Technical Protection Measures: *Tilting* at Copyright's Windmill

DR. IAN R. KERR,* ALANA MAURUSHAT**
AND CHRISTIAN S. TACIT***

Canada's imminent decision whether to ratify the WIPO Copyright Treaty *(WCT) and the* WIPO Performances and Phonograms Treaty *(WPPT) raises questions about the extent to which Canadian law ought to protect the technologies that protect works subject to copyright in a digital environment. In addressing this question, the authors commence with a detailed description of the current state of the art in technological protection measures (TPMs). The authors demonstrate that an attempt to provide a simple description of TPMs has been complicated by the introduction of more sophisticated information systems designed to protect intellectual property, known as digital rights management systems (DRMs).*

Following their technological description of TPMs and DRMs, the authors analyze the TPM concept and investigate the legal implications of Canada's commitment as a signatory of the WCT and WPPT to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures. After situating their analysis in a broader philosophical context, the authors consider the consequences of affording an additional layer of protection over and above the existing protections offered by copyright law, contract law and

La décision imminente du Canada concernant la ratification du Traité de l'OMPI sur le droit d'auteur *et du* Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes *soulève des questions quant à l'étendue de la protection en droit canadien des technologies visant à protéger les œuvres qui font l'objet d'un droit d'auteur dans un environnement numérisé. Les auteurs font d'abord une description de l'état actuel des mesures de protection technologique. Ils démontrent qu'il n'est pas facile d'arriver à une description simple, étant donné l'introduction de systèmes d'information complexes conçus pour la protection de la propriété intellectuelle, dits systèmes de gestion des droits d'auteur électroniques.*

Après cette description des mesures de protection et des systèmes de gestion des droits d'auteur électroniques, les auteurs analysent la notion de protection électronique. Ils explorent les répercussions juridiques pour le Canada en tant que signataire des traités précités de l'OMPI sur le plan de l'engagement à assurer une protection adéquate et des recours juridiques efficaces en cas de contournement des mesures technologiques en vigueur. Transposant leur analyse dans le contexte philosophique plus large, les auteurs s'interrogent sur le bien-fondé de l'ajout

* Dr. Ian Kerr, Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa; Special Counsel, Technology Law, Nelligan O'Brien Payne LLP

** Alana Maurushat, Assistant Lecturer, Faculty of Law, University of Hong Kong; L.L.M. (with Concentration in Law & Technology), Faculty of Law, University of Ottawa; Former Student Intern at Nelligan O'Brien Payne LLP

*** Christian S. Tacit, Partner with Nelligan, O'Brien Payne LLP and Technology Law Practice Group Leader

This article is based on two studies funded by Canadian Heritage. The authors wish to thank Bruce Stockfish for his support. The authors are also indebted to Loris Mirella for his invaluable comments and suggestions. Thanks also to Andrew Huzar, Steven Pink, Tracey Ross, Shannon Ross, Christopher Rootham, Erin Smith, and Wing Yan for their contributions to an earlier draft. Finally, thanks to the Centre for Innovation Law and Policy for providing the support necessary to adapt the original Heritage studies into the current law review article.

the technologies themselves. They then examine various possible implementations of the WIPO treaties as well as legislative responses from Australia, Japan, the European Union, with particular emphasis on the United States and the cases and commentary that it has produced.

The authors conclude that, until the market for digital content and the norms surrounding the use and circumvention of TPMs become better known, it is premature to ascertain the appropriate legal response. Consequently, they suggest that Canada should not implement any new legal measures to protect TPMs at this time. Recognizing the possibility that such measures might need to be adopted in the face of new empirical evidence, the authors recommend that the legislative creation of access-control right must be counter-balanced by a newly introduced access-to-a-work right. Under this approach, copyright owners would have a positive obligation to provide access-to-a-work when persons or institutions fall within the exceptions or limitations that would be set out in the Copyright Act. *Such an obligation might entail the positive obligation to allow access to works in the public domain, or to provide unfettered access-to-works to educational institutions and other organizations that are currently exempted from a number of the provisions in the* Copyright Act. *Finally, the authors end by pointing out that the approach to the TPM issue has thus far neglected a question that is* logically prior *to those raised by the current debate about anti-circumvention laws. They point out that, before asking whether and under what circumstances copyright legislation ought to protect TPMs, perhaps it is necessary to first ask whether and under what circumstances TPMs should be permitted to flourish.*

d'un nouveau palier de protection aux mesures déjà prévues par la loi sur le droit d'auteur, le droit des contrats et les technologies elles-mêmes. Ils examinent diverses mises en œuvre possibles des traités de l'OMPI, y compris les solutions législatives de l'Australie, du Japon, de l'Union européenne et en particulier des États-Unis, ainsi que la jurisprudence et les études en résultant.

Les auteurs concluent que tant que le marché de contenu numérisé et les normes régissant l'usage de mesures de protection technologique et leur contournement ne sont pas mieux connus, il est trop tôt pour dire quelle est la solution juridique appropriée. Par conséquent, ils suggèrent que le Canada ne devrait pas, à ce moment-ci, mettre en œuvre de nouvelles mesures législatives pour la protection technologique. Reconnaissant que les recherches empiriques futures pourraient démontrer la nécessité de telles mesures, les auteurs recommandent, lors de la création de lois régissant les droits d'accès et de contrôle, de viser un équilibre avec le tout nouveau droit d'accès au travail. De cette façon, les propriétaires du droit d'auteur auraient une obligation d'assurer un accès au travail aux personnes et aux établissements qui font l'objet des exceptions et des limitations prévues dans la Loi sur le droit d'auteur. *Cette obligation pourrait inclure l'obligation d'autoriser l'accès aux œuvres du domaine public ou l'accès au travail sans entraves aux établissements d'enseignement et autres organismes déjà exemptés de l'application de plusieurs dispositions de la* Loi sur le droit d'auteur. *Enfin, les auteurs notent l'omission de prendre en considération dans le traitement actuel des mesures de protection électronique une question qui devrait* logiquement *avoir* priorité *sur le débat actuel concernant les lois interdisant le contournement de telles mesures. Selon eux, avant de se demander si la loi sur le droit d'auteur doit protéger les mesures de protection électronique et dans quelles circonstances, il serait peut-être bon de se demander d'abord s'il faut permettre le développement de mesures de protection technologique et si oui, dans quelles circonstances.*

Table of Contents

11 I. Introduction

13 II. Technological Protection Measures
13 A. Introduction
13 B. Access Control Technology Protection Measures
15 1) Access TPM Devices and Players
17 2) Content Scramble System (CSS)
19 3) Asymmetric Application Segmentation (AAS)
19 4) Digital Tickets
19 C. Use Control (Copy Control) TPMs
20 1) Macrovision
20 2) Serial Copy Management Systems (SCMS)
21 3) Digital Transmission Content Protection (DTCP)
22 4) Secure Digital Music Initiative (SDMI)

23 III. Circumvention

25 IV. Digital Rights Management (DRM) Systems
25 A. The DRM Concept
26 1) DRMs That Do Not Utilize TPMs
26 2) TPM-Enabled DRMs
26 (i) Digital Object Identifier
27 (ii) Extensible Rights Mark-Up Language (XrML)
28 B. The Policy Implications of DRMs

29 V. The Future of TPMs and DRMs

31 VI. The Legal Concept of TPMs
31 A. Introduction
32 B. The TPM Concept in the *WCT* and *WPPT*
34 1) Effective
35 2) Used by Authors to Exercise Copyright
36 3) Unauthorized Acts Permitted by Law
36 C. Classes of Legal Protection

37 VII. Philosophical Considerations

42 VIII. Affording Legal Protection to TPMs
43 A. Existing Layers of Protection for Copyright Holders
43 1) TPM and DRM Technologies
43 2) Copyright Law
44 3) Contract Law
45 B. Two Possible Responses

46 IX. Possible Implementations of the WIPO Treaties
47 A. General Access Control Measures
50 B. Limited Access Control Measures
51 C. Use Control Measures
53 D. Anti-Device Measures
55 E. Effective Remedies

58 X. Legislative Responses in Other Jurisdictions
58 A. Australia
59 B. Japan
61 C. The European Union
64 D. The United States
64 1) Access Control Measures
64 (i) Basic Ban
65 (ii) Circumvention of Access Control TPMs
65 (iii) "Effective" Access TPM
65 (iv) Prohibition of Access Control Circumvention Devices
66 2) Copyright Control Measures
66 (i) Circumvention of Copy Control TPMs
67 (ii) "Effective" Use Control TPMs
67 (iii) Prohibition of Use Control Circumvention Devices
68 3) Exemptions
68 4) Some Effects of the *Digital Millennium Copyright Act*
69 (i) *US v. Sklyarov*
69 (ii) Felten
70 (iii) Ferguson
71 (iv) *RealNetworks v. Streambox*
71 (v) *Universal City Studios v. Reimerdes*
73 (vi) Church of Scientology Cases
75 5) Academic Reactions to the *Digital Millennium Copyright Act*

76 XI. Concluding Remarks

Technical Protection Measures: *Tilting* at Copyright's Windmill

DR. IAN R. KERR, ALANA MAURUSHAT
AND CHRISTIAN S. TACIT

> "Fortune," said Don Quixote to his squire, as soon as he had seen them, "is arranging matters for us better than we could have hoped. Look there, friend Sancho Panza, where thirty or more monstrous giants rise up, all of whom I mean to engage in battle and slay, and with whose spoils we shall begin to make our fortunes. For this is righteous warfare, and it is God's good service to sweep so evil a breed from off the face of the earth."
>
> *–Miguel de Cervantes, 1605*

I. Introduction

THOUGH IT IS PERHAPS DIFFICULT to conceive of today, three decades ago, advancements in photocopying technologies were seen as a serious threat to copyright industries and even to the law of copyright itself.[1] Reacting to this technological threat, the World Intellectual Property Organization (WIPO) convened a copyright committee to examine the extent of the danger as well as some possible legal responses. Some 25 years later, yet another copyright committee was convened at WIPO to discuss the most current technological threat to copyright law—digital technologies.[2] The result of the latter committee's discussions led to the formation of the *WIPO Copyright Treaty*[3] and *WIPO Performances and Phonograms Treaty*,[4] both of which aim to supplement existing copyright law with further protections in light of the potential harm caused by digital technologies. Although it is a signatory to these two treaties, Canada is now considering whether or not to ratify them, and if so, how such measures should be adopted under domestic law.

The proliferation in our ability to copy and disseminate information through electronic means has been driven by inexpensive and powerful personal

---

1. See generally Paul Goldstein, *Copyright's Highway: The Law and Lore of Copyright from Gutenberg to the Celestial Jukebox* (New York: Hill & Wang, 1994).
2. See Herman Cohen Jehoram, "The Future of Copyright Collecting Societies" [2001] 23 Eur. I.P. Rev. 134.
3. *WIPO Copyright Treaty*, 20 December 1996, 36 I.L.M. 65 (entered into force 2 March 2002) [*WCT*], online: World Intellectual Copyright Organization <http://www.wipo.int/clea/docs/en/wo/wo033en.htm>.
4. *WIPO Performances and Phonograms Treaty*, 20 December 1996, 36 I.L.M. 76 (entered into force 20 May 2002) [*WPPT*], online: WIPO Performances and Phonograms Treaty <http://www.wipo.int/clea/docs/en/wo/wo034en.htm>. The *WCT* and *WPPT* will hereinafter be referred in combination as the WIPO Treaties.

computing equipment, coupled with widespread access to network technologies. As a result, it is possible to encode various kinds of information into digital form, duplicate the digital content without loss of fidelity, and transmit it to incredible numbers of recipients worldwide at negligible incremental cost. This new environment provides many new opportunities for the rapid and inexpensive dissemination of digital content. It also poses special challenges for the enforcement of both intellectual property rights (such as copyright) and other rights (such as contractual rights) in various kinds of digitized works. As a result, rights owners in digital content are increasingly turning to the use of technological protection measures (TPMs) to enforce and protect their rights and to aid in the dissemination of their works. Because the protection that these technologies provide may be circumvented through the use of other technologies, rights holders have advocated that the circumvention of such TPMs should be protected with the force of law.

The objective of this article is to examine a range of policy considerations associated with the use of technological protection measures (TPMs) as a means of extending copyright in digital environments. We will also investigate various policy choices implicated in the decision to provide legal protection to TPMs in the context of Canadian copyright law.[5] In order to achieve this objective we aim to furnish a clearer understanding of what TPMs are, how they are used, and what their circumvention might entail. This will be accomplished through technological descriptions of various TPMs and digital rights management systems (DRMs).

Following this introduction, our analysis in Part II investigates some recent trends in the development of TPMs. In Part III, we discuss the possibility of their circumvention. The subject matter of this investigation is then magnified in Part IV through an examination of full-scale DRMs.[6] In Part V, we briefly contemplate the future of TPMs in order to situate our broader policy analysis of the use and legal protection of TPMs in the context of the question whether, and if so, how Canada might choose to implement the WIPO Treaties. Part VI provides a conceptual analysis of the basic elements stipulated in the WIPO Treaties with respect to the legal protection of TPMs. The analysis will include an enumeration of possible interpretations of the conditions for compliance set out in the relevant *WCT* and *WPPT* provisions. In Part VII, we offer some key philosophical considerations underlying Canadian copyright law. Part VIII is an examination of existing methods of protecting unauthorized use to copyright works. In Part IX, we examine in detail four classes of legal measures that might be implemented pursuant to *WCT* and *WPPT* to protect TPMs. The advantages and disadvantages of each are explored, with particular emphasis on their potential effects and interaction with copyright law. Part X provides a critical analysis of the implementation of legal measures to protect TPMs in various countries. Finally, Part XI offers a number of concluding remarks.

---

5. The reference to Canadian copyright law is somewhat misleading as the WIPO Treaties do not require legal protection of TPMs to be addressed by copyright law specifically.
6. Digital rights management systems are also referred to as electronic rights management systems (ERMS), rights management information systems (RMIs) and copyright management systems (CMS).

II. Technological Protection Measures

A. INTRODUCTION

In its simplest form, a TPM is a technological method intended to promote the authorized use of digital works. This is accomplished by controlling access to such works or various uses of such works, including copying, distribution, performance and display.[7] TPMs can operate as safeguards or 'virtual fences' around digitized content, whether or not the content enjoys copyright protection.[8] Two common examples of TPMs are passwords and cryptography technologies.

