TECHNOLOGICAL PROTECTION MEASURES

ISSUE

21(1)(a),21(1)(b)

BACKGROUND

Content producers use digital rights management tools to maintain control over their digital works. These tools include TPMs/digital locks, which prevent unauthorized access to or copying of works (e.g., encryptions placed on DVDs to prevent copying), and rights management information (RMI), which embeds copyright information in digital copies (e.g. watermarks).

To give additional force to such measures, the 1996 WIPO Internet treaties require that parties provide "adequate legal protection" to digital locks and "effective legal remedies" against their circumvention. The treaties also require adequate and effective legal remedies against the removal or alteration of RMI and the distribution of copies of works

21(1)(a),21(1)(b)

While the music industry appears to be moving away from using digital locks, the adoption of new legal protections for them remains a priority for other content industries.

Previous Reform Efforts

Bill C-61 (2008), proposed broad protections, covering circumvention acts, services and devices, with some specific carve outs as well as a regulation-making power that would have allowed the government to constrain the scope of the protections in very specific contexts. By contrast, its predecessor, Bill C-60 (2005), proposed more limited protections against circumvention acts and services (but not devices) where the intent is to infringe copyright.

International Benchmarks

The U.S. model is considered the 'highwater mark' for strong protections: it prohibits all acts of circumvention (access and copying) except for a very limited list of exceptions (although it provides rule-making power to vary the list of exceptions), and criminalizes the sale and distribution of circumvention tools and the offering of circumvention services. Examples of anti-competitive effects have been raised in the US courts and, as a result, the judiciary has read down the scope of TPM protection in relation to the availability of after-market goods or services. Also, several specific exceptions are set out as well as a rule-making power which provides some flexibility and corrective ability. The government has used it to further limit the protections (e.g., to ensure that consumers are not prevented from unlocking cell phones). All in all, the correlation

between this strong framework and reductions in levels of piracy and infringements in the US is unclear.

The Australian regime largely mirrors the USA's – a condition of the Free Trade Agreement the countries signed in 2006 – save that it avoids some of its potential anti-competitive effects by limiting TPM protections to situations of explicit copyright infringement.

The EU has also devised a protection regime that ensures that the anti-competitive effects witnessed in the US are avoided by not affording protection outside copyright infringement situations. To ensure that TPMs are not used to deprive users from the benefit of certain specific exceptions, it encourages voluntary agreements between stakeholders in respect to access to exceptions and allows for state intervention through judicial access orders where agreements have failed.

The UK regime is naturally very similar to the EU's. State intervention occurs as a matter of last resort with respect to users' rights, the preferred approach being voluntary agreements governing access to locked material.

New-Zealand appears as one of the least coercive regime among countries that have implemented TPM protections. There is no prohibition on possessing and using a circumvention device for non-infringing purposes. It is permitted to circumvent a TPM for a non-infringing purpose. The law provides for several mechanisms for ensuring that a work is available to users for non-infringing uses, including applying to the rights holder to provide assistance in circumventing a TPM or, failing that, engaging the assistance of a qualified person to do so. Access control TPMs are not protected (and consequently regional coding and other market lock-outs as well).

Consultation Results

Generally, rights holders (especially, the major film and software industry players) and key trading partners support strong protections for digital locks, which they argue is essential for maintaining the control over content needed to implement online business models. However, some rights holders have acknowledged that such a "control" model is not feasible, and prefer that public policy focus on remuneration models that would permit activities such as music copying (i.e., format shifting) and recording of TV programs (i.e., time-shifting) while providing compensation to creators for such uses.

Users typically object to the use of TPMs, which inhibit their ability to use legitimately-acquired content even for non-infringing purposes. If protections for TPMs are introduced they argue that they should be specifically more limited in scope and better targeted to the policy objectives.

CONSIDERATIONS

The protection of RMI is far less contentious than the protection of TPMs. As a result, the principal policy decision is to determine what protection needs to be provided against circumvention of TPMs.

