

# The WIPO Treaties: Technological Measures

March 2003

## WHAT ARE TECHNOLOGICAL MEASURES?

With the introduction of legal protection for technological measures, the WIPO Treaties create a unique new way of protecting copyrighted products as new digital and internet-based uses emerge.

The treaties recognise that authors and other rights owners increasingly rely on technical means—commonly known as technological protection measures or TPMs—such as encryption and other mechanisms to control unauthorised copying, transmission and use of their products.

TPMs take various forms and their features are continually changing, but some major features remain constant. The most basic and most important

kind of TPM is **access control** technology. One common way of controlling access is encrypting or scrambling the content. In such case the user gets the data but must follow an additional procedure to make it usable.

Another form of access control is a procedure that allows access to a source only with proof of authorisation, for example, password protection for a computer server.

The other major type of TPM, **copy or use controls**, enable the rights owner to allow certain permitted activities but to prevent illicit activities by a user who has access to the work.

The WIPO Copyright Treaty (WCT) and the WIPO Per-

formances and Phonograms Treaty (WPPT) require adequate legal protection and effective legal remedies against the circumvention of TPMs applied to protected works and phonograms. (WCT Art. 11; WPPT Art. 18.)

These provisions are formulated in a broad and neutral way, oriented more to the desired result than on how to achieve it. In implementing these treaty provisions, however, governments have recognised that their laws need to cover the **act of circumvention** itself, as well as the manufacture and distribution of a range of **circumvention devices**, in order to provide adequate and effective protection.

### EXECUTIVE SUMMARY

**Technological protection measures (TPMs) deter piracy, encourage rights owners to use new media like the internet, and provide consumers a sophisticated new range of ways of enjoying music.**

**The WIPO Treaties require effective legal protection of TPMs. Governments have recognised that this means protecting against 'hacking' and covering a range of circumvention devices and related illicit activities.**

## WHY IS IT IMPORTANT TO PROTECT TPMs?

Technological solutions themselves are not invulnerable. Technical systems can be hacked. Unauthorised passwords and access codes frustrate access-control software. And the making and distribution of circumventing devices pose a serious danger to the integrity of any TPM.

As no technological measure can permanently resist deliberate attacks, a TPM is only as good as its legal protection.

Protecting TPMs is important both for rights owners and consumers. Of course, TPMs de-

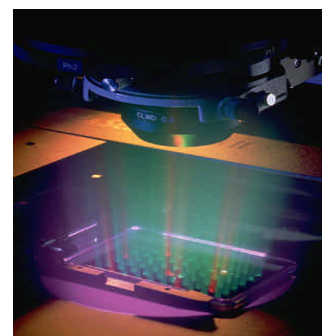
ter piracy, and encourage rights owners to use new media like the internet.

But by allowing a wide range of listening, copying and transmission options, TPMs also permit the development of new marketing, distribution and usage models, which open up a sophisticated new range of ways of enjoying music.

Consumers will benefit from these new ways of enjoying music and other copyrighted products, but only if TPMs are meaningfully protected.

TPM protection also benefits telecommunications and equipment providers. Internet services profit from increased traffic and legitimate electronic commerce in copyrighted material.

And consumer electronics and computer producers, which spend substantial sums developing new equipment and encryption technologies to play protected material, find their innovation frustrated and their investment rendered worthless if TPMs can be neutralised by hacking.



## HOW SHOULD THIS BE IMPLEMENTED?

### WIPO TREATY TEXT

#### WCT Art. 11.

*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.*

#### WPPT Art. 18.

*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorised by the performers or the producers of phonograms concerned or permitted by law.*

Most countries are finding that their copyright laws require some modernising to deal with TPM protection adequately. There are several elements that governments and rights owners have found crucial to effective legal protection for TPMs:

■ **Protection of access and copy control technologies.** The treaties require protection of TPMs (1) that are used in connection with the exercise of rights, and (2) that restrict unauthorised acts. This only covers TPMs applied to works protected by copyright or related rights.

Clearly this protection should apply to copy and use control TPMs that directly restrict unauthorised reproduction, public communication, or other direct exercises of the rights owner's rights.

Protection likewise should apply to access-control technologies, which also meet both tests of the treaties. Rights owners use access control, presently the most popular type of TPM, in connection with the exercise of their rights—whether selling physical copies or disseminating electronic copies to the public.

Access controls not only prevent unauthorised use but also discourage unauthorised reproduction, distribution and transmission.

■ **Protection against act of circumvention.** The treaties explicitly require legal protection and effective remedies against the act of circumvention of TPMs. Circumvention is sometimes called 'hacking'—manipulating the technological measure in some way so as to limit or eliminate the function it was designed to perform. The US law implementing the treaties defined circumvention as 'avoiding, bypassing, removing, deactivating, or otherwise impairing' a technological measure.

■ **Prohibition of circumventing devices.** Adequate legal protection and effective legal remedies cannot stop at prohibiting circumvention itself. In order to control widespread hacking and other circumventing activities, circumvention devices and other means designed to facilitate hacking also must be controlled.

This does not require outlawing multi-purpose devices like personal computers as such, simply because they can be used for a range of illicit purposes. Governments have recognised that devices must be controlled, however, if they are **designed or adapted** to circumvent.

This formulation has been refined in EU legislation and elsewhere to include devices that (1) are **primarily designed or produced** for the purpose of circumvention, (2) have only a **limited commercially significant purpose or use** other than to circumvent; or (3) are **marketed, promoted or advertised** for circumvention purposes.

■ **Devices, components and other means.** Circumvention devices are not always an isolated 'black box', such as a pirate decoder. They can also be one part of a more complex piece of equipment, or an intangible means such as computer software or access codes, that has the same function as a stand-alone circumvention device.