We describe a number of TPMs that control access to works and other TPMs that control the use of works. It is not our aim to provide a comprehensive overview of TPMs—such a task would be overwhelming due to the speedy evolution of technology. Rather, our aim is to provide sufficient technological detail to allow for a more robust understanding of "*effective technological measures*" and other key terminology set out in WIPO's *WCT* and *WPPT*.[9] Consequently, the descriptions of these technologies are not set out in a way that would satisfy the intellectual curiosity of the technicians who create and use them. The threshold here is much lower. Our aim is merely to provide descriptions of the technologies that are sufficient to inform a meaningful policy debate about the requirements for compliance with the *WCT* and *WPPT*.

TPMs are often classified by their function. A commonly used distinction is often drawn between TPMs that control *access* to works and those that control the *use* of works.[10] However, as indicated below, TPMs often display both sorts of characteristics. This creates difficulties for legislators who may only want to confer anti-circumvention protection to one class of TPMs but not to the other. It also makes the classification of access control and use control TPMs rather imperfect, as the ensuing discussion demonstrates.

B. ACCESS CONTROL TECHNOLOGY PROTECTION MEASURES

This first category of TPMs is used to prevent unauthorized persons from *gaining access* to digital works. It is the equivalent of a virtual lock on such works. A num-

---

7. M. Perry and C. Chisick, "Copyright and Anti-circumvention: Growing Pains in a Digital Millennium," (2000) New Zealand Intellectual Property Journal 261.
8. Authors, including E. Mackaay, have used the metaphor of the digital fence to illustrate how intangible property may be protected. Fencing techniques such as TPMs or contractual arrangements allow rightsholders the ability to control access to and, in some circumstances, the use of their works. Such metaphors build on the notion articulated by Robert Ellickson who discussed how the invention of barbed wire allowed smaller lots to be used for breeding cattle, thereby changing the economics of such land use. See E. Mackaay, "Intellectual Property and the Internet: The Share of Sharing" in Neil Netanel & Niva Elkin-Koren, eds., *The Commodification of Information* (The Hague: Kluwer Law International, 2002); Robert C. Ellickson, "Property in Land" (1993) 102 Yale L. J. 1315 at 1330.
9. *Supra* notes 3 and 4. As will be discussed in greater detail in Part VI, both WIPO treaties require that, "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of *effective technological measures...*" [emphasis added].
10. Kamiel J. Koelman & Natali Helberger, "Protection of Technological Measures" in P. Bernt Hugenholtz, ed., *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (The Hague: Kluwer Law International, 2000) at 165 [Hugenholtz, *Copyright Management*]. See also Jeffrey P. Cunard, "Technological Protection of Copyrighted Works and Copyright Management Systems: A Brief Survey of the Landscape" (Paper presented to the ALAI Congress, June 2001) [unpublished], online: ALAI 2001 Congress Program and Presentation <http://www.law.columbia.edu/conferences/2001/program_en.htm>.

ber of different methods can be used to identify whether a particular person is authorized. The two most common methods are passwords and cryptography.[11]

Cryptography is the science of encryption and decryption. Julius Caesar popularized the practice. Not trusting his messengers when communicating with his governors and officers, he encrypted his messages.[12] Encryption is the coding of plaintext into an unreadable form called ciphertext so that it cannot be understood by those who are not privy to the code. Caesar created a rather simple system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. Authorized recipients of his messages were provided with the means of decrypting them. Decryption is the process of converting ciphertext back into its original form so that it can be understood and acted upon.[13] Cryptography allows the communication of information in a manner that is disguised so as to keep its content hidden from unintended or unauthorized recipients.[14]

Caesar's system was premised on the creation and sharing of a private code, nowadays referred to as a private key (made up of characters or numbers).[15] Private key cryptography, also known as symmetric cryptography, uses the same key for both the encryption and decryption processes.[16] The following is an explanation of how symmetric encryption works:

> The encrypted messages and the keys are sent separately to the intended recipient. If this were simply a case of two friends wanting to share secret information, it would be easy. Person A encrypts the message and sends the encrypted message and the key separately to Person B. Person B is then able to decrypt the message [using the key]. If the key is left in clear format (decrypted) it could potentially be captured during transmission and readily used to decrypt the message leading to a compromise of security.[17]

For this reason public key (or asymmetric) cryptography is often the preferred approach. In public key cryptography, a twin pair of keys is created: one key is private, the other public. Their fundamental property is that, although one key cannot be derived from the other, a message encrypted by one key can only be decrypted by the other key. Because two keys are required—one to encrypt, the other to decrypt—no one has to share her private key with anyone. In fact, it is essential that the private key be kept secret and remain in the custody of the per-

---

11. Jacques de Werra, "The Legal System of Technological Protection Measures under the WIPO Treaties, the *Digital Millennium Copyright Act*, the European Union Directives and other National Laws (Japan, Australia)" (Paper presented to the ALAI Congress, June 2001) [unpublished], online: ALAI 2001 Congress Program and Presentation <http://www.law.columbia.edu/conferences/2001/program_en.htm>.
12. Mitchell McInnes *et al.*, *Managing The Law: The Legal Aspects of Doing Business* (Toronto: Pearson Education Canada, 2003) at 382.
13. *Ibid.*
14. C. Risher, "Technological Protection Measures (Anti-Circumvention Devices) and their Relation to Exceptions to Copyright in the Electronic Environment" (Paper presented to the IPA Copyright Forum Frankfurt Book Fair, 20 October 2000) [unpublished]. See also Network Associates, Inc. and its Affiliated Companies, *Introduction to Cryptography*, online: The International PGP Home Page <http://www.pgpi.org/doc/pgpintro>.
15. McInnes, *supra* note 12.
16. Lech Janczewski, *Internet and Intranet Security Management: Risks and Solutions* (Hershey, PA: Idea Group, 2000) at 149.
17. Risher, *supra* note 14 at 2.

son to whom it belongs. The public key, on the other hand, is only useful if it is possessed by as many people as possible. Only by making the public key readily available is it possible to enable others to send encrypted data. Although not necessary, the keys are often interchangeable. In other words, "if key A encrypts a message, then key B can decrypt it, and if key B encrypts a message, then key A can decrypt it."[18]

A similar procedure is used to create electronic/digital signatures, which can be used to authenticate the identity of an individual in order to determine whether he or she is authorized to gain access to a digital work. A simple electronic signature is the ciphertext resulting from encrypting a message. This electronic signing process is one way to fulfill the functional equivalence requirement for electronic signatures in most Canadian electronic commerce legislation. If one person signs his message and sends it to another along with an appended electronic signature, she can decrypt the appended electronic signature with his public key and compare it to the message. If they are identical, and assuming that the public key that was used to decrypt the signature really is his public key, she can reasonably infer that the message was in fact from him since it must have been signed with his private key.[19] Thus, decrypting an electronic signature using a public key is one way to verify an electronic signature.

Another form of authentication similar to a digital signature is a digital certificate. Digital certificates act as a form of identification for users in the digital world and are distributed by trusted third parties known as Certification Authorities (CAs). A digital certificate contains the version number of the certificate, the serial number of the user, the algorithm used to sign the certificate, the CA that issued the certificate, the expiration date of the certificate, the user's name, the user's public key and the user's digital signature.[20] Certificates play an important role in security, since system administrators can configure servers to accept only certificates signed by certain CAs. To further enhance security on the Internet, protocols have been developed that handle only the encryption and decryption of data. One such example is the secure socket layer (SSL) protocol: "SSL provides an entire channel of communication between two systems that is devoted solely to the exchange of encrypted data ... [and] can be used as an underlying tool for other [web] application protocols such as HTTP, SMTP, TELNET, FTP, etc."[21]

1) Access TPM Devices and Players

Using cryptography as a model, a number of methods have been developed to link encrypted files to devices or players comprised of hardware and/or software so that an encrypted message can only be decrypted using that particular device or player.[22]

---

18. *Ibid.*
19. A more sophisticated technique involves first making a "hash," or compressed version of the message, from which the message cannot be derived, and encrypting the hash. See Richard E. Smith, *Internet Cryptography* (Reading, MA: Addison Wesley, 1997) at 280.
20. Janczewski, *supra* note 16 at 12. The author analogizes digital certificates with a driver's license or a passport.
21. *Ibid.*
22. Risher, *supra* note 14 at 2.

Risher describes a number of different methods:[23]

· *Sealed content:* The content is encrypted and can only be opened when a unique and authentic token is present in the device. The token itself cannot be replicated. Therefore, the content cannot be decrypted on another machine since the other machine would not have the same token. However, in some early systems, once the content is opened with the aid of the token, the content would be available in an unprotected manner thereafter and could be copied and distributed.

· *Device Binding:* Computer central processing units (CPUs), hard drives and network interface cards (NICs) have unique identifiers (IDs). This method takes advantage of this characteristic by linking the decryption key to one of these unique IDs in a computer from where the content purchase is made. Therefore, the device in the computer that decrypts and reads the content (the "reader") uses one of these device IDs to obtain the decryption key required to decrypt the content so it can be read but it is only decrypted while being used on that specific device. Therefore, if a file is subsequently distributed to another computer, it cannot be "read" on that computer.

· *Trusted player:* Some e-book reader systems look for the key embedded with the content. The reader will only enable the content to be viewed if the key is present. The key is unique to a particular make and version of reader.

· *Trust-enabled player:* In this scenario a player that can read unencrypted content works in conjunction with a plug-in (*i.e.*, software downloaded to the system and recognized by the reader) that controls access to the content when the reader is used. The plug-in takes over control of the reader during the reading process. Thus, for example, the plug-in may not allow certain content viewed with the reader to be printed or saved to a file.

· *Trusted device (closed environment):* A player belonging to this category is designed to play certain types of content but no software can be run on the devices. Certain types of readers for e-book content belong to this class. The content is encrypted and the decryption key only works in the closed environment of the reader itself. Therefore, there is no opportunity for other software to find the key and the reader is limited to the uses for which it was provided.

· *Trusted device (detection):* In the case of audio and video content, an additional measure is employed to secure content in addition to encryption. The content, in order to be identified as authorized, must include a certain mask or code that must be detected by the playback device before the device will play it.

· *Online access controls:* Streaming content is used for the display of live or real-time performances of music and video. The digital content is decrypted for a short time while it is delivered to the player and then it is re-encrypted to prevent copying. Some variations only allow 10–20% of the content to be decrypted as it is made audible or visible. This technology works because these kinds of content files are very large and any copying can only be done slowly in the brief moments while the content is perceptible by human senses.

· *Multiple-key high security:* In some systems, decryption is done on a page-by-page basis. Each page uses a separate key transmitted with the content for that page and as soon as the page is viewed, the key used to decrypt that page is

23. *Ibid.* at 2-4.

destroyed. This system requires an online connection when the content is being viewed.

Prior to concluding the discussion on access control TPMs that employ encryption, two critical observations are in order. First, some of the TPMs described above control not only access to a work, but also the subsequent use of that work. For example, a trust-enabled player controls not only access to content through encryption, but can also be used to determine whether or not that content, once legitimately decrypted can be copied, stored or printed by the user. This illustrates that the classification scheme set out above is overly simplified: often, the distinction between the access control or use control functions is illusory.

Second, TPMs—especially access control TPMs—can create problems for legitimate users of a work. Consider, for example, a consumer who has purchased online access to content that is secured using device binding. Recall that device binding is device specific—a file will be accessible on a specific device (*e.g.* a particular notebook computer) but will be inaccessible using a different device (*e.g.* another computer). The first problem that the user will encounter is that it will not be possible to access the content from the other computer. In addition, if the hard drive bearing the ID used for device binding fails and is replaced by another hard drive, as is often the case with notebook computers, the consumer will lose all access to the content despite being a legitimate user.

2) Content Scramble System (CSS)

CSS is well known as a TPM designed to protect movies released in the Digital Versatile Disk (DVD) format. CSS has the following characteristics:

1) The contents of the disk are encrypted;

2) The keys that enable a DVD player or DVD-ROM drive to access that content are also encrypted;

3) Only DVD devices manufactured in accordance with a CSS licence can decrypt and play back the movie on a protected disk; and

4) DVD devices are prohibited from allowing copies to be made of the contents of protected DVDs, except in certain circumstances.[24]

CSS decryption licences impose the following requirements on CSS-enabled DVD devices:

1) Content that is lawfully decrypted within a DVD device must be protected securely from unauthorized access within the device (*i.e.*, the DVD device must be protected from tampering);

2) Contents can only be sent to certain authorized outputs, namely:

(a) Analog outputs with technology (such as, for example, Macrovision) to prevent copying by, for example, analog VCRs;

(b) Secure digital outputs, such as DTCP (discussed below) that also guarantee that the content will travel to a known destination with a copy control TPM;

3) Devices sold in a particular geographic region can only play back disks authorized for playback in that region;

4) Manufacturers who violate these contractual rules can be sued, have

24. Cunard, *supra* note 10.

their products enjoined and pay stiff damages; and

5) Movie studios are given the right to "encode" their DVD movies and they can prevent any digital copies from being made onto a recorder.[25]

Interestingly, CSS technology and the licence to use it combine multiple content protection features. Such features include but are not limited to, "access control, copy control, control over electronic distribution and even a means of attempting to limit unauthorized geographic redistribution of the DVD disks themselves."[26]

As will be discussed in greater detail later in this article,[27] CSS was hacked using the technology of DeCSS.[28] DeCSS was developed by Jon Johansen, a Norwegian teenager, collaborating with two other individuals on the Internet, for the purpose of developing a DVD player operating on the Linux operating system. If a user runs DeCSS on a Microsoft operating system platform with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to access the DVD files and place a copy on the user's hard drive. The resulting file, while very large, can be played on a non-CSS-compliant player and may be copied or manipulated like regular computer files. The quality of the resulting decrypted movie is virtually identical to that of the original encrypted movie on the DVD. The file produced by DeCSS can also be compressed by software called DivX readily available on the Internet.[29] The compressed file can be copied onto a DVD and can be transmitted over the Internet.[30]

The circumvention of CSS gave rise to a major test case for the anti-device provisions of the *Digital Millennium Copyright Act of 1998*[31] in the United States.[32] Although the Court upheld those provisions and granted eight film studios a permanent injunction prohibiting three defendants from posting DeCSS on their website and linking to other sites containing DeCSS, this circumvention device continues to be widely available on the Internet.

