOCK-UP OF COPYRIGHT WORKS: since end users are not allowed to circumvent TPMs even for non-infringing purposes, authors can now digitally lock up their works or require payment for each access and use of the work, which makes it impossible for end users

to browse or view the protected works. Even where a work exists in an alternative format, the exercise of a user privilege in relation to an alternative format may be so inconvenient that it can, practically, be regarded as impossible. Such works are digitally locked up despite the existence of alternative formats (Besek, 2004: 481).

THE DIGITAL LOCK-UP OF WORKS IN THE PUBLIC DOMAIN: neither the American nor the European prohibition on circumvention and trafficking in circumvention devices is conditional on subsequent copyright infringement. Works in the public domain protected by technological protection measures are rendered inaccessible, as any circumvention (even circumvention of technological protection applied to works in the public domain) will result in a contravention of the prohibition. This can, of course, result in a digital lock-up of works in the public domain.

PAYMENT FOR USE: access control technologies control not only initial access but also every subsequent access (Ginsburg, 1999: 147). For each access, initial or subsequent, an end user needs an access key. The author usually provides access keys only against payment. With access controls protected against circumvention, end users can now be required to pay for each access (Besek, 2004: 467). The drawback of such a pay-per-use model is that even users who want to access and use a work in accordance with a copyright exception, which use would have been free in the past, can now be required to pay for such access. The fact that payment can now be required for each and every access of a work can result in a situation where no use of a copyright work will be free, not even browsing. In the analogue world it was possible to page through a book at no cost to determine whether you wanted to obtain it. In the digital world, even mere browsing can have cost implications, since browsing requires access, and access can be gained only against payment.

USER PRIVACY: the ability of authors to control access to (and hence the use of) their works will make it easier to prevent copyright infringement from taking place, or to detect copyright infringement after it took place (Smith, 1997: 418). But it may also have serious privacy implications for end users. In the digital world, it is private individuals who access and use works, and so unauthorised access can be detected only by policing private behaviour. To enforce a prohibition on circumvention would involve entering into the private sphere of the user. This type of policing has been made possible by metering technologies, which reveal not only the type of information accessed, but also the identity of the person who accessed it. It is questionable whether this type of policing is desirable in any democratic society (Koelman, 2000: 276-277).

THE INABILITY TO USE COPYRIGHT WORKS THAT WERE OBTAINED LAWFULLY: the fact that possession of the physical object that contains the copyright work (the CD-ROM, for example) no longer guarantees access to the work can have serious implications for the possessor of such object. Even a lawful possessor will not be able to access a copyright work shielded behind a TPM

without an access key, or without circumventing the TPM. And without access, it is impossible to use the copyright work.

It goes without saying that global information networks like the Internet offer significant opportunities for improving access and transfer of knowledge for developing countries:

For example, the growing size and number of digital libraries creates unprecedented kinds of access to all published information anywhere in the world. In the future, developing countries may be able to build a national digital network to provide access to library resources from around the world to every remote village.... Similarly, initiatives such as the African Virtual University (AVU) are showing the potential of the Internet as a tool and resource for distance learning in the developing world. Since its launch in 1997, more than 24,000 students in 17 African countries have completed semester-long courses in technology, engineering, business and the sciences through the AVU. It also provides students with access to an on-line digital library with over 1,000 full text journals and the AVU web site currently receives more than one million hits per month (UK CIPR, 2002: 117-118).

But these opportunities can be lost, in the ways shown above, by providing overbroad protection along American or European lines for protection against the circumvention of TPMs:

... technological protection rescinds traditional "fair use" rights to browse, share, or make private copies of copyrighted works in digital formats, since works may not be accessible without payment, even for legitimate uses. For developing countries, where Internet connectivity is limited and subscriptions to online resources unaffordable, it may exclude access to these materials altogether and impose a heavy burden that will delay the participation of those countries in the global knowledge-based society (UK CIPR, 2002: 118).

Where developing countries do adopt protection of TPMs against circumvention, appropriate exceptions and limitations in favour of research and education should be enacted at the same time.

SOUTH AFRICA

South Africa has signed the WCT but not ratified it. So the Copyright Act 98 of 1978 is predictably silent on the issue of TPMs.

However, in 2002 Parliament enacted the Electronic Communications and Transactions (ECT) Act 25 of 2002 (RSA, 2002). Chapter XIII deals with cyber crime. For the purposes of this chapter, the term "access" includes "the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data" (section 85). A person who intentionally accesses data without authority or permission to do so commits a criminal offence (section 86(1)). Also, any person "... who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is

designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section”, commits a criminal offence (section 86(3)). The same sanction meets a person “... who utilizes any [such] device or computer program ... in order to unlawfully overcome security measures designed to protect such data or access thereto” (section 86(4)).

In South Africa, then, the prohibition on the circumvention of TPMs that control access to copyright works is complete – not only the circumvention of access control is proscribed, but also trafficking in devices that are “designed primarily” for circumventing access control. And the prohibition is absolute – there are no exceptions; no technical exception (such as for reverse engineering, encryption research, and security testing); nor an exception in favour of research or education.