Scope of TPM Protections

Although some rights holders claim that legal protections for digital locks are essential in order to roll out new business models in a secure manner, such protections could have various unintended effects. Limitations on the scope of protections for TPMs may be considered to address the following concerns in this regard:

Users' Rights vs. Copyright Owners' Interests:

The key consideration is respect of protection for TPMs is whether to prohibit circumvention only in the case of copyright infringement, or for any purpose whatsoever. The latter would allow copyright owners to effectively trump users' rights / exceptions in the Act. Copyright owners argue it is necessary for effective enforcement. Economic theory may be relied upon to assess the appropriate balance. For instance, it has been suggested that TPM protection may only be warranted where (i) it achieves providing rights holders with economic rent and (ii) it does not thwart technological innovation. Some economists argue that TPMs are essential to the efficient functioning of markets but some exceptions are required for the same market efficiency reasons (exceptions for interoperability, reverse engineering and security testing required; exceptions required when a TPM involves an increase of transaction costs).

Anti-competitive Lock-Out

Concerns have been raised regarding the potential use of TPMs for anti-competitive purposes. Specific examples include locking cell phones to prevent subscribers from switching service providers, limiting inter-operability of protected content with competing reading devices, and preventing competitors from developing competing after-market products (e.g. garage door openers). This concerns may however be adequately addressed by competition law.

Privacy & Security

Some digital locks have been designed to collect personal information about the user of the digital content, but without their consent. TPMs, such as BMG XCP (Sony's Rootkit), designed to monitor use of digital music files on the Sony BMG CDs without interference of the user, may also make the consumer's computer vulnerable to security problems such as virus infections. It is noteworthy that collection and use of personal data concerns may already be adequately addressed in various federal and provincial statutes, regulations and policies, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and *Telecom Regulatory Policy CRTC 2009-657.*

21(1)(b).23

OPTIONS

21(1)(a).21(1)(b)

21(1)(a),21(1)(b)

RECOMMENDATION

ANNEX A

Detailed discussion on potential competition issues associated with TPMs:

Commentators have stressed that TPMs can be designed to prevent users from using non-infringing competing products as alternatives to those provided by the TPM content developer or from using independent service vendors other than those affiliated with or licensed by the original TPM-encoded product or service. Consumers may suffer harm when TPMs are used to lock-out competing products and services. It has been argued that use of TPMs as lock-out devices significantly raises switching costs for consumers [e.g. locked cell phone not usable on another wireless service provider network], creates inefficiencies in the marketplace for such technologies, and puts consumers at risk of being stuck with inadequate or debilitating purchases.

The Canadian Competition Bureau has raised some specific concerns about digital locks:

- Limiting inter-operability such that only particular devices can function with the purchased product;
- Situations may arise where, in order to use a copy protected product, the consumer would also have to purchase a particular type of player or device, which might raise an instance of *tying* under the *Competition Act*;
- In addition, while the concept has not yet been employed by any Canadian courts, it is possible that TPMs that restrict access to, or use of, a legally-acquired copy of a work would be the basis for a "copyright misuse" claim.
- Lastly, to the extent that TPMs restrictions on the ability of a purchaser to access and use a legally acquired copy of a work are inconsistent with the advertised attributes of the work, this could form the basis for a misleading advertising charge pursuant to Section 52 of the *Competition Act*.

The Bureau also notes that, although the *Competition Act* does not expressly discuss the essential facilities doctrine in the context of IP rights, potentially relevant provisions of the statute include Section 75 that deals with refusal to deal, and Section 79 that is directed to the abuse of dominant position. The essential facilities doctrine compels a dominant or monopoly owner of a resource, access to which is considered "essential" for effective competition, to provide such access to competing firms.

In light of the foregoing, it can be suggested that anti-circumvention provisions in the *Copyright Act* would not prevent the application of the *Competition Act* and pro-competition doctrines.