One interesting lesson to be gleaned from this case is that once a software-based circumvention device becomes available, anti-circumvention legislation coupled with tough enforcement is not always sufficient to restrict the threat of circumvention. Another interesting lesson is that the mass dissemination of DeCSS over the Internet has fostered the creation and development of innovative technology. The compression software DivX was developed through the open access to the source code in DeCSS, and is now widely used in many legitimate application features such as game consoles, and video streaming. The irony is that

---

25. *Ibid.*
26. *Ibid.*
27. See Part X.D.4 below.
28. *Universal City Studios v. Reimerdes*, 111 F.Supp. 2d 294; 2000 Copr. L. Dec. P 28, 122 (S.D.N.Y. 2000) [*Universal v. Reimerdes*], aff'd sub nom. *Universal City Studios v. Corley*, 273 F.3d 429; 2001 Copr. L. Dec. P 28, 345 (2nd Cir. 2001) [*Universal v. Corley*].
29. Compression is the reduction of a file's size using a mathematical algorithm that removes redundant or non-essential information. See Stephen M. Kramarsky, "Copyright Enforcement in the Internet Age: The Law and Technology of Digital Rights Management" (2001) 11 DePaul-L.C.A. J. Art & Ent. L. & Pol'y 1 at 5-6.
30. *Universal v. Reimerdes*, *supra* note 28 at 314.
31. Pub. L. No. 105-304, 112 Stat. 2860 (codified, in relevant part at 17 U.S.C. § 1201) (Supp. IV 1999) [*DMCA*].
32. *Universal v. Reimerdes*, *supra* note 28 at 345.

DivX is a technology that many companies, including Sony and Universal Studios, use to stream video online.[33]

3) Asymmetric Application Segmentation (AAS)[34]

AAS is a technology that consists of removing a small piece of executable code from a binary application, putting the extracted code on a server and filling the gap created through the extraction with a "hook."[35] When the user runs the application, it runs until the hook is hit. Once it hits the hook, the application recognizes a need for the extracted executable code. This causes the computer to access the Internet in search of the missing code. The hook also keeps track of the context of the application—namely, who is running it, where it is being run, and at what stage the application is at. The hook travels to the appropriate server, which authenticates the user and prompts the application input context. The remote server then inputs the application context into the extracted code. It derives an output, which is sent back to the user. This enables the application so that it can continue to run. Because the application is utterly useless without the extracted code, the application is unlikely to be copied.

4) Digital Tickets

"Digital ticket" technology is based on a code embedded in a plastic card or computer.[36] This code determines whether someone has the right to access the digital content. When the ticket is presented, "it is electronically 'punched' to indicate that a right was used."[37] As a result, "a person could use a digital ticket stored on a PC or other device to display an image, print a book, or play music."[38]

The interesting part of this method is that the ticket may be transported or associated with the content in perpetuity. Thus, if the content (*e.g.*, a song, movie, or book) is emailed, downloaded, or copied, the ticket is punched again. This allows the content owner to be paid each time a copy is made. In other words, in addition to protecting unauthorized access to digital works, digital tickets can be used for fee tracking and payment as part of a DRM.

C. USE CONTROL (COPY CONTROL) TPMs

This second category of TPMs allows a rights holder to *control the underlying use* of a work, even once access has been obtained. Typically this has meant *controlling unauthorized copies* of a work—copy control protection measures are the most com-

---

33. See DivX's website announcing companies that use its technology, online: DivX <http://www.divx.com>.
34. The description of AAS in subsection II.B.4, above, and the description of "digital tickets" in subsection II.B.5, above, are only two of many examples of proprietary developments in TPM access technologies.
35. Described, online: Netquartz <http://www.netquartz.com/solutions/techno.asp>. AAS was designed and patented by Netquartz and is used in the company's digital rights management system.
36. ContentGuard is the developer and patent holder of "digital ticket" technology. For a description of "digital tickets", see ContentGuard, Press Release, "ContentGuard Awarded New Patent for 'Digital Tickets'" (27 July 2001), online: ContentGuard <http://www.contentguard.com/press_072701.asp>.
37. *Ibid.*
38. *Ibid.*

monly applied use control.[39] However, such TPMs allow for use controls other than mere copying. As de Werra notes:

> ... these technologies can protect not only against the mere copying of the work, but also against acts infringing *other* exclusive rights of copyright owners ... A technological protection measure for audio (and video) content could also be developed in order to prevent the streaming of these works on the Internet. Because streaming 'does not copy the music onto the listener's hard drive', but 'merely allows her to hear it', such a technology would mainly prevent the infringement of the right of public performance and the right of distribution, and not the right of reproduction.[40]

A discussion of some of the most popular copy control TPMs follows.

1) Macrovision

Macrovision is a copy protection method for analogue VHS videocassette recorders (VCRs). It is used to prevent the copying of pre-recorded videotapes. If a protected tape is copied, the images on the copy will not display properly when played back on a Macrovision-enabled VCR. Instead, the picture will go dark periodically and will become unstable when it is darkest.[41]

Macrovision works by exploiting the automatic gain control (AGC) circuit in the VCR when a tape is being recorded. The purpose of the AGC is to ensure that weak signals are amplified and strong signals are attenuated, so that the full recording capabilities of VCR tapes are utilized. With Macrovision, new signals are inserted in the non-visible portion of the picture. These signals make the VCR detect that the normal picture is too bright. The AGC circuit darkens the picture until it detects that it is normal but, because the picture was not too bright to start with, it now becomes too dark. This process repeats itself. TVs are not, by themselves, affected because most TVs do not have AGC circuits, and those that do operate differently than VCR AGC circuits.

This type of TPM can be used for pay TV, pay-per views, and videocassettes to prevent making copies of the audiovisual works or by deteriorating the quality of the recording or playback.

Circumvention of Macrovision is possible with the aid of commercial stabilizers.[42] Commercial stabilizers are inexpensive devices that can defeat commercial security software such as Macrovision.[43]

2) Serial Copy Management System (SCMS)

Through the use of a watermark, SCMS prevents the illegal production of multiple generations of digital copies from a copyright-protected original.[44] A watermark is information that is digitally encoded in a hidden manner into a digital

---

39. Koelman & Helberger, *supra* note 10 at 168.
40. de Werra, *supra* note 11 at 6 [footnotes omitted].
41. Macrovision FAQ, online: Hackers Catalog <http://66.40.78.100/Services/TECH_Notes/nineteen.html>. A technical description of Macrovision is available on this site.
42. *Ibid.*
43. See newsgroup posting, Daffy Duck, "Re: Why So Upset?" (4 November 1999), online: Slashdot, Post-Hacked DVD: Where to Go? <http://slashdot.org/articles/99/11/04/1415200.shtml>.
44. Online: Mitsui CD-Store.com <http://www.mitsuicdrstore.com/SCMS_nh.html>.

work.[45] The watermark information can be used to authenticate or otherwise trace copies,[46] or to assist in the implementation of a copy control function.

In SCMS, the watermark information is used to indicate whether or not a CD may be copied without restriction, copied once (for personal use), or not at all.[47] If someone attempts to use an SCMS compliant recording device to copy a CD that does not contain a SCMS watermark, the attempt will fail.[48]

A number of circumvention techniques already exist for SCMS equipment.[49] It is also noteworthy that SCMS does not prevent the making of multiple digital copies of a digital work if each copy is made from the SCMS-encoded CD. SCMS can only prevent the making of digital copies of digital copies.

3) Digital Transmission Content Protection (DTCP)

The purpose of DTCP technology is to prevent unauthorized distribution of audiovisual content received in the home in digital form once it has been decrypted.[50]

The technology controls content travelling between a DTCP "source device" (such as a cable or satellite TV set top box, DVD player, or a Sony PlayStation) and a DTCP "sink device" (such as a television set, a personal computer, or a VCR). The sink device is programmed to treat the received content securely. Thus, for example, it cannot be used to resend the content to the web.[51] DTCP has the following characteristics:

1) DTCP includes encryption between all source and sink devices;

2) DTCP requires a handshake between all source and sink devices on the system (for the purpose of ensuring that the sink devices will handle content as required by DTCP rules). Until this occurs the source device will not be permitted to send content to the sink device;

3) DTCP includes a provision for the carriage of "copy control information" in the bit stream between all source and sink devices that sends a signal to the sink device indicating if and when it can make a copy of content received via DTCP; and

4) DTCP supports the "revocation" of devices that have been hacked, or of pirated clones of hacked devices. Revoked devices simply are disabled from receiving digital content via DTCP.[52]

---

45. Rosemarie F. Jones, "Wet Footprints? Digital Watermarks: A Trail to the Copyright Infringer on the Internet" (1999) 26 Pepp. L. Rev. 559 at 568–569.
46. For example, "watermarks can be used for tracing the origin of copyrighted works when they are found on websites or other places where they are not supposed to be." See Cunard, *supra* note 10.
47. *Supra* note 43.
48. The *Audio Home Recording Act of 1992*, Pub. L. No. 102-563, 106 Stat. 4237 (codified as amended at 17 U.S.C. § 1001-1010 at 1002 (1994)) requires the incorporation of SCMS functionality into all digital audio recording devices imported, manufactured or distributed in the United States.
49. See e.g. "SCMS - Serial Copy Management System" (7 April 1997), online: Heiko's DAT page <http://www.fet.uni-hannover.de/~purnhage/dat/dat.html>.
50. Cunard, *supra* note 10. DTCP was jointly developed by: Hitachi Ltd., Intel Corporation., Matsushita Electric Industrial Co. Ltd., Sony Corporation, and Toshiba Corporation. The consortium is referred to as the 5C (five companies). See especially "5C Digital Transmission Content Protection White Paper" (14 July 1998), online: Digital Transmission Licensing Administrator <http://www.dtcp.com/data/wp_spec.pdf>.
51. *Ibid.*
52. *Ibid.* See also "DTCP Tutorial"(16 June 1999), online: Digital Transmission Licensing Administrator <http://www.dtcp.com/data/dtcp_tut.pdf>.

DTCP technology, like CSS, is also subject to a comprehensive licensing scheme. The DTCP scheme contains the following elements:

1) Content owners are permitted to encode certain movies and types of transmissions or delivery services as:
   (a) "copy never"—no copies can ever be made;
   (b) "copy one generation"—one generation of digital copies is permitted; or
   (c) "copying is permitted, but with no retransmission"—multiple copies can be made but no retransmission to an unauthorized output is permitted;
2) DTCP-enabled devices must be built robustly;
3) Devices can hand off content protected by DTCP only to:
   (a) copy protected analogue outputs; and
   (b) DTCP outputs or other approved, secure digital outputs;
4) The content can never be sent to the Internet, since connections to the Internet are not secure;
5) Devices can only record if the copyright owner has authorized copying, as indicated by the encoding rules; and
6) Any copies made by a DTCP-licensed device must be recorded securely, for example, only by an authorized encryption system, so that the recording itself is encrypted.[53]

4) Secure Digital Music Initiative (SDMI)

Encryption has not typically been employed to protect the contents of commercially produced music CDs. The music on these CDs can easily be recorded and digitally compressed into much smaller files. The most common technology used for this purpose is MP3. Music that has been treated in this fashion can be copied onto hard drives, then copied onto recordable CDs, or easily distributed over the Internet while approximating its original sound quality.[54]

SDMI, an initiative of more than 200 companies and organizations representing information technology, consumer electronics, security technology, the worldwide recording industry and Internet service providers, undertook to address this issue.[55] SDMI drafted guidelines and specifications aimed at implementing technological protection measures into commercial music files. The protection measures are manifested in an encryption scheme allowing only for particular uses, *i.e.*, authorized interactions with the content. Sometimes, the encryption and related certificates are referred to as watermarking—this is the case when protection measures are built into rendering devices to recognize the embedded content code and compare it against a revocation list. Music watermarked as "no

53. Cunard, *supra* note 10. See also "Digital Transmission Content Protection Specification Volume 1 (Informational version)" (25 February 2002), online: Digital Transmission Licensing Administrator <http://www.dtcp.com/data/info_dtcp_v1.pdf>.

54. Cunard, *supra* note 10. See also Fraunhofer Institut Integrierte Schaltungen (Inventions of ISO-MPEG Audio Layer-3), online: Fraunhofer Institut Integrierte Schaltungen <http://www.iis.fhg.de/amm/techinf/layer3/index.html>; Moving Pictures Experts Group (MPEG) Home Page, online: <http://mpeg.telecomitalialab.com>.

55. Secure Digital Music Initiative Foundation, online: <http://www.sdmi.org>. See also Recording Industry Association of America, online: <http://www.riaa.org/Music-SDMI-1.cfm>.

copy" would be both understood and enforced by sympathetic rendering devices.

Under SDMI, music would have been protected not only by watermarks, but also by secure (*i.e.*, encrypted and authenticated) communications between an SDMI-compliant software application and a portable device, such as a handheld MP3 player.[56] In September 2000, SDMI published its code and issued a challenge to the cryptography community, offering $10,000 to any persons who could "remove the watermark or defeat the other technology on our proposed copyright protection system."[57] A research team from Princeton University promptly cracked the encryption algorithms protecting the digital content.