It is incomprehensible that South Africa, a developing country, should opt for a system of protecting TPMs that is far more destructive of research and education than the systems adopted in the United States and Europe. Were the United States to conclude a free trade agreement with the Southern African Customs Union (SACU),⁴ and were such agreement to mandate the adoption of protection of TPMs along American lines, researchers and educators in South Africa would be better off than they are now. It is a supreme irony that the South African negotiators have been resisting the inclusion of such protection in an FTA, probably because the left hand (one government department) does not know what the right hand (another government department) has done. □

⁴ On the background to the negotiating process from an American perspective, see http://www.ustr.gov/Trade_Agreements/Bilateral/Southern_Africa_FTA/Background_Information_on_the_US-SACU_FTA.html, accessed 1 October 2006.

REFERENCES

- Besek, JM (2004) Anti-circumvention laws and copyright: A report from the Kernochan Center for Law, Media and the Arts, *Columbia Journal of Law & the Arts*, Vol. 27, No. 4, Summer; Columbia Law School, New York, NY.
- Braun, N (2003) The interface between the protection of technological measures and the exercise of exceptions to copyright and related rights: Comparing the situation in the United States and in the European Community, *European Intellectual Property Review*, Vol. 25, No. 11, November; Sweet & Maxwell, Oxford.
- Clark, C (1996) The answer to the machine is in the machine, in Hugenholtz, PB (ed), *The future of copyright in a digital environment*, Kluwer Law International, London.
- Dusollier, S (1999) Electrifying the fence: the legal protection of technological measures for protecting copyright, *European Intellectual Property Review*, Vol. 21, No. 6, June; Sweet & Maxwell, Oxford.
- Dusollier, S (2003) Exceptions and technological measures in the European Copyright Directive of 2001 – an empty promise, *International Review of Intellectual Property and Copyright Law*, Vol. 34, No.1, Max Planck Institute Intellectual Property; Competition and Tax Law, Munich.
- eIFL & IFLA (2006) Statement by International Library Groups at WIPO General Assembly; Electronic Information for Libraries (eIFL) and International Federation of Library Associations (IFLA), Geneva, <http://ipjustice.org/wp/2006/10/03/statement-by-international-library-groups-at-wipo-general-assembly>, accessed October 2006.
- European Commission (EC) (2001) *Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001, on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society*, <http://europa.eu/scadplus/leg/en/tyb/tyb26053.htm>, accessed 11 March 2004.
- Ficsor, M (2002) *The law of copyright and the Internet: The 1996 WIPO treaties, their interpretation and implementation*, Oxford University Press, Oxford.
- Ginsburg, JC (1999) Copyright legislation for the 'Digital Millennium', *Columbia-VLA Journal of Law and the Arts*, Vol. 23, No. 2, Spring; Columbia Law School, New York, NY.
- Ginsburg, JC (2005) *Legal protection of technological measures protecting works of authorship: International obligations and the US experience*, Columbia Public Law & Legal Theory Working Papers, <http://lsr.nelco.org/columbia/plll/papers/0593>, accessed 1 October 2006.
- Koelman, KJ (2000) A hard nut to crack: The protection of technological measures, *European Intellectual Property Review*, Vol. 22, No. 6, June; Sweet & Maxwell, Oxford.
- Lunney, GS (2001) The death of copyright: Digital technology, private copying and the Digital Millennium Copyright Act, *Virginia Law Review*, Vol. 87, No. 5, September; University of Virginia, Charlottesville, VA.
- Marks, DS & Turnbull, BH (2000) Technical protection measures: The intersection of technology, law and commercial licences, *European Intellectual Property Review*, Vol. 22, No. 5, May; Sweet & Maxwell, Oxford.
- Republic of South Africa (RSA) (2002) *Electronic Communications and Transactions (ECT) Act*, Act 25 of 2002.
- Samuelson, P (1999) Intellectual property and the digital economy: Why the anti-circumvention regulations need to be revised, *Berkeley Technology Law Journal*, Vol. 14, No. 2, Spring; University of California at Berkeley, Berkeley, CA.
- Singer, P (2002) Mounting a fair-use defense to the anti-circumvention provisions of the Digital Millennium Copyright Act, *University of Dayton Law Review*, Vol. 28, No. 1, Fall; University of Dayton, Dayton, OH.
- Smith, NA (1997) United States of America, in Dellebeke, M (ed), *Copyright in cyberspace: Copyright and the global information superstructure*, Cramwinckel, Amsterdam.
- UK Commission on Intellectual Property Rights (CIPR) (2002) *Integrating intellectual property rights and development policy*, London http://www.iprcommission.org/graphic/documents/final_report.htm, accessed 1 October 2006.
- United States (1998) *Digital Millennium Copyright Act (DMCA)*, Pub. L. No. 105-304, 112 Stat. 2860, 28 October.
- World Intellectual Property Organisation (WIPO) (1996) *WIPO Copyright Treaty (WCT)*, www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html, accessed 1 October 2006.