By comparison, in the USA, the courts have had to deal with cases where TPMs were used to prevent competition in after markets. For instance, in the case of *Chamberlain Group Inc.* v. *Skylink Technologies Inc.* (the garage door opener case), the seventh circuit Court of appeal refused an interpretation of the US anti-circumvention provisions that would "allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products". It therefore rejected a construction of TPM protection provisions that would allow virtually any company to attempt to leverage its

sales into aftermarket monopolies, a practice that both the antitrust laws and the doctrine of copyright misuse normally prohibit. Essentially, the basis for these contentious issues stems from the scope of TPM protection which, in the US, primarily encompasses access control TPMs (vs. copy control TPMs).

Other examples of TPMs being used as lock-out mechanisms have arisen in the USA in the context of printers and printer ink cartridges, magnetic tape library storage systems, car repair diagnostic software (in Canada, refer to the Canadian Automotive Service Information Standard (CASIS) agreement signed by representatives of Canadian auto manufacturers and the aftermarket auto repair industry which restores full aftermarket access to original equipment manufacturer service and training information and service tools), online videogame servers and digital camera film files.

Detailed Legal Considerations

[Legal Opinions – We have asked for an update on the IC Legal opinion on TPMs]

Canadian law already provides suitable protections in some cases, although these would unlikely be sufficient to meet international standards. For instance, the RCMP has recently used anti-hacking provisions in the *Criminal Code* to prosecute a producer/distributor of circumvention devices used in video game consoles (i.e., "Mod chips").

TPMs may raise some concerns under the *Canadian Charter of rights and Freedoms*, especially with respect to the freedom of expression entailing the right to access information. For instance, provisions prohibiting the circumvention of DVD regional coding may violate the *Charter* where the user seeks to access information that is consistent with the rights (s)he may have purchased and where no copyright infringement occurs (N.B. Notwithstanding the potential constitutional invalidity of anti-circumvention provisions re. regional coding, the circumvention may nonetheless be unauthorized and therefore unlawful under applicable contractual terms).

Noteworthy DOJ Legal Opinions:

1) March 13, 2007, Theoretical constitutionality of anti-circumvention provisions of the US DMCA in Canada as a matter of vagueness (s. 7 *Charter*):

- Conclusion: language more likely to be constitutional than not

2) March 2, 2007, Assessment of the potential *Charter* risks of prohibiting the act of circumvention of access-control TPMs and the provision of services or sale of devices to circumvent any kind of TPM. Also, potential violation of the *Canadian Bill of Rights*:

- DOJ notes that some Canadian legislation does prohibit TPM circumvention in certain specific instances. Section 9(1)(c) of the *Radiocommunication Act* prohibits the unauthorized decoding of encrypted subscription programming signals and network feeds. Sections 341.1 and 342.2 of the *Criminal Code* prohibit, among other things, the fraudulent interception of a function of a computer system.
- DOJ's opinion overall suggests that legislation prohibiting anti-circumvention acts, devices and services would not be held unconstitutional (either they would

not breach the freedom of expression right or, if they did contravene, would be justified) where they are tied/linked to copyright infringement.
- Reserves: May be problem with *Charter* if no exception for the perceptually disabled or if too broad so as to capture publication of data (e.g., encryption research data) in an academic context.
- Low risk of successful challenge under 1(a) and 2(e) of the *Canadian Bill of Rights* (re.: property guarantees - this was raised in the context of access to a legitimately acquired copy being blocked by a regional code).

3) October 25, 2004, Assessment whether current exceptions allow Reverse Engineering, System Security Testing, Software Error Testing, and Interoperability, in a scenario where TMPs circumvention would be allowed in these cases.

- Unlikely 30.6 applies to reverse engineering or security testing, but may apply to inter-operability and error correction in some cases and under limited circumstances.
- Reverse engineering may be fair dealing for research or private study, depending on facts; not so clear with inter-operability, security testing, error correction, but possible.