Subsequently, one of the researchers was threatened against publishing the details of the SDMI crack under the United States' *DMCA* provisions prohibiting the distribution of technology that circumvents protection measures and/or removes or alters copyright management information.[58] The research team countered with a federal lawsuit against RIAA that sought permission to publish their results under the tenets of the scientific research community and academic freedom.[59] The researchers lost the initial contest, and have since "decided to forgo ongoing appeals in the light of government and industry assurance that academics are free to do and publish research."[60]

III. Circumvention

IT IS IMPORTANT TO RECOGNIZE that the very technologies that have been used to control intellectual property rights in cyberspace and elsewhere have also been used to exploit them. "Circumvention" of a TPM refers to the breaking or avoidance of the use of a protection measure to prevent unauthorized access to a system or mechanism such as a database, satellite system or security mechanism attached to DVD movies.[61]

Circumvention of a TPM put in place by a copyright owner to control a digital work subject to copyright has been described by some as the electronic equivalent of breaking and entering into a locked room in order to obtain a copy of a work, such as a book.[62] Some estimates of the cost of illegal circumvention are

---

56. EC, Commission, *Working Paper: Digital Rights: Background, Systems, Assessment* (Brussels: EC, 2002) at 19 ["EU DRM Project"], online: Europa <http://www.europa.eu.int/information_society/newsroom/documents/drm_workingdoc.pdf>. See e.g. Cunard, *supra* note 10. See generally "SDMI Portable Device Specification Part 1 Version 1.0" (8 July 1999), online: Secure Digital Music Initiative Foundation <http://www.sdmi.org/download/port_device_spec_part1.pdf>.
57. Secure Digital Music Initiative Foundation , Press Release, "An Open Letter to the Digital Community" (6 September 2000), online: Secure Digital Music Initiative Foundation <http://www.sdmi.org/pr/OL_Sept_6_2000.htm>.
58. Read the RIAA's letter to Professor Edward Felten, online: Electronic Frontier Foundation <http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html>. For a more detailed analysis, see Part X.D.4, below.
59. See *Felten v. RIAA*, No. 01 Civ. 2669 (E.D.N.J. Nov. 28, 2001) [unreported], online: Electronic Frontier Foundation <http://www.eff.org/Cases/Felten_v_RIAA/20011128_hearing_transcript.pdf>.
60. Recent EFF Legal Cases and Efforts (February 2002), online: Electronic Frontier Foundation <http://www.eff.org/Legal/recent_legal.html>.
61. *Universal v. Reimerdes*, *supra* note 28.
62. U.S., (H.R. Rep. No. 105-551) (1998) at 17, cited in David Nimmer, "A Riff on Fair Use in the Digital Millennium Copyright Act" (2000) 148 U. Pa. L. Rev. 673.

staggering. For example, the Motion Picture Association (MPA) estimates that the American motion picture industry experiences lost revenue in excess of US$3 billion each year due to piracy.[63] Additionally, the Business Software Alliance (BSA) estimates that the software industry lost US$11.75 billion of revenue in the year 2000 as a result of piracy.[64] Canadian estimates in the same year suggested a CDN$305 million loss in the national packaged software industry alone.[65] As well, increases in security costs resulting from the proliferation of circumvention technologies translate into higher costs for content consumers, and corresponding disincentives for continued production.[66]

Although several instances of circumvention have already been mentioned above, it is important to have a clearer understanding of what circumvention devices are and how they function. Risher has provided the following examples of circumvention technologies:

> *Posting passwords and registration numbers:* The posting of such information allows others who have not purchased access rights to use pirated versions of software or to gain unauthorized access to a network or other system containing copyrighted works.
>
> *Intercepting decrypted content:* This method involves using software that captures the program as it is decrypted and before it interacts with the software used for viewing or playing the content.
>
> *Brute-force decryption:* This form of circumvention employs multiple variations of algorithms until the content is decrypted and therefore requires substantial computer power.
>
> *Stealing the key during transmission:* Digital pirates engage in channel interception in order to intercept a key when it is transmitted.
>
> *Hacking Closed Systems:* This form of circumvention involves dissembling closed system trusted devices and breaking the decryption code by interacting with the circuits.
>
> *Pirated Plug-ins:* This circumvention method entails the development of illegal software plug-ins that can override the trust-enabled player plug-ins.[67]

As noted above, some of the most commonly used TPMs, such as Macrovision, CSS, SCMS and SDMI, have already been circumvented. In short, there is an escalating "arms race" between those who design TPMs and those who defeat them. However, it is important to note that the reasons motivating circumvention vary. Although sometimes motivated by "infringement" and the desire to illegally disseminate copyrighted digital works, there are also legitimate reasons

---

63. See online: Motion Picture Association of America <http://www.mpaa.org/anti-piracy/content.htm>.
64. See "Sixth Annual BSA Global Software Piracy Study" (May, 2001), online: Business Software Alliance <http://www.bsa.org/resources/2001-05-21.55.pdf>.
65. See "Canadian Software Provincial Piracy Study" (November, 2001), online: Canadian Alliance Against Software Theft <http://www.caast.org/resources/FINAL.CanadianReport.pdf/>.
66. See Lawrence Lessig, *Code and Other Laws of Cyberspace*, (New York: Basic Books, 1999) [Lessig, *Code*].
67. Risher, *supra* note 14 at 5-6.

for circumvention. Circumvention has often been motivated by: the aim of achieving system interoperability; the desire to test the robustness of a TPM and thereby improve the state of the art; the desire to satisfy intellectual curiosity; other purely academic purposes; and the aim of advancing the science of cryptography.

Some people also claim to be motivated to circumvent TPMs for the sake of justice, especially when they perceive that TPMs prevent them from exercising rights in a digital work that they claim to have, or ought to have, under the law. As will be discussed in greater detail, the motives for circumventing TPMs articulated above suggest that a policy choice that would result in anti-circumvention laws should be approached with great caution.[68]

IV. Digital Rights Management (DRM) Systems

A. THE DRM CONCEPT

The attempt to provide a simple description of TPMs has been complicated by the introduction of more sophisticated information systems designed to protect intellectual property. These systems are known as digital rights management (DRM) systems. Some DRMs incorporate technological measures within their infrastructure, while other DRMs exhibit characteristics making them more like an advanced kind of TPM. One author has defined DRMs as "technology systems facilitating the trusted, dynamic management of rights in any kind of digital information, throughout its lifecycle and wherever and however it is distributed."[69]

Typically, a DRM consists of two components: a database containing information which identifies the content and rights holders of a work; and a licensing arrangement which establishes the terms of use for the underlying work.[70]

DRMs fall into two general categories: those that utilize technological protection measures and those that do not.[71]

---

68. For a real-life example of the chilling effect that TPM anti-circumvention legislation can have on legitimate research in the area of cryptography, see Niels Ferguson, "Censorship in Action: why I don't publish my HDCP results" (15 August 2001), online: <http://www.macfergus.com/niels/*dmca*/cia.html>.

69. Nic Garnett, "Technological Protection of Copyright Works, and Copyright Management Systems" (Paper presented to the ALAI Congress, June 2001) [unpublished], online: ALAI 2001 Congress Program and Presentation < http://www.law.columbia.edu/conferences/2001/program_en.htm>. This is a fairly broad definition of DRMs for, as the author notes, "[t]he term DRM has now come to be applied to a variety of different technologies, most of which relate to the control of access to information or to its copying."

70. See Daniel J. Gervais, "Electronic Rights Management and Digital Identifier Systems" (1999), The Journal of Electronic Publishing, online: University of Michigan Press < http://www.press.umich.edu/jep/04-03/gervais.html>. See also P. Bernt Hugenholtz, "Copyright, Contract and Code: What Will Remain of the Public Domain" (2000) 26 Brook. J. Int'l L. 77 at 78 [Hugenholtz, "Public Domain"]. Hugenholtz has defined a DRM similarly as a contract, typically a licensing agreement, coupled with technology, typically a technological protection measure such as encryption.

71. See Tarja Koskinen-Olsson, "Secure IPR-Content on the Internet" (Paper presented to the WIPO Second International Conference on Electronic Commerce and Intellectual Property, 19–21 September 2001) [unpublished], online: WIPO Electronic Commerce <http://ecommerce.wipo.int/meetings/2001/conference/presentations/pdf/koskinen.pdf>.

1) DRMs That Do Not Utilize TPMs

These types of DRMs are readily associated with copyright management organizations (CMOs) or copyright societies.[72] CMOs are generally organizations that represent artists who grant users permission to use works within the CMO's repertoire. Typically, CMOs negotiate the fees and terms of use for works on behalf of artists, and are later responsible for collecting those fees and distributing the royalties. Because CMOs often determine and authorize reproduction rights (*i.e.*, to reuse, republish, redistribute and copy), they are sometimes referred to as copyright clearance agents.[73]

Many CMOs provide Internet and other online technologies to mediate the clearing of rights, establishment of licence terms and payment of fees for the use of a work.[74] Such technologies facilitate the expediency and efficiency of licensing content. The use of such technologies must be contrasted with the use of TPMs. The latter refers only to those technologies that control access to, or the use of, a work via the technology itself, as opposed to via a licensing arrangement.

2) TPM-Enabled DRMs

While DRMs are a generic term for a method that identifies content and sets out licensing conditions, it seems that the term DRM has more recently become synonymous for those DRMs that use TPMs. More and more, DRMs rely on TPMs to manage the rights that accompany digital content.[75] For the remainder of this article, reference to a DRM means a TPM-enabled DRM.

DRMs are capable of controlling, monitoring and metering most uses of a digital work. In this respect, DRMs can be linked to royalty tracking and accounting systems where the copyright holder is able to track usage and payment. They also enable a wide variety of business models beyond sales and subscriptions, such as licensing with variable terms and conditions. For example, DRMs make it possible for a copyright holder to permit potential customers to sample digital content in a demonstration mode. DRMs also "make it possible to offer site licenses based on numbers of simultaneous users or linked to specific hardware."[76] Terms of use can be based on limited and unlimited use, or time related use. This is perhaps best illustrated by way of the example in the following section.

(i) Digital Object Identifier

The Digital Object Identifier (DOI) Foundation is an international non-profit organization working to develop an international identification system for digital

72. A well-known Canadian example of a CMO is SOCAN. A well-known U.S. example is the Copyright Clearance Center. For an excellent overview of the different types of copyright management organizations both domestically and internationally, see Canadian Heritage, *Collective Management of Copyright and Neighbouring Rights in Canada: An International Perspective* by Daniel Gervais (Ottawa: Copyright Policy Branch, Canadian Heritage, 2001), online: Canadian Heritage: Copyright Policy <http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/collective/index_e.cfm> [*Collective Management*].

73. Koskinen-Olsson, *supra* note 71.

74. *Ibid.*

75. Cunard, *supra* note 10.

76. Risher, *supra* note 14.

intellectual property.[77] The Foundation is a consortium of publishing organizations such as Microsoft Corporation and the Association of American Publishers.[78] The DOI is being developed as a voluntary standard within the publishing field.

The identification of content to which rights specified by a DRM are attached is a pre-condition for the effective enforcement of digital rights. Identifier standards such as ISBN, ISWC and ISRC have been developed to identify various classes of physical works. The DOI is their electronic equivalent.

The DOI system uses a distributed central directory. The particular advantage of this system is its ability to route those searching for a particular piece of content using a DOI identifier to the destination that contains this content. When a user clicks on a DOI, a message is sent to the directory where the current address associated with the DOI is listed. The location information is sent to the user, permitting redirection within a browser to the actual destination associated with the DOI. Thus, the user will either see the content itself, or further information about the provider of the content and how the content may be obtained.[79]

Once digital content has been identified, the DOI connects to a description of a work. The description, which is called metadata, includes information about the ownership of the content. Typical information includes items such as the author's name, date of publication and operating territory.[80]

Once digital content has been identified and described, a set of rules for its use must be developed. Digital rights fall into a number of categories. For example, transport rights include the rights to copy, transfer or loan. Render rights include the rights to play or print. Derivative rights include the rights to extract, embed and edit. A number of rights languages have been developed that describe various rights.[81] For example, a rule might permit a piece of content to be printed, but not digitally copied.

(ii) Extensible Rights Mark-up Language (XrML)

XrML is a digital rights language software developed at the Xerox Palo Alto Research Centre under the direction of Dr. Mark Stefik. XrML is an automated system that allows rights holders to embed rules into hypertext/code.[82] This software can be used in the selling and licensing of electronic books, digital video and music, computer games, software and other objects in digital forms. XrML describes the rights, costs and conditions of a work. Sophisticated tools for rule-setting are being developed. Software such as XrML from ContentGuard will enable more complex rules to be established.[83] Some basic features of this soft-

77. See online: The International DOI Foundation <http://www.doi.org/overview/sys_overview_021601.html>.
78. See online: The International DOI Foundation <http://www.doi.org/idf-member-list.html>.
79. *Supra* note 77.
80. See "EU DRM Project," *supra* note 56 at 10. It has been noted that metadata technologies are in an advanced state of development.
81. Mark Stefik, "Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing" (1997) 12 Berkeley Tech. L.J. 137 at 140–141.
82. See online: XrML <http://www.xrml.org/about.asp>.
83. "EU DRM Project" *supra* note 56 at 10.

ware include:[84]

· Rights are associated with a part of a digital product;

· Each class of usage rights has corresponding transactions;[85]

· Transactions define what a repository does when the rights are realized;

· Rights are described in terms of machine-oriented language;

· Digital Product transactions require restrictions based on the underlying usage rights for the product;

· Rights in a digital product can be changed, if the change is allowed by the owner of the rights;

· Each right is connected with the set of conditions for using a digital product;

· Each condition can have different types: charge per the use, time of use, type of access, type of digital watermark, type of devices on which these operations are performed and so on;

· Each digital product has its own specification that defines groups of rights for each work as a whole and its parts.

The essence of XrML is to provide rights holders with a tool to prevent unauthorized access and use of their work.

B. THE POLICY IMPLICATIONS OF DRMs

Some believe that DRMs will one day soon become an industry standard. Others believe that they already have.[86] Those who contend that DRMs have yet to become an industry standard point to various remaining problems associated with their technological development, the difficulty in determining relevant standards and other difficulties related to interoperability.[87] In any event, the evolution and future use of DRMs as a standard method of digital protection remains somewhat unknown.

Given their ability to unbundle copyright into discrete and custom-made products, DRMs promise a much greater range of consumer choice and perhaps even a reduction in pricing. At the same time, the adoption of DRMs will also give greater control to copyright holders to exercise their rights in digital content, thereby facilitating legitimate access to digital works. At first blush, this may seem like a win-win situation. However, the degree of control that publishers will

---

84. See online: Digital Intellect <http://www.intellect.vsu.ru/en/management/technology/xrml_e.htm>.

85. *Ibid.*

Category of Rights	*Actions*
Transfer of rights from one user to another	Product movement from one repository to another
Rights to reproduction	Print and display of product
Rights to derived products	Using the product for creation of new products
Rights to file management	Creation and restoration of reserved copies
Rights to system configuration	Software installation in repository

86. See generally Michael A. Einhorn, "Digital Rights Management and Access Protection: An Economic Analysis" (Paper presented to the ALAI Congress, June 2001) [unpublished], online: ALAI 2001 Congress Program and Presentation <http://www.law.columbia.edu/conferences/2001/program_en.htm>. See also Jan Kaestner, "Law and Technology Convergence: Intellectual Property Rights," online: Eclip <http://www.eclip.org/documentsII/sum/research.htm>.

87. See Cunard, *supra* note 10. See also Stefik, *supra* note 81 at 157.

obtain over works in a digital environment could also result in attempts to apply and enforce copyright in ways never previously contemplated by Canadian copyright law. For example, it might allow copyright holders to exclude various forms of public access to a digital work. This very real possibility could entirely undermine the delicate balance between private rights and the public interest that copyright law seeks to achieve. DRMs may additionally have privacy implications. These issues will be explored in greater detail throughout the rest of our article.

v. The Future of TPMs and DRMs

THE FUTURE ABOUNDS with question marks. Still, it is evident from the recent trends discussed above that the development of full-scale DRMs requires the cooperation of a number of different stakeholders including copyright owners, system operators, manufacturers of end-products and consumers. The success of new DRM technologies will likely require agreements to be reached amongst this motley crew of interest groups. The process of achieving acceptable standards and protocols could, in some instances, take a number of years. Consequently, the full-scale adoption of DRMs could be significantly delayed.[88] It follows that the adoption of corresponding TPMs might also be significantly delayed. These delays might lead to the development of an unmanageable number of isolated, interim TPMs by those who are unwilling to wait for the culmination of the slow consensus-building process required for the development of more widespread DRMs. A proliferation of interim TPMs would significantly diminish the interoperability between the various technologies, something that consumers would find frustrating and unacceptable.