It is thus important that rules on circumvention devices apply equally to **parts and components** of devices, **software, algorithms** and **access information** such as **passwords** and **access codes** that otherwise meet the definition of an illicit device.

■ **Manufacture, distribution, offering to the public, communication of devices and services.** A range of activities related to circumvention devices should be covered. In most cases, treaty imple-

menting legislation has extended to all manner of manufacture, marketing, offering to the public and distribution of circumvention devices, as well as services that assist with such circumvention.

Not only are the features of TPMs and devices subject to continuous change, but the catalogue of activities that promote circumvention of TPMs also will change over time—requiring a broad definition of the acts covered by legislation dealing with circumvention devices and services.

■ **Effective remedies.** The treaties also explicitly call for effective legal remedies. This is of great importance, because action against hacking and other circumvention of TPMs must be sufficiently speedy, efficient and deterrent to counteract the otherwise great incentive hackers and pirates have to break TPMs and steal content.

Effective legal remedies should include both **criminal** law sanctions and **civil** law remedies. Criminal penalties should permit fines and prison terms in appropriate cases.

To serve as a deterrent, civil law should allow fast and efficient preliminary proceedings, injunctive relief, payment of damages including statutory damages, and the obligation to cooperate in neutralising harm already caused.

To get illicit devices out of circulation, remedies also should allow tracing, seizure, retention and destruction of physical devices and intangible software and information.

Criminal penalties and civil remedies should not be any lower than those available for copyright infringement.

## FREQUENTLY ASKED QUESTIONS (FAQS)

### How strong must a technology be in order to enjoy protection?

A TPM should be protected as long as, in the ordinary course of its operation, it effectively restricts access to or use of the content in any manner. There is no threshold standard of sophistication or security. The fact that a TPM has been circumvented, or the availability of a circumventing device, should not affect whether a device is deemed 'effective'. TPMs that have been subjected to attacks are the ones that need protection most.

### Could someone be held liable for unknowingly assisting in the circumvention of a protected TPM?

No. The offering and supply of services and assistance in the circumvention of TPMs need only be prohibited if the activity, viewed subjectively or objectively, has this purpose.

### Will TPMs lead to excessive restrictions on access to works or even public-domain materials?

No. TPMs permit wider and more convenient access.

Technology permits rights owners to cater to the demands and tastes of consumers in more refined ways, with more flexible pricing options.

Works will remain available in traditional formats as well as protected formats for a long, long time. And legal protections only cover TPMs applied to works protected by copyright or related rights.

### What kind of exceptions are appropriate to protection of TPMs?

The problem with allowing exceptions to protection of TPMs is similar to allowing someone to break the lock on a safe. Anyone then can get in, for any purpose.

Allowing hacking or circumvention devices weakens the overall robustness of the TPM encryption or other technology. Carried too far, this can make use of TPMs pointless

and investment in equipment and technologies worthless.

Governments therefore have recognised that any exceptions to TPM protection must be carefully limited. US law, for example, provides only a few exceptions, permitting circumvention only for such purposes as encryption testing under carefully limited conditions.

Allowing circumvention in any case where a traditional copyright exception applies is unworkable. Between private copying, educational use, 'fair use', and other typical exceptions, such a rule would effectively allow every citizen of a country to become a hacker.

Governments also have recognised that circumvention devices can do even greater harm than individual acts of circumvention. Exceptions to TPM protection generally have allowed only certain acts of circumvention, but not distribution of circumvention devices.

## SAMPLE IMPLEMENTING LEGISLATION

**IFPI Model Legislation (Option 1):** It shall be unlawful to circumvent any technological protection measure applied to a work or phonogram; or to manufacture, offer to the public, distribute or in any other way traffic in devices, components, services or other means designed, adapted or promoted to circumvent such a measure. The civil and criminal procedures, remedies and sanctions applicable to copyright infringement shall apply to any violation of this provision.

### IFPI Model Legislation (Option 2):

(a) It shall be unlawful to circumvent any technological measure that is applied to a work, phonogram or other protected material and that is designed to prevent or restrict, in the normal course of its operation, access to the material or acts that are not authorised by the rights owner. 'Circumvent' shall mean avoid, bypass, remove, deactivate or otherwise impair.

(b) It shall be unlawful to manufacture, import, distribute, sell, rent, possess for commercial purposes, offer to the public, advertise, communicate or otherwise provide any device, part, component, technology, service or other means that—

- (1) is primarily designed, produced, adapted or performed for the purpose of circumventing,
- (2) has only a limited other commercially significant purpose or use other than to circumvent, or
- (3) is marketed, promoted or advertised for the purpose of circumventing

any such technological measure.

(c) The civil and criminal procedures, remedies and sanctions applicable to copyright infringement shall apply to any violation of this section.

**Other example:** Lithuania Copyright Law, Art. 64(1)(4): The following acts shall constitute infringements of copyright: (4) removal of technological protective measures used by subjects of copyright and related rights for the exercise and protection of the rights provided for in this Law, as well as the manufacture, importation, transportation, keeping for the purpose of distribution and distribution of any technical devices or equipment specifically designed or adapted to circumvent those technological protective measures.

IFPI has represented the international recording industry since 1933. Its membership comprises more than 1,400 record producers and distributors in over 70 countries. For more information, please contact

IFPI  
54 Regent Street  
London, England, W1B 5RE  
Phone: +44 (0)20 7878 7900  
Fax: +44 (0)20 7878 7950  
E-mail: [info@ifpi.org](mailto:info@ifpi.org)  
Web site: [www.ifpi.org](http://www.ifpi.org)