4) March 30, 2004 WIPO Copyright Act
5) December 1, 2003 Privacy Liability
6) December 4, 2003 WIPO art. 11 & 18 (TPMs); December 5, 2003 (amend.)
7) November 6, 2003 WIPO Ratification
8) September 30, 2003 WIPO Treaties

Detailed Economic Arguments

- Marcel Boyer, "Assessing the Economic Impact of Copyright Reform on Authors, Makers, Photographers and Publishers in Canada in Reference to Two New Copyright-Related Treaties: WIPO Copyright Treaty (WCT), WIPO Performances and Phonograms Treaty (WPPT)", Prepared for Industry Canada (2003)

- Ruth Towse, "Assessing the Economic Impacts of Copyright Reform on Performers and Producers of Sound Recordings in Canada", Prepared for Industry Canada (2003)

- Abraham Hollander, "Assessing Economic Impacts of Copyright Reform on Selected users and Consumers", Prepared for Industry Canada (?)

TPMs

Towse:

- Considers that the economic rationale for TPMs protection is to be measured against the cost and trouble of legal proceedings, which could be a determining factor in the choice of policy option. In other words, the protection is worthwhile if, when in place, it provides economic rent to the rights holders.
- Relies on data suggesting that legal online music delivery services cannot compete against illegal P2P.

- Considers that at present, it is cheaper for the record industry to close down illegal sites than to compete (and existing law already enables closure). This makes it difficult to assess the strength of the incentive to develop online delivery that TPMs can provide to sound recording makers: it might be a nice weapon to have in the arsenal but how much will it be used? Also, a strong TPM regime might act as a disincentive to further technological development and business models. This is a cost benefit calculation that it is very hard to make for the future. Considers that there is no evidence that TPMs will restore the value of sales at present being lost to piracy and downloading since there is no clear explanation for the fall in CD sales.

Boyer:

- Argues that the roles of TPM and RMI are essential to the efficient functioning of markets because (1) they allow the proper protection of copyrights and (2) they make sure that proper information is available at low cost to prospective buyers.
- Argues that TPMs should not affect market efficiency by increasing transaction costs. As a result, private copying and its levies, a response to transaction costs should not be disturbed by TPMS. Circumvention for private copying and other exceptions should therefore be allowed. Also suggests that an exception from liability should apply in respect of bona fide activities that affect TPMs, which are carried out for the purposes of ensuring interoperability, reverse engineering and security testing.
- Suggests that the preferred remedy option appears to be civil sanctions with the possibility of criminal sanctions for large-scale infringement or infringement done for commercial purposes. Too heavy sanctions may trigger inhibition of consumers in the market or prevent innovation.

Rights Management Information

Hollander:

- Suggests that museums, libraries and archives would likely suffer some adverse effects from measures designed to protect rights management information.
- However, these effects are not sufficiently important to justify a grant of broad exemptions from anti-tampering rules to these institutions.
- Suggests that rights holders should be entitled to injunctions and damages when the RMI embedded in their copyrighted works is tampered with.

Towse:

- Considers that the expected direct economic effects of Digital Rights Management (DRM) are the reduction of transaction costs of rights management and the gain of revenues from licensing fees and other remuneration for collecting societies.
- Refers to wider concerns about the indirect effects that DRM may cause. In law and economics terms, there is a concern about limitation of access to copyright material for 'fair use' (or 'fair dealing' in the UK, Australia, and Canada) by consumers and other users, including creators.