While we are still at a stage where many TPMs exist and others will become available, the success of full-scale DRMs requires the development of uniform and interoperable information systems. Three possible approaches have been proposed for the creation of a more comprehensive copy protection architecture. These are:

1) A set of cascading technologies and legal obligations, in which one TPM will only hand off a copyrighted work that it protects to another TPM when there is adequate assurance that the downstream TPM will handle the work securely;

2) The development of a single comprehensive TPM architecture for handling TPMs that includes features such as encryption, authentication, watermarks, mechanisms that will only download to secure outputs, and other such mechanisms;

3) A requirement that licensees who wish to build a product in a particular format adopt a corresponding TPM through linked grants of intellectual property rights from the licensor of the technologies.[89]

Although it is theoretically possible that, one day, one of the above proposals might possibly lead to the development of a full-scale DRM that manages to maintain copyright's delicate balance between private rights and the public

88. See Cunard, *ibid.*
89. *Ibid.*

interest,[90] it goes without saying that none of the above proposals could ever prevent the future circumvention of TPMs. Still, there are at least two general approaches that are thought to assist in minimizing the threat of circumvention.

The first approach is technological. In the context of digital rights management, *renewal* refers to "the process of issuing a new certificate using the same public key from the previous certificate."[91] This is done as a means of validating each interaction between the rendering device and the copyright work. The original certificate is obtained by registering a valid registry code provided post-payment. However, due to the ability to create fraudulent registry certificates,[92] a certificate validation process determines the trustworthiness of the current enabling certificate prior to certificate renewal. If found invalid, either due to being tampered with or being included in a certificate revocation list,[93] the certificate is revoked rather than renewed. In this context, revocation refers to the ability to disable a device that handles copyright works if that device has been hacked. Certificate revocation prevents the copyright work from being rendered.[94] Renewal and revocation each have their own shortcomings. If renewal occurs through software downloads, users may be disgruntled at having to upgrade. They may also have concerns about privacy and loss of autonomy with respect to their private usage of copyright works.[95] Revocation is problematic insofar as it remains susceptible to other circumvention devices that cloak the fact that the TPM has been hacked.

The second general approach is not technological but legal. This approach involves the creation of a prohibition on the circumvention of some or all types of TPMs (with a circumscribed range of possible exceptions).[96] This approach is fraught with other difficulties that will be examined at length in the ensuing sections of this article. Before we tackle the policy implications of TPMs, it is worth noting that a fundamental question lingers: *Will TPMs be used as widely as predicted?*

Unfortunately, there is no way to forecast with certainty since the answer to this question must surely depend on the response of consumers to the unbundled, pay-per-play world of digital content both online and off. And it is early days

---

90. Despite the urging of Stefik and others, it is worth noting that very few intellectual property scholars are optimistic about this possibility. See *e.g.* those cited at *infra* note 128.
91. Entrust Resources Security Glossary, online: <http://www.entrust.com/resources/glossary.htm#2>.
92. A product is 'cracked' when a product registration is 'hacked,' *i.e.*, the renewal process is sidestepped or fooled.
93. A list of certificates that have been revoked as a result of being cracked or expired.
94. For greater explanation of both renewal and revocation in the context of digital rights management, see Entrust Resources Security Glossary, *supra* note 91.
95. This practice raises the issue of anonymity with respect to the furtherance and enjoyment of the marketplace of ideas and cultural content. In order to encourage participation in the marketplace of ideas or the public commons—the very foundation of a democracy—an individual's right to not be publicly associated with a particular piece of content must be respected. See generally Anne Wells Branscomb, "Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces" (1995) 104 Yale L.J. 1639; A. Michael Froomkin, "Anonymity and Its Enmities" (1995) J. Online L. art. 4; M. Ethan Katsh, "The First Amendment and Technological Change: The New Media Have a Message" (1989) 57 Geo. Wash. L. Rev. 1459; George P. Long, "Who Are You?: Identity and Anonymity in Cyberspace" (1994) 55 U. Pitt. L. Rev. 1177; David G. Post, "Pooling Intellectual Capital: Thoughts of Anonymity, Pseudonymity, and Limited Liability in Cyberspace" (1996) U. Chicago Legal F. 139.
96. As discussed in considerable detail in Part X, variations on this approach have already been adopted in the United States and some European Union countries.

in this regard. Still, it should be recalled that in the early 1980s many companies that sold software applications employed a form of copy protection to prevent the floppy disks on which their applications were sold from being copied. Massive consumer resistance to this approach led to the abandonment of this TPM and yet software companies subsequently found the risk of illegal copying to be within acceptable limits.[97]

If consumers find TPMs cumbersome, overly restrictive, or too expensive to use, they may just put their money where their mouse is, forcing content providers to minimize the use of TPMs. This is particularly true if the use of newer TPMs creates compatibility problems that prevent new content (protected with newer TPMs) from being played on older equipment or older content (not incorporating the latest TPM) from being played on newer equipment, both of which are likely outcomes if TPMs evolve outside of a single, coherent digital format at a rapid pace.

There is an important observation to be gleaned from any attempt to predict the future of TPMs. Given the uncertainty of so many factors necessary to the long term success of using TPMs as a means of protecting intellectual property rights in digital content, it would seem that great caution should be exercised by policymakers who are considering an immediate legal response to what is still a relatively unknown, if not practically unborn, technology.

VI. The Legal Concept of TPMs

A. INTRODUCTION

As a signatory to the *WCT* and the *WPPT*, Canada currently appears committed to provide some degree of legal protection against the circumvention of TPMs.[98] However, the technologies employed by DRMs are not yet sufficiently sophisticated to mirror the law of copyright because TPMs themselves remain incapable of distinguishing between infringing and non-infringing uses of digital works.[99] One question that remains, therefore, is whether it is possible to legally protect TPMs without undermining the tradition of copyright law and its well-established body of public interest exceptions.

Proponents of the legal protection of TPMs would argue that technological protection measures merely preserve the *status quo* already established under copyright legislation. On the other hand, opponents fear that affording additional legal protection to TPMs will tilt copyright's balance firmly in favour of copyright owners, much to the detriment of the public interest. Adding an additional layer of legal protection, opponents would say, makes it easier for those who use TPMs to undermine, rather than preserve, the desired balance that copyright law

---

97. P. Bernt Hugenholtz, "Code As Code, Or the End of Intellectual Property as We Know It" (1999) 6 M.J.E.C.L. 308, online: Institute for Information Law <http://www.ivir.nl/publications/hugenholtz/MAASTRIC.DOC> [Hugenholtz, "Code as Code"].

98. Although the two treaties have been signed by Canada, they remain subject to ratification.

99. See Kamiel J. Koelman, "The Protection of Technological Measures vs. the Copyright Limitations" (Paper presented to the ALAI Congress, June 2001) [unpublished], online: ALAI 2001 Congress Program and Presentation <http://www.law.columbia.edu/conferences/2001/program_en.htm>; Nimmer, *supra* note 62.

strives to achieve. Of course, this begs the question of whether traditional limitations on copyright remain relevant in a digital environment. The following sections explore these and other related issues in the context of a more narrow investigation concerning the extent of legal protection, if any, that ought to be afforded to TPMs to prevent copyright infringement through their circumvention.

B. THE TPM CONCEPT IN THE WCT AND WPPT

In December of 1996, delegates from almost 150 countries met to determine whether international copyright reform was perceived necessary in light of the proliferation of illegal copying transmitted through electronic means.[100] The question whether to afford legal protection to TPMs was one of the items considered. Based on the general recognition that TPMs are vulnerable to circumvention, a consensus was reached that would require legal protection against circumvention. This consensus was ultimately reflected in article 11 of the *WCT* and article 18 of the *WPPT*.[101] In order to understand these provisions and their potential application in Canadian national law, it is useful to describe briefly how these provisions evolved into their present form.

Some estimates about the cost of illegal circumvention, both in terms of lost revenues and increased security costs, are staggering. Much of the impetus for the two WIPO provisions originated from the strong lobby of content holders and software organizations in the United States, although the current versions of article 11 of the *WCT* and article 18 of the *WPPT* are much weaker than those originally proposed by the United States.[102] The original U.S. proposal to WIPO was stronger in that it included a blanket prohibition on the circumvention of TPMs (rather than restricting the ban to circumvention for infringing purposes). Moreover, under the U.S. proposal, a manufacturer could be liable even where it had no knowledge that a device would be used for infringement. The European Union also made a proposal to WIPO regarding the legal protection of TPMs.[103] The European proposal was preferred to the U.S. proposal because the European proposal imposed a knowledge requirement, though it still prohibited circumvention *per se*, rather than circumvention for infringement.[104]

---

100. Tamber Christian, "Implementation of the WIPO Copyright Treaty—How Hard Can it Be?" (1998) 15:3 Computer Law. 8 at 8.

101. *WCT*, *supra* note 3; *WPPT*, *supra* note 4. The *WCT* and *WPPT* entered into force with the depositing of the 30th ratification.

102. Adoption of the weaker provisions was said to be due to the domestic opposition by the U.S. administration to similar draft legislation circulating domestically within the U.S. A very interesting recitation of the involvement of the United States in developments leading to the WIPO *WCT* is provided by Jessica Litman, *Digital Copyright* (Amherst: Prometheus Books, 2001). Chapter 9, "The Bargaining Table" provides an extensive overview of the American influence on the drafting of the *WCT* and *WPPT*. See also Pamela Samuelson, "The U.S. Digital Agenda at WIPO" (1997) 37 Va. J. Int'l L. 369 [Samuelson, "U.S. Digital Agenda"].

103. Thomas C. Vinje, "The New WIPO Copyright Treaty: A Happy Result in Geneva" (1997) 19 Eur. I.P. Rev. 230 at 234.

104. *Ibid.*

Pursuant to a WIPO document known as the Basic Proposal,[105] which was circulated before the language of the *WCT* was finalized, the term "technological measures" was defined as "any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty."[106] Article 13 of the Basic Proposal addressed the legal protection of TPMs as follows:

> 1) Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the device or service will be used for, or in the course of, the exercise of rights provided under this Treaty that it is not authorized by the rightholder or the law.
>
> 2) Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).
>
> 3) As used in this Article, "protection-defeating device" means any device, product or component incorporated into a device or product, the primary purpose or primary effect of which is to circumvent any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty.[107]

Although this provision introduced a knowledge requirement directed at infringement, European scholars argued that this provision would effectively write the various existing exceptions out of copyright law, thereby creating information monopolies, without any examination of whether such a change in copyright law is appropriate.[108] Manufacturers agreed with this assessment and also pointed out dangers to innovative consumer electronics and computer products.[109] For example, consumer electronics manufacturers were concerned that the Basic Proposal could require them to alter their equipment, such as VCRs, to function with a number of various protection systems.[110] Computer manufacturers were apprehensive that the Basic Proposal could outlaw computers as "protection-defeating" devices.[111]

During the diplomatic conference held in Geneva in December 1996, these concerns were also expressed by numerous delegations and no country insisted on the passage of the Basic Proposal as originally put forward.[112] Some countries were opposed to the inclusion of any legal protection for TPMs in the *WCT*.[113] Other countries were opposed to the Basic Proposal on the basis that it would restrict access to works in the public domain and uses of copyright

---

105. WIPO (Chairman of the Committee of Experts), "Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference," Doc. No. CRNR/DC/4 (30 August 1996) [Basic Proposal], online: <http://www.wipo.org/eng/diplconf/4dc_star.htm>.
106. *Ibid.*, art. 13.
107. *Ibid.*
108. Vinje, *supra* note 103.
109. *Ibid.* at 235.
110. *Ibid.*
111. *Ibid.*
112. *Ibid.*
113. *Ibid.*

materials permitted by law.[114] Other delegations, including Canada, were concerned about restrictions on legitimate activities.[115] In the end, the final wording of article 11 of the *WCT* was adopted pursuant to a compromise agreed to by certain parties prior to the diplomatic conference and advanced by South Africa at the conference.[116] The final text of article 11 of the *WCT* and article 18 of the *WPPT* read as follows:

> Article 11 (*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 authorized by the authors concerned or permitted by law.[117]

> Article 18 (*WPPT*)
> 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 authorized by the performers or the producers of phonograms concerned or permitted by law.[118]

Pursuant to article 11 of the *WCT*, the only TPMs subject to legal protection against circumvention are those that: (a) are effective; (b) are used by authors to exercise copyrights; and (c) restrict acts not authorized by authors or permitted by law.[119]

i) Effective

The meaning of "effective" in this provision is not entirely clear. Some scholars have suggested that the word "effective" was inserted in order to ensure that TPMs that can be too easily or accidentally circumvented are not subject to legal protection.[120] This reasoning, however, generates a rather strange antinomy: if the TPM is effective, it gets full protection but needs none; if the TPM is ineffective, it needs full protection but gets none.[121]

Other more political rationales have also been provided. For example, Samuelson postulates that the requirement of "effective" was included in order to

---

114. *Ibid.*
115. *Ibid.*
116. *Ibid.*
117. *WCT*, *supra* note 3.
118. *WPPT*, *supra* note 4. Since the language of the two provisions is so similar, the analysis that follows is provided in the context of art. 11 of the *WCT*. However, it applies by analogy to art. 18 of the *WPPT* as well.
119. Koelman & Helberger, *supra* note 10 at 171. The "used by authors" requirement applies in the case of the *WCT*. In the case of the *WPPT*, the requirement is "used by performers or producers of phonograms."
120. de Werra, *supra* note 11 at 10. See also Koelman & Helberger, *supra* note 10 at 172. Both works draw from the writing of André Lucas, *Droit d'auteur et numérique* (Paris: Litec, 1998) at 274. Lucas elucidates on the effective requirement, "Elle s'explique probablement par l'idée que le droit n'a pas à venir au secours de celui qui n'utilise même pas toutes les ressources de la technique."
121. de Werra, *supra* note 11 makes a similar point.

provide a mechanism with which to challenge those foreign national legislatures that adopted insufficient or weak TPM protection provisions.[122]

It is worth noting that most cryptologists are of the view that there is no such thing as an effective technological measure for preventing copying. As one cryptologist recently put it, "If I can see something, I can record it. And if I can record it, I can eventually copy it."[123] Most computer scientists are of the view that anything that can be encrypted can ultimately be decrypted. This renders implausible the idea that an "effective" TPM is one that is difficult or impossible to crack. Perhaps, then, the more sensible understanding is to say that a TPM is "effective" if it normally costs more to circumvent the TPM than it would to pay for the product it is meant to protect.

One relatively uncontroversial conclusion that can be drawn from the presence of the word "effective" in these provisions is that *not every* TPM is subject to legal protection.[124] The word "effective" is clearly meant to limit the parameters of legal protection afforded to TPMs.

Contracting States are also provided considerable freedom with respect to implementing the *WCT*'s requirement of "effective" legal remedies for circumvention. That is, States are free to employ criminal and/or civil remedies according to their own domestic law.[125] However, the use of the word "effective" suggests that the chosen remedies must have at least some remedial effect (and possibly a deterrent effect) against the circumvention activities that the particular State proscribes.

2) Used by Authors to Exercise Copyright

A literal interpretation of the requirements that TPMs must be "used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention" *and* "restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law" suggests that TPMs must restrict acts that are protected by copyright law in order to qualify for legal protection pursuant to article 11 of the *WCT*.[126]

According to this interpretation, article 11 of the *WCT* does not require states to prohibit the circumvention of a TPM in order to benefit from one of the exceptions to copyright (such as, for example, fair dealing in Canada). This suggests that only circumventions resulting in copyright infringement will be subject to article 11.[127] Accordingly, states are not obliged to confer legal protection to TPMs used for other purposes (such as, the geographical distribution of works, databases, or mere access to works).[128]

---

122. Samuelson, "U.S. Digital Agenda" *supra* note 102 at 415.
123. Words to this effect were offered by a Canadian computer scientist named Matthew Scala during his intervention at the recent Digital Copyright Consultation in Ottawa on April 11, 2002 [unpublished].
124. Koelman & Helberger, *supra* note 10 at 172.
125. de Werra, *supra* note 11 at 13-14.
126. *Ibid.* at 11.
127. *Ibid.* at 11-12. See also Koelman & Helberger, *supra* note 10 at 173.
128. de Werra, *supra* note 11 at 12.

3) Unauthorized Acts Permitted by Law

Others have interpreted the clause, "restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law" to mean that article 11 of the *WCT* aims to protect rightsholders against the circumvention of access control TPMs.[129] Those who adopt this interpretation believe that the *WCT* implicitly creates a *sui generis* right of access-control.[130]

Differing approaches as to the correct interpretation of TPMs (for the purpose of compliance with article 11) are made manifest in the dissimilar legal regimes adopted by some States that have already implemented the *WCT* into their domestic law. For countries who have not yet implemented the *WCT*, such as Canada, choosing an appropriate interpretation is a crucial first step—likely much more important than the arduous details in the statutes that are ultimately drafted. For this reason, the differences between the various approaches will be discussed in further detail below.

To sum up our preliminary discussion of the TPM concept, it is clear that there is no singular correct approach to interpreting articles 11 and 18. The *WCT* and *WPPT* provide WIPO Members with large degrees of latitude as to how a particular state might choose to fulfill its obligations with respect to the relevant provisions. Consequently, there is considerable flexibility as to how Canada might implement these provisions, should the Government elect to ratify the two WIPO Treaties.

C. CLASSES OF LEGAL PROTECTION

In addition to the significant latitude left to member states in constructing the TPM concept, the *WCT* and *WPPT* have also left room for the construction of several classes of legal protection.

For example, article 11 of the *WCT* does not require anti-circumvention measures to be integrated into copyright legislation. States therefore have a choice. Such measures could be dealt with in other kinds of legislation, such as

---

129. *Ibid.* Recall that access control TPMs are used to prevent persons from *gaining access* to digital works. Access control TPMs are thought to be the equivalent of a virtual lock on such works.

130. Many well-reputed academics disagree, arguing that the introduction of an access-control right to copyright law would be unprecedented. See *e.g.* Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised" (1999) 14 Berkeley Tech. L.J. 519 [Samuelson, "Intellectual Property"]. See also Koelman, *supra* note 99. Others, such as Ginsburg, characterize this access right as an evolution where, "the access right is an integral *part* of copyright, and therefore should be subject to exceptions and limitations analogous to those that constrain 'copy'-right." Jane C. Ginsburg, "From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law," online: Social Science Research Network Paper Collection <http://papers.ssrn.com/sol3/delivery.cfm/000421651.pdf?abstractid=222493> at 3; Jane C. Ginsburg, "From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law" in Hugh Hansen, ed., *U.S. Intellectual Property: Law and Policy* [forthcoming in 2003]. See also the CANCOPY submission to the Consultation on Copyright Reform in which it is argued that, "the lack of exceptions to technological measures would constitute a new 'access' right. The reality is that this merely provides the rightsholders with an effective means of controlling the distribution of their works in a digital environment so that they may be commercially exploited. This ability to control the distribution of a work has always been part of copyright." Canadian Copyright Licensing Agency "Submission of the Canadian Copyright Licensing Agency (CANCOPY) on Digital Copyright Issues," online: <http://www.accesscopyright.ca/pdfs/submissionpaper2.pdf> at 11. The policy implications of a new right of access-control will be further addressed below.

criminal law or competition law.[131]

As well, article 11 is silent with respect to the type of anti-circumvention measures that can be used to achieve compliance. Because *WCT* article 11 merely requires a contracting state to prevent circumvention through "adequate legal protection," the form of legal protection could conceivably consist of a prohibition against acts of circumvention, a prohibition against trafficking in circumvention devices or a prohibition against both types of activities. Anti-circumvention measures might be understood to fall generally into four classes: general access control measures, limited access control measures, use control measures and anti-device measures.[132]

VII. Philosophical Considerations

HAVING ANALYZED THE TPM CONCEPT and having determined that a decision to implement this concept into domestic law would require Canada to choose from a number of classes of legal protection, it seems appropriate to briefly situate the ensuing policy discussion in a broader philosophical context.

As is well known, Canadian copyright law borrows from both the Anglo-American and Continental traditions of intellectual property. Much ink has been spilled on the influences of each and it is therefore unnecessary to give a full account here.[133] For our present purposes, it is less crucial to grasp the subtle differences between these two systems than it is to see the posture of their stance. To employ a rather crass and oversimplified mnemonic: we borrow from the Europeans the perspective of the creator of a work; from the Anglo-Americans, the perspective of the society for whom it was created.[134]

This age-old juxtaposition, which no doubt has its roots in the clash of traditions between Kant and Mill, has been post-modernized in the recent public debates between Lawrence Lessig and Jack Valenti.[135] The historical tensions have

---

131. de Werra, *supra* note 11 at 12–13. For example, Japan has elected to adopt circumvention device provisions within its *Anti-Unfair Competition Law*, as discussed below in Part X.B. Of course, these provisions could also be dealt with in multiple legal regimes.

132. Each of these measures and their respective implications will be analyzed in Part IX.

133. See *e.g.* W.L. Hayhurst, "Intellectual Property Laws in Canada: The British Tradition, the American Influence and the French Factor" (1996) 10 I.P.J. 265; M. Goudreau, "Le droit moral de l'auteur au Canada" (1994) 25 R.G.D. 403; Ysolde Gendreau, "Moral Rights" in Gordon F. Henderson *et al.*, eds. *Copyright and Confidential Information Law of Canada* (Toronto: Carswell, 1994) 161; David Vaver, *Copyright Law* (Toronto: Irwin Law, 2000) at 12; David Vaver, *Intellectual Property Law: Copyrights, Patents, Trade-Marks* (Concord: Irwin Law, 1997); Sunny Handa, *Copyright Law in Canada* (Markham: Butterworths Canada, 2002) at 28–40, 62–69, 369–387; H.G. Fox, *The Canadian Law of Copyright* (Toronto: University of Toronto Press, 1944) at 12–32; Mikus, *Droit de l'edition et du commerce du livre* (Montréal: Éditions Thémis, 1996); R.J. DeSilva, "Droit Moral and the Amoral Copyright: A Comparision of Artists' Rights in France and the United States" (1980) 28 Bull. Copyright Soc'y 1; Jane C. Ginsburg, "A Tale of Two Copyrights: Literary Property in Revolutionary France and America" (1990) 64 Tul. L. Rev. 991; Roberta Rosenthal Kwall, "Copyright and the Moral Right: Is an American Marriage Possible?" (1985) 38 Vand. L. Rev. 1; R. Monta, "The Concept of 'Copyright' Versus the 'Droit d'Auteur'" (1959) 32 S. Cal. L. Rev. 177; E. Damich, "The Right of Personality: A Common-Law Basis for the Protection of the Moral Rights of Authors" (1988) 23 Ga. L. Rev. 1; Jane C. Ginsburg, "French Copyright Law: A Comparative Overview" (1989) 36 J. Copyright Soc'y 269.

134. See *e.g.* Monta, *ibid.*

135. See "The Future of Intellectual Property on the Internet," online: The Berkman Center for Internet & Society at Harvard Law School <http://cyber.law.harvard.edu/futureofip/>.

been recast and are perhaps best articulated in the clever quip of one of the MIT Media Lab's brightest lights, Stewart Brand, who gave us the following paradox. The first half of Brand's slogan is well known and has been touted on a variety of virtual bumper stickers across the Infobahn: "*Information wants to be free.*"

But, as John Perry Barlow once pointed out, very few people are aware of the entire passage:[136]

> Information wants to be free. Information also wants to be expensive. Information wants to be free because it has become so cheap to distribute, copy, and recombine—too cheap to meter. It wants to be expensive because it can be immeasurably valuable to the recipient. That tension will not go away. It leads to endless wrenching debate about price, copyright, 'intellectual property,' and the moral rightness of casual distribution, because each round of new devices makes the tension worse, not better.[137]

Despite having been written some 15 years prior to the date of this article,[138] Brand certainly was able to see, if not help to invent, our future. The tension around our "newest round of devices" is palpable. Such tensions, as Barlow has characterized them, are the "dreams of building fences around a tornado...."[139] Barlow went on to describe the strategy underlying TPMs as a proposal "that all new intellectual creations will be put in cryptographic bottles."[140] What Barlow (and perhaps even Brand) had not anticipated was that the technological capacity of TPMs could go on working indefinitely, "thus transforming a market where wine is sold in bottles from which everyone may drink infinitely—as is the case with books—into a market where all wine is sold by the sip. Forever."[141]

Thus, the ensuing policy issue is not merely a question of copyright's ability to balance but also one of technology's power to control. How can copyright's tripartite balance between the rights of creators, owners, and the public be maintained in an architecture that promises copyright owners complete control and the facility—as never before seen—to unbundle copyright into such discrete parcels?

Each of the various stakeholders may appeal to different aspects of copyright's intricate web. Content creators would appeal to the Continentalist's

---

136. Apparently this includes Barlow himself who, when discussing the passage at an online roundtable, cited a penultimate version of the now classic text, see John Perry Barlow, "Life, Liberty and the Pursuit of Copyright, Round Two: Response," online: The Atlantic Online <http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm>.

137. Stewart Brand, *The Media Lab: Inventing the Future at MIT* (New York: Viking Penguin, 1987) at 202.

138. This article is being written at a time when the shelf life of a classic work seems to have become about 3 years.

139. Barlow, *supra* note 136 at para. 2.

140. *Ibid.*

141. *Ibid.* at para. 6. Of course, the idea that a digital work might be protected indefinitely undermines the time-limited protection afforded by copyright law and, as Lessig has described, it is tantamount to "hardwiring the legal regime into the technology..." Lessig, *Code*, *supra* note 66 at 139.

doctrine of moral rights,[142] in particular, to the right of integrity.[143] Under a moral rights view, they would say, the creators of original works ought to have some ability to control the use of those works—not merely because their financial livelihoods depend on it but, also because of the ease with which a digital work can be unbundled. The unbundling of a digital work threatens the integrity of the work and poses serious challenges for those creators who wish to ensure that elements of their work are given proper attribution. As such, the personality and reputational rights of authors, which are so deeply and inextricably tied to the products of their creation, are in jeopardy. The TPM strategy does not, in theory, pose a direct threat to creators. In fact, use control TPMs *could* be used by creators to restrict uses of a work in a manner that protects their moral rights. However, the practical commercial and industrial realities are that content owners, usually corporate entities, are the ones in a position to implement TPMs and do so primarily for their own benefit.

Content owners may appeal to aspects of the Anglo-American tradition and its reliance on social utility and economics as a means of justifying their control over the uses of digital works. They would argue that a vigorous protection of copyright is necessary to maximize social utility. Protecting rightsholders against infringement, they would argue, facilitates the production and dissemination of information, which results in technological progress, thereby producing a better-informed and more knowledgeable society and, ultimately, a more participatory democracy—all of which will to lead to progress in our civilization.[144] As one of Canada's finest copyright scholars very recently reminded us, copyright is also, "a *strategic industrial right* that allows key cultural industries, such as book and music publishing, record production, computer software programming, and film production to grow."[145] According to content owners, the legal protection of TPMs is required to level the playing field, which was drastically altered once it became possible to encode various kinds of information into digital form, duplicate the digital content without loss of fidelity, and transmit it to incredible numbers of recipients worldwide at negligible incremental cost. In the wired world, once control over access is lost, it is next to impossible to ensure the legitimate and authorized use of digital content.

Users would also appeal to various philosophical underpinnings of copyright law to protect their interests, including the foundational notion that copyright does not provide a monopoly on ideas but only affords a time-limited protection to the expression of those ideas under specifically prescribed circumstances. Once the legislated period of protection has elapsed, the work, free as air, enters the public domain. These fulcrums of copyright law are founded on the

---

142. See generally *supra* note 49. See also Vaver, *Copyright Law*, *supra* note 133 at 158–168; Handa, *supra* note 133 at 63–69, 369–386. See also Jacqueline Lipton, "Copyright in the Digital Age: A Comparative Study" (2001) 27 Rutgers Computer & Tech. L.J. 333 at 335. Lipton describes the Continental system as a "tradition [that] sees copyright as springing from the personality rights or the individual creator of the subject matter. Companies and organisations [sic] as such cannot be creators. Copyright is thus rooted in protection of the individual personality and interests of the author as expressed in her work."

143. Vaver, *ibid.* at 161–64; Handa, *ibid.* at 380–81.

144. See Vaver, *ibid.* at c. 1; Handa, *ibid.* at 119.

145. See Gervais, *Collective Management*, *supra* note 72 at para. 6.

recognition that "when copyright gives control to one person, it extracts some measure of freedom to imitate from everyone else."[146] From a user perspective, when copyright gives control to creators or publishers of works, it takes away from potential users the freedom to browse, freedom to read, freedom to learn, freedom to teach, freedom to participate in social and political decision-making, and a number of other crucial aspects of any open society that cherishes free expression.