- Suggests that much depends upon the economic interpretation of fair use. The 'classic' article on this by Gordon on the *Betamax Case* argued that fair use is a response to market failure, by which she meant the difficulty of a market spontaneously developing when there are numerous consumers with a very low willingness to pay but where their combined consumption would be valuable and cause considerable losses to the supplier. Other economists have argued that fair use is giving way to 'fared use' with DRM that overcomes market failure in the Gordon sense and facilitates the capture of the whole consumers' surplus by price discrimination and so erodes fair use.
- Refers to the distinction between 'productive' and 'reproductive' fair use, the former being necessary for the creation of new works. Refers to the arguments developed in the literature, viz. that over-strong copyright protection limits productive fair use and raises the cost of creation (transaction costs of checking on what is copyright material, tracing owners for permissions, etc.) and reduces freedom of expression and free speech. Excessive reproductive fair use, however, reduces the value of copyrights and blunts the incentive to create. The balance is maintained in copyright law allowing fair use that does not significantly reduce the value of the copyright and by the limited duration of copyright (and this balance is upset by extension of the duration). Argues that although this analysis predates discussions about DRM technology, the general principle is surely still applicable - These concerns were raised by objectors to the U.S. DMCA Anti-Circumvention provisions.
- Underscores that it can be seen from this discussion, that this is a vast topic that involves the whole of copyright law and its cultural and economic rationale: It would be manifestly difficult to place economic value on fundamentals such as creativity, freedom of expression, freedom of speech, respect for the law and suchlike; There are also public choice issues here of representation for many small gainers versus a few powerful and well organized interest groups; These are questions governments have to resolve on political as well as economic grounds.

Detailed International Comparisons

U.S.A.: The USA provide protection against circumvention of technological measures used by rights holders to protect their work. The provisions divide TPM into two categories: measures that prevent unauthorized *access* to a copyrighted work and measures that prevent unauthorized *copying* of a copyrighted work. Making or selling devices or services that are used to circumvent either category of TPM is prohibited if (i) they are primarily designed or produced to circumvent; (ii) they have only limited commercially significant purpose or use other than to circumvent; or (iii) they are marketed for use in circumventing. As to the act of circumvention in itself, the provision prohibits circumventing access control TPMs but not copy control TPMs. This was meant to allow to make fair use of a copyrighted work, knowing that fair use is not a defence to the act of gaining unauthorized access to such a copyrighted work. These liabilities are subject to a number of exceptions such as reverse engineering, encryption research, protection of minors, personal privacy, security testing. The government is also provided with a rule-making power to exempt classes of copyright users who are adversely affected by these provisions in their ability to make non infringing uses. The U.S. model is considered the 'highwater mark' for strong protections. Examples of anti-competitive effects have been raised in the courts in the U.S., and, as a result, courts have read

down the scope of protection in relation to the availability of after-market goods or services. Also, the rule-making power has been used to further limit the protections (e.g., to ensure that consumers are not prevented from unlocking cell phones). Several other countries, notably Australia, have been mindful of these 'lessons learned' when implementing their own digital lock protections.

E.U.: Directive 2001/29/EC transposes into Community law the main international obligations arising from the two 1996 WIPO treaties and requires member states to provide for adequate legal protection against acts of circumvention (with actual or deemed knowledge) of "effective technological measures" and against dealings in circumvention devices & services. It is noteworthy that the definition of "technological measures" is such that it only requires member states to protect TPMs in relation to copyrighted works or subject-matters and to sui generic rights in database. The definition seeks to link TPM protection to the exercise of copyright. TPMs applied to protect non copyrightable subject matter or works in the public domain are therefore not protected under the Directive. "Effective technological measures" refer to (i) access and (ii) copy control applications or mechanisms. Further, despite the reference to "access control" in the definition of "effective TM", this cannot be relied upon to widen the scope of the exclusive rights such as to include an exclusive access right (where no infringement occurs). As a result, TPMs used to control after-markets in spare parts of hardware goods (e.g. garage door openers, ink cartridges) are not protected under the Directive. Similarly, TPMs used for the sole purpose of segmenting geographical markets (e.g. regional coding) are not protected. The Directive also provides for the obligation to ensure, in the absence of voluntary agreements between right holders and users, that right holders make available to the beneficiary of certain specific exceptions and limitations the means of benefiting from these exceptions or limitations. It also allows a member state to permit circumvention for private copying unless it has already been made possible by right holders and to the extent it does not affect their ability to limit the number of private copies (N.B. the general view is that the Directive does not provide a right to private copying). The Directive does not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in Directive 91/250/EEC.