Many advocates of the user perspective have expressed a concern that the strategy of TPMs, if realized, would mean the death of libraries. This would drastically alter the social strata of an information society since libraries are, as Carnegie once put it:

> ...the best agencies for improving the masses of the people, because they give nothing for nothing. They only help those who help themselves. They reach the aspiring, and open to these the chief treasures of the world—those stored up in books.[147]

Barlow, well known as an advocate of the user perspective, describes TPMs as a system that would "informationally pauperize those who were already economic paupers and would greatly amplify and permanently institutionalize the adage that 'the rich get richer'."[148] According to Barlow, "[i]t would also make a private garden of the ecology of ideas, robbing us all of the new wealth of ideas that might [be] built by the poor from the compost of those previous thoughts to which they would no longer have access."[149] To the extent that TPMs transform digital environments from architectures of freedom to architectures of control, users will argue that TPMs upset the balance that copyright law seeks to achieve.

Because Canadian copyright law postures itself, at times in the Continental tradition and at other times in the Anglo-American tradition, it is not immediately obvious which of the above appeals ought to be received most sympathetically. Our courts have recently paid some attention to both.

For example, our courts have addressed the central role of author's rights or moral rights on several occasions.[150] In the recent decision of *Desputeaux c. Éditions Chouette (1987) inc.*,[151] the Quebec Court of Appeal wrote:

---

146. Goldstein, *supra* note 1 at 6.

147. Andrew Carnegie quoted in Timothy Rub, "The Day of Big Operations: Andrew Carnegie and His Libraries" (1985) 173:8 Architectural Record 81 at 81.

148. Barlow, *supra* note 136 at para. 7.

149. *Ibid.*

150. Decisions recognizing the role of moral rights in Canadian copyright include *CCH Canadian Ltd. v. Law Society of Upper Canada*, [2000] 2 F.C. 451, 179 D.L.R. (4th) 609, rev'd (2002), 18 C.P.R. (4th) 161 (F.C.A.), 212 D.L.R. (4th) 385; *Bishop v. Stevens*, [1990] 2 S.C.R. 467, 72 D.L.R. (4th) 97; *Snow v. Eaton Centre Ltd.* (1982), 70 C.P.R. (2d) 105 (Ont. H.C.).

151. [2001] R.J.Q. 945 at paras. 35–36, 16 C.P.R. (4th) 77, leave to appeal to S.C.C. granted (2002) 285 N.R. 397. This decision will likely receive much attention by copyright academics as motion for leave to appeal to the Supreme Court has been granted. It will be interesting to see whether this strong moral-rights rhetoric will be used by the Supreme Court or whether a more balanced approach will emerge.

> Le droit d'auteur est reconnu comme bi-frontal, droit de la personnalité et droit pécuniaire. L'oeuvre protégée par le droit d'auteur est, en effet, à la fois une émanation de la personnalité de l'auteur et une source d'intérêts é[c]onomiques. Une oeuvre n'est pas seulement un produit que l'on peut vendre, c'est le résultat d'un acte de création personnelle. L'auteur communique sa pensée, ses émotions de sorte que l'oeuvre fait partie de la personnalité de l'auteur et lui demeure attachée toute sa vie.
>
> La *Loi sur le droit d'auteur* protège, sous le titre «*Des droits moraux*» cet aspect éminemment personnel du droit d'auteur.

On the other hand, and even more recently, the Supreme Court of Canada not only reiterated the need for a balanced approach but also emphasized the importance of the public domain in incorporating and embellishing creative innovation:

> The proper balance among these and other public policy objectives lies not only in recognizing the creator's rights but in giving due weight to their limited nature. In crassly economic terms it would be as inefficient to overcompensate artists and authors for the right of reproduction as it would be self-defeating to undercompensate them. Once an authorized copy of a work is sold to a member of the public, it is generally for the purchaser, not the author, to determine what happens to it.
>
> Excessive control by holders of copyrights and other forms of intellectual property may unduly limit the ability of the public domain to incorporate and embellish creative innovation in the long-term interests of society as a whole, or create practical obstacles to proper utilization. This is reflected in the exceptions to copyright infringement enumerated in ss. 29 to 32.2, which seek to protect the public domain in traditional ways such as fair dealing for the purpose of criticism or review and to add new protections to reflect new technology, such as a limited computer program reproduction and "ephemeral recordings" in connection with live performances.[152]

Some Canadian scholars believe that the Supreme Court of Canada's philosophical considerations in *Théberge* ought to influence the Canadian treatment of TPMs. A leading Canadian internet law scholar has even gone so far as to say that:

> [b]y sending a clear message about its support for a fair copyright balance, the Supreme Court has indirectly provided the most important submission on the current digital copyright reform consultations. The Court has begun to sketch the limits of copyright protection—those limits include recognizing the rights of users as well as the fact that more copyright protection does not necessarily foster more creativity and innovation.[153]

---

152. *Théberge v. Galerie d'Art du Petit Champlain Inc. et al.* (2002), 210 D.L.R. (4th) 385 (S.C.C.), 285 N.R. 267 at paras. 31–32, 34 [*Théberge*].
153. Michael Geist, "Key Case Restores Copyright Balance" *The Globe and Mail* (18 April 2002), online: globeandmail.com <http://www.theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20020418/TWGEIS>.

VIII. Affording Legal Protection to TPMs

AS INDICATED AT THE OUTSET, rights owners of digital content are increasingly turning to the use of TPMs and DRMs to enforce and protect their rights and to ensure authorized uses. In fact, many copyright holders[154] claim that the existing laws *are not adequate* to prevent the massive illegal dissemination of digital works that takes place off and online everyday. Consequently, creators and content owners argue that legal protection of TPMs is required and that Canada ought to implement laws that make it illegal to circumvent TPMs or to traffic in circumvention devices.

In response to these claims and to the obligations called for in the *WCT* and *WPPT*, several scholars have underscored the fact that currently no empirical data exists suggesting that the legal protection of TPMs is warranted.[155] Part of the problem for policy makers and legislators is that the demand and supply characteristics of the new markets for TPMs and other digital information products remain as yet unknown. TPM and DRM technologies are still in relatively early stages of development, and new business models for the delivery of digital information products are still being beta-tested. Moreover, state of the art TPMs are still unable to distinguish between infringing and non-infringing uses. Consequently, TPMs are currently unable to provide selective access to works in situations in which such access would not result in copyright infringement.

Given all of the above, it is perhaps too early to predict whether the legal protection of TPMs is in fact necessary to the success of mass markets for digital works. It is perhaps also too early to determine whether the failure to adopt such measures would ultimately prove to be injurious to such markets. In fact, we do not even know whether the legal protection of TPMs might actually undermine the very aim of the TPM strategy by retarding the research and development of newer, more secure TPMs and other innovative means of distributing digital information products, thereby leading to sub-optimal consumption.

TPMs and DRMs currently allow works to be controlled by copyright owners and other rightsholders in a manner and to a degree not previously contemplated by copyright law. TPMs allow rightsholders to exercise a significant degree of control over the access and terms of use of digital works. Additionally, rightsholders are further able to exert a degree of control over the use of their works through contractual arrangements, such as licensing.[156] Such contractual regimes are often built into DRMs. As previously indicated, the use of TPMs, coupled with the ability to set licensing terms, could result in a transfer of control in defining permitted uses of works from the public rules established by Parliament under the *Copyright Act*[157] to the private decrees of rightsholders. All of

---

154. Including a number of very large, powerful corporations.

155. Koelman & Helberger, *supra* note 10 at 221.

156. See Hugenholtz, "Public Domain", *supra* note 70 at 79–80. The author describes the growing trend in the distribution of copyright works, whether they are digital books or software, to limit the terms of use through licensing arrangements. See also Lucie M.C.R. Guibault, "Contracts and Copyright Exemptions" in Hugenholtz, Copyright Management, *supra* note 10 at 125; Gervais, *Collective Management*, *supra* note 72.

157. R.S.C. 1985, c. C-42.

this may have serious implications for consumer privacy, freedom of expression, and may upset the historical balance created by copyright as set out above.

A. EXISTING LAYERS OF PROTECTION FOR COPYRIGHT HOLDERS

Copyright owners currently have three available methods of assuring authorized access to their works: TPM and DRM technologies; existing copyright law; and the law of contract.

1) TPM and DRM Technologies

The first layer of protection is the ability to restrict access to or the use of a work through technology. As we have seen, TPMs have been constructed to serve as technological fences operating as a layer on top of the legal protection afforded by existing copyright law.[158] As we have already revealed, TPMs can be circumvented and the frequency of this possibility is rapidly increasing. Consequently, it is presently unclear how widely the TPM strategy will ultimately be adopted and whether new TPM architectures[159] will be more resistant to circumvention on a large scale without an additional layer of legal protection of the sort contemplated in the *WCT* and *WPPT*. At the same time, it is important to remember that DRMs utilize TPMs in conjunction with other existing legal instruments, such as contracts and licensing schemes.[160]

2) Copyright Law

Copyright law already protects digital works so long as the underlying work satisfies the applicable tests.[161] Consequently, the circumvention of a use control TPM will result in an actionable copyright infringement. The same will be true for some access control TPMs, so long as the digital content protected by the TPM is subject to copyright and its circumvention results in some kind of copying not subject to the exceptions provided by copyright law.

Additionally, software-based TPMs may themselves be protected under the *Copyright Act*. As Dusollier explains:

---

158. In this regard it should be noted that software-based TPMs and works enfolded in TPMs might be works entitled to copyright protection. It is also important to reiterate that some TPMs are being used to extend the term of copyright forever, *i.e.* "lock-up" works that are or will be in the public domain.

159. Newer architectures include features such as 'renewal' and 'revocation'. These features are discussed in Part IV. See also Koelman & Helberger, *supra* note 10 at 221.

160. Hugenholtz, "Public Domain", *supra* note 70 at 84.

161. In order for a work to enjoy copyright protection in Canada, three requirements must be met: i) the work must be original; ii) the work must be fixed; and iii) the work must be connected to Canada (or to a World Trade Organization, Berne or Universal Copyright Convention member state). The test for whether a work is subject to copyright protection formerly involved a "skills and labour" test. There has, however, been a shift to an "originality" test. For a detailed discussion of this shift, see Handa, *supra* note 133 at 217-219.

> [w]hen the technical protection measure that prevents copying, accessing the work or ensures its authentication, is a computer program, hacking it could constitute an infringement of the copyright vested in the software. Tampering with the protective mechanism could arguably imply a reproduction, even if transient, of the software.[162]

In the Canadian context, the *Copyright Act* allows a single reproduction of a computer program provided that the person owns a copy of the computer program.[163] Thus, it could be argued that where a person owns a copy of a software-based TPM, they may be entitled to "tamper" with it. However, the ability to circumvent or tamper with the TPM would be subject to the restrictions contained in section 30.6 of the *Copyright Act*, as well as to the terms of applicable software licences. Thus, tampering or circumventing in a manner contrary to the restrictions imposed by the *Copyright Act*, or the terms of the licensing agreement, may result in an actionable copyright infringement. In this sense, it could be said that the act of circumventing a TPM already falls within the ambit of protection afforded under the *Copyright Act*.

3) Contract Law

Contract law is yet another layer of protection available to copyright holders. Copyright holders are able to set the terms of use through licences. Such licences are often incorporated into DRMs. The use of DRMs can facilitate the automatic 'negotiation' of contracts between content providers and users. In this environment, the bargaining power between the content providers and users may well be unequal.[164] The combined use of TPMs and contracts in this manner could therefore lead to unconscionable transactions. As some commentators have expressed:

> Are we heading for a world in which each and every use of information is dictated by fully automated systems? A world in which every information product carries with itself its own unerasable, non-overridable licensing conditions? A world in which what is allowed and what is not, is no longer decided by the law but by *computer code*?[165]

> Where technological constraints substitute for legal constraints, control over the design of information rights is shifted into the hands of private parties, who may or may not honor the public policies that animate public access doctrines such as fair use. Rightsholders can effectively write their own intellectual property statute in computer code.[166]

User licences are becoming the rule and content providers are, with increasing frequency, using the terms of these licences to override existing

---

162. Séverine Dusollier, "Situating Legal Protections for Copyright-Related Technological Measures in the Broader Legal Landscape: Anti-Circumvention Protection Outside Copyright" (General Report presented to the ALAI Congress, June 2001)[unpublished], online: ALAI 2001 Congress <http://www.law.columbia.edu/conferences/2001/Reports/GenRep_ic_en.doc> at 15.
163. *Supra* note 157, s. 30.6.
164. Hugenholtz, "Public Domain", *supra* note 70 at 79.
165. *Ibid.* at 86–87.
166. Dan L. Burk & Julie E. Cohen, "Fair Use Infrastructure for Rights Management Systems" (2001) 15 Harv. J.L. & Tech. 41 at 51.

copyright limitations.[167] Indeed, this is quickly becoming an area of much debate and academic work.[168] To what extent may the terms of a licence override statutory copyright exemptions? As Guibault so aptly articulates:

> Concerns arise from the possibility that an unbridled use of technological measures coupled with anti-circumvention legislation and contractual practices would permit rights owners to extend their rights far beyond the bounds of the copyright regime, to the detriment of users and the free flow of information. The copyright bargain reached between granting authors protection for their works and encouraging the free flow of information would be put in serious jeopardy if, irrespective of the copyright rules, rights owners were able to impose their terms and conditions of use through standard form contracts with complete impunity. If this were the case, the copyright regime would succumb to mass-market licences and technological measures. Unless the legislator clarifies the issue, these concerns may become all too real with the gradual implementation of electronic copyright management systems, whose workings are based on technology and contractual relations, with the generalisation of mass-market licences as the main vehicle for transactions in information....[169]

The protection already afforded to copyright owners by virtue of the existing three layers of protection begs the question of whether an additional layer of legal protection is required.

B. TWO POSSIBLE RESPONSES

The above analysis suggests that there is no clear trajectory favouring the strategy of legally protecting TPMs at this early stage in its development. This suggestion leads to one of two possible responses from which Canada might choose.