U.K.: The UK implementation provisions closely resemble the Directive provisions. There are accordingly separate anti-circumvention provisions for computer programs vs. other works. Regarding the ability for users to benefit from exceptions and limitations, the UK approach is based on voluntary measures and agreements between users and rights holders on the lifting of the anti-circumvention measures. Beneficiaries do not have an immediate actionable right and no positive obligation of the person applying TPMs subsists. Instead, a complaint procedure administered by the State is set up whereby the right holder is subject to an actionable right when he breaches a state order, previously and when granted, to make available the means necessary to carry out the permitted acts.

Australia: Amendments were first introduced in 2001 in order to comply with the main international obligations arising from the two 1996 WIPO treaties, including TPM protection. Essentially, the provisions only applied to dealings in devices and not to the act of circumvention. It appears that the Australian regime did not mirror the US DMCA and did not adopt the wider ambit it affords as a result of granting protection to access control, without the necessary linkage to copyright infringement (see *Stevens v Kabushiki Kaisha Sony Computer Entertainment* [2005] HCA 58, where it was

emphasized, for instance, that control over access to copyrighted works or materials would permit the achievement of economic ends additional to, but different from, those ordinarily protected by copyright law and would give right holders broader powers over pricing of their products in their self-designated markets than the Copyright Act in Australia would ordinarily allow).

The Government modified the TPM scheme to implement the Australia-United States Free Trade Agreement (AUSFTA) through legislation that came into force in Dec. 2006. Essentially, the new scheme provides for protection against circumvention of TPMs and against dealings in circumvention devices & services. Liability for the act of circumvention is limited to the circumvention of access control TPMs (vs. copy control TPMs).

The scope of the scheme has been limited to preventing circumvention of TPMs designed to stop copyright piracy and TPMs must therefore be linked to copyright infringement to afford protection. The scheme will not cover TPMs which are not designed to prevent or inhibit people from infringing copyright. The scheme will not apply to TPMs solely designed for other purposes, such as market segmentation (e.g. DVD regional coding) or the lock-out of competition in aftermarket goods (e.g. spare parts) where the TPM does not have a connection with copyright.

The new scheme introduces civil remedies and criminal penalties where a person circumvents an access control TPM. It also builds on the existing scheme which already provides criminal penalties for dealing in circumvention devices and services. To discourage the dealing in these devices, the provisions provide criminal penalties of five years imprisonment and/or fines of 550 penalty units (currently $60,500).

The AUSFTA sets out specific exceptions to TPM liability, namely:

- Interoperability between computer programs,
- Encryption research,
- Computer security testing,
- Online privacy,
- Law enforcement and national security, and
- Acquisitions by libraries and other related institutions.

Like the US, the scheme has a mechanism, via general regulation-making power, for creating additional exceptions. Outside the foregoing list of exceptions, unless it is provided in the regulations, no circumvention is allowed for the purpose of benefiting from the other exceptions to copyright infringement in the Copyright Act.

New Zealand: Provides protections that are significantly weaker than the U.S. model. Access control TPMs are not protected (and consequently regional coding and other market lock-outs as well). Further, there is no prohibition on possessing and using a circumvention device. The offering of circumvention services and devices that will be used to circumvent a TPM only in order to infringe copyright is prohibited. The law provides for a limited criminal offence provision that will apply where there has been large-scale commercial dealing in devices, means and information enabling people to circumvent copyright. It is noteworthy that it is permitted to circumvent a TPM for a non-infringing purpose (i.e. a permitted act) and that the law provides for several

mechanisms for ensuring that a work is available to users for non-infringing uses, including applying to the rights holder to provide assistance in circumventing a TPM or, failing that, engaging the assistance of a qualified person to do so.