First, Canada could choose not to confer additional legal protection to TPMs and simply allow them to flourish or fail in an unregulated environment until such time as there is more compelling evidence of a need to legislate. There are a number of reasons against affording additional legal protection to TPMs at this time. First, as explained above, copyright holders already enjoy multiple layers of protection. Second, as previously indicated, it is not yet known how the information market will develop. Although the open architectures of the internet originally seemed to tip the balance in favour of the public interest in access to works, the shifting architecture of the net and the use of TPMs may yet provide more advantages than disadvantages to content owners, due to lower costs of distribution and a potentially decreasing need to enforce copyright. Third, if the legal protection of TPMs interferes with the public interest in access to works as traditionally defined, it is difficult to explain why these fundamental rights should carry less weight in the digital environment than in others. Fourth, affording legal protection may be of little consequence due to enforceability issues. Napster and other online phenomena demonstrate the difficulty in terms of sheer volume with

---

167. Hugenholtz, "Public Domain", *supra* note 70 at 80.

168. See *e.g.* Guibault, *supra* note 156. See also J.H. Reichman & Jonathan A. Franklin, "Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information" (1999) 147 U. Pa. L. Rev. 875.

169. Guibault, *supra* note 156 at 160.

policing the activities of each computer in the world.[170] This is further complicated by the increasing availability of newer and more sophisticated circumvention methods and devices. As Koelman has stated:

> If the protection of technological measures does not cure the problem it is supposed to solve, it could be argued that it should not be inserted. The difficult choice between the protection of the measures and maintaining the limits of copyright needs then not be made.[171]

The decision not to afford legal protection to TPMs could affect the possibility of Canada ratifying the WIPO Treaties. The chief consequence of such a decision is that Canada would be deprived of the reciprocal protection afforded by other states under the treaties in the area of copyright. It might be said, however, that such a choice would provide Canada with maximum flexibility in establishing a legitimate national policy when the appropriate time arrives, rather than offering an immediate response as a matter of mere expedience.[172]

Second, Canada could choose to provide some measure of "adequate legal protection." It is suggested that, if Canada ratifies the WIPO Treaties and legal intervention is to take place, legislative provisions should be designed to preserve to the greatest extent possible copyright's delicate balance between private rights and the public interest. It is further suggested that such legislative measures should also seek to promote the policy objectives for digital copyright already identified by the Government of Canada. These objectives are: the framework rules must promote Canadian values; the framework rules should be clear and allow, easy, transparent access and use; the framework needs to be cast in a global context; and the framework should be technologically neutral, to the greatest possible extent.[173]

IX. Possible Implementations of the WIPO Treaties

HAVING CANVASSED VARIOUS philosophical considerations and having examined the basic consequences of affording legal protections to TPMs, we are now in a position to elaborate on four potential classes of legal protection.

---

170. Koelman, *supra* note 99 at 3–4. See also Glynn S. Lunney, Jr., "The Death of Copyright: Digital Technology, Private Copying, and the *Digital Millennium Copyright Act*" 87 Va. L. Rev. 813 at 918–919: "In designing protection for the digital age, we must first determine whether the possibility of widespread private copying threatens the public interest in ensuring an adequate supply and distribution of creative work, or merely the private interest in maximizing the copyright industries' revenue."

171. Koelman, *supra* note 99 at 4.

172. Of course, it could be argued that the flipside of this same coin is that a failure for Canada to ratify now—on its own terms—could result in serious pressure from the US government and the powerful lobby of various multi-national corporate stakeholders to adopt domestic legislation similar to the *DMCA*, *supra* note 11. This legislation will be discussed in detail, below in Part X.D.

173. Industry Canada and Canadian Heritage, *Consultation Paper on Digital Copyright Issues* (Ottawa: Intellectual Property Policy Directorate, Industry Canada and Copyright Policy Branch, Canadian Heritage, 2001) at 13–15.

A. GENERAL ACCESS CONTROL MEASURES

Recall that a general access control measure prohibits *any* act that circumvents an access control TPM—irrespective of whether the TPM that has been circumvented functions to control a work subject to copyright and irrespective of whether the act of circumvention actually infringes copyright.

Traditionally, a copyright holder was not easily able to prohibit access to a work. The only way to prevent users from accessing a work was to keep the work private and, thus, unpublished. Once a work was published or disseminated to the public, the author lost the ability to control access to the work and, to some extent, its use. Thus, adopting a general access control measure into domestic law could be tantamount to the introduction of an 'access right.'[174] The introduction of an access-control right would be novel to copyright and is by no means required under articles 11 *WCT* or 18 *WPPT*.[175] Should there be an access-control right in digital works that would allow the rightsholder to control each time a work is accessed or should a work that has been legitimately accessed be accessible to the public?[176] The dilemma is well illustrated in the following statement:

> In the physical world, publication has three important characteristics: It is public, it is irrevocable, and it provides a fixed copy of the work. In the digital world, none of these may be true. In the physical world, publication is fundamentally public and irrevocable because, while the work does not become the property of the public, enough copies are usually purchased (*e.g.*, by libraries and individuals) that it becomes part of the publicly available social and cultural record. Publication is irrevocation because once disseminated, the work is available. Works may go out of print, but they are never explicitly taken "out of publication" and made universally unavailable; copies of printed works persist....
>
> Works published in electronic form are not necessarily irrevocable, fixed, or public. They can be withheld from scrutiny at the discretion of the rightsholder. Nor are they inherently public: Software enables fine-grained control of access, making works as open or as restricted as the rightsholder specifies, with considerable ability to fine-tune who has what kind of access.[177]

Access-control rights raise a number of difficulties, most importantly the question of how to achieve a balance between private rights and the public interest. Allowing copyright holders the ability to control how access is obtained and who is permitted access poses a threat to the public interest. In particular, creating an access-control right that is not accompanied by a robust and very carefully tailored set of exceptions will impact the public's ability to exercise the fair dealing defence and various statutory exceptions to copyright infringement and will have a broader impact on the bundle of rights falling under the banner of free

---

174. More precisely this could be termed *access-control right*, since it does not provide a right-of-access but rather the opposite—it allows access to be controlled. The policy implications of a new right of access will be further addressed below.

175. There is some debate whether such an access-control right would indeed be novel or whether the concept is merely evolutionary. This debate, however, may be more appropriately characterized as whether an access-control right is an appropriate extension of copyright law. See Thomas Heide, "Copyright in the E.U. and United States: What 'Access Right'?" (2001) Eur. I.P. Rev. 469.

176. See National Research Council, "The Digital Dilemma: Intellectual Property in the Information Age, Executive Summary" (2001) 62 Ohio St. L.J. 951.

177. *Ibid.* at 956-957.

expression. The implementation of an access-control right could potentially allow corporations that collect cultural content to prevent the legitimate use of a work. This type of prohibition could also have the stifling effect of denying access to works that are in the public domain or works which would otherwise be exempted by the fair dealing provisions under the current copyright regime. Since the combination of TPMs and contracts can already be used to prevent access to works that even exceptions to copyright permit, such as fair dealing, a legal prohibition on circumvention of TPMs that control access to public works, depending on how it is drafted, could further prevent the public from exercising existing rights.

The inclusion of a general access control measure that, by definition, is not accompanied by a robust and carefully tailored set of exceptions might also undermine free expression values.[178] In other words, an anti-circumvention provision that precludes individuals from accessing works (whether subject to copyright or not) might well interfere with self-fulfillment, the attainment of truth, participation in social and political decision-making, and the fostering of a tolerant and diverse society.[179] The prohibition of circumvention through a general access measure could significantly curtail freedom of expression, as it could provide an effective censorship tool for private organizations. For example, it is conceivable that a company or organization could utilize TPMs to deny certain individuals access to their sites and publications (even though those individuals or groups would otherwise be permitted access under the current copyright regime). Perhaps even more problematic would be situations where a TPM is designed to block access to targeted groups.

Thus, the net effect of a general access control measure is to provide a legal catalyst to what some scholars have referred to as the "second enclosure movement."[180] The first enclosure movement commenced in England during the 15th Century and lasted until the 19th Century. Its process involved fencing off common land and turning it into private property.[181] The second enclosure movement, say Boyle, Samuelson,[182] Lessig[183] and others, is happening now and involves the virtual fencing of the cyber-commons, by turning it into spaces controlled exclusively by private interests.

---

178. For a more detailed articulation of the notion of free expression values, see *e.g. R. v. Keegstra*, [1990] 3 S.C.R. 697, [1991] 2 W.W.R. 1.
179. These principles were espoused in *Irwin Toy Ltd. v. Québec (A.G.)*, [1989] 1 S.C.R. 927 at 976, 58 D.L.R. (4th) 577.
180. See James Boyle, "The Second Enclosure Movement and the Construction of the Public Domain" (Paper presented to the Conference on the Public Domain at Duke Law School, November 2001), online: The Duke Law School Conference on the Public Domain <http://law.duke.edu/pd/papers/boyle.pdf>.
181. *Ibid.* at 1–3.
182. See Pamela Samuelson, "Digital Information, Digital Networks, and The Public Domain" (Paper presented to the Conference on the Public Domain at Duke Law School, November 2001), online: The Duke Law School Conference on the Public Domain <http://law.duke.edu/pd/papers/samuelson.pdf>.
183. Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Random House, 2001). See also Lawrence Lessig, "The Architecture of Innovation" (Paper presented to the Conference on the Public Domain at Duke Law School, November 2001), online: The Duke Law School Conference on the Public Domain <http://law.duke.edu/pd/papers/lessig.pdf>.

If TPMs are capable of being used to enclose spaces previously enjoyed by the public to achieve self-fulfillment, the attainment of truth, participation in social and political decision-making, and the fostering of a tolerant and diverse society, then the implementation of a general access control measure could well be contrary to section 2(b) of the *Charter*.[184] The promulgation of a general access control measure therefore runs the risk of being struck down as unconstitutional.[185] Although a law that infringes freedom of expression can be saved, pursuant to section 1 of the *Charter*,[186] this will only occur if the law is narrowly targeted, addresses a pressing concern, and is reasonable and proportionate to the objective.[187] It is questionable whether a law that indirectly creates a right of enclosure of public spaces would meet this test.

There are two main arguments in favour of the introduction of a general access control measure. One argument is that, in the absence of adequate protection, producers have little incentive to make content available in a digital form capable of networked distribution. Another argument has been made that the legislation must introduce both access control measures and anti-device measures, because relying solely on an anti-device measure renders the legal enforcement of copyright cumbersome and ineffective.

It is questionable whether the argument for implementing such measures on the basis that they would make copyright enforcement easier is justified at such an early stage in the development of the internet and the various technologies used to protect and circumvent digital works. It is unclear at the moment whether information sharing will ultimately be facilitated and fostered within the digital environment, whether information will be enclosed in domains subject to an owner's exclusive control, or whether a median will be negotiated between these two competing visions of our online future. It is early days. The market is too immature to draw any conclusions. Consequently, it is suggested that the scope and type of legal protection of TPMs should be determined in response to the *actual* development, use, and effects of TPMs and circumvention technologies, and should not be based on speculation.

Given the great likelihood that a general access control measure could drastically disturb copyright's delicate balance between private rights and the public interest—especially where issues of fair dealings and free expression are concerned—it is suggested this class of additional legal protection is unwarranted at this time. The introduction of an access-control right that, by definition, is not accompanied by a robust and carefully tailored set of exceptions is excessive and unnecessary.[188]

---

184. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [*Charter*]. S. 2 of the *Charter* provides, in part:
"Everyone has the following fundamental freedoms:
(b) freedom of thought, belief, opinion and expression, including the freedom of the press and other means of communication..."

185. Alana Maurushat, "Technological Measures in the Digital Era and Freedom of Expression: Global Anarchic Conversation or Global Monopolistic Conversion?" [unpublished, archived with the authors].

186. S. 1 of the *Charter* provides: "*The Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

187. *R. v. Oakes*, [1986] 1 S.C.R. 103, (1986) 26 D.L.R. (4th) 200.

188. This point will receive further elaboration in the discussion of the U.S. legislation in Part X.D.

B. LIMITED ACCESS CONTROL MEASURES

A limited access control measure places a *limited* prohibition against the circumvention of an access control TPM. A limited access control measure prohibits only *some* acts that circumvent an access control TPM. Unlike a general access control measure, it will protect an access control TPM *only if* the TPM functions to prevent access to a work subject to copyright. So long as the TPM prevents access to copyright protected works, a limited access protection measure would operate—even if the act of circumvention does not ultimately infringe copyright.

The advantage of adopting a limited access control measure is that its ability to exclude access is less pervasive. Since limited access control measures are targeted at the circumvention of TPMs that serve to protect works subject to copyright, such measures appear to be more rationally connected with the objectives of copyright law. While this may be true in theory, the practical benefits of limited access control measures are in fact illusory.

The illusion is multi-tiered. From a technological standpoint, the adoption of a limited access control measure will not prevent the possibility of using a TPM to deny access to a work not subject to copyright. At present, TPMs are unable to detect whether they are protecting works subject to copyright. Moreover, because any given technology can be used for more than one purpose, it would be difficult for a prosecutor or a judge to distinguish between a TPM, the purpose of which is to block access generally, and a TPM, the purpose of which is to block access only to protect copyright. Similarly, TPMs cannot distinguish between an infringing and non-infringing use. Given these important practical realities, the adoption of a limited access measure is problematic for the very same reason that a general access control measure is: both of these measures could indirectly introduce a new general access-control right *via* copyright law.

The chief difference between the two is that, in the case of a limited access control measure, one might devise a system of exceptions to the right of access-control with the aim of restoring the balance between private rights and the public interest. If such a system of exceptions could be devised, this difference would make the limited access control measure seem more appealing than a general access control measure. Again, its perceived appeal is quite possibly illusory.

It is important to understand precisely what such a system of exceptions would achieve. In essence, it would allow a person to circumvent an access control TPM under certain circumstances prescribed by statute.[189] This is unproblematic, so long as the person who wishes to exercise the fair dealing exception has the technological know-how to circumvent the TPM. Since most Canadians simply do not have such technological savvy, it would be difficult to imagine such a system of exceptions being practically available to the majority of Canadians in a manner that would actually restore the balance that would be upset if the right of access-control was introduced.

189. An example of this would be fair dealing.

C. USE CONTROL MEASURES

A use control measure places a prohibition against the circumvention of a use control TPM.[190] Usually, it is a prohibition against the circumvention of TPMs meant to control unauthorized copies of a work.[191] Such TPMs would determine whether the user is permitted to copy a work; if so, how many copies are permitted; and under what circumstances are copies permitted. A use control measure could have a significant advantage over access control measures because determinations regarding the nature of the work[192] could be made prior to circumvention. Such a measure would, at least in theory, be more compatible with copyright law than access control measures.

The argument in favour of use control measures is, however, somewhat tenuous. First, TPMs very often display both access control and use control characteristics. Caution must therefore be exercised when a legal measure is used to prevent the circumvention of a use control TPM, because the legal measure may end up protecting access control as well. Where use control TPMs have both access and use characteristics, the adoption of a use control measure will raise many of the same issues discussed above in the context of general and limited access control measures.

A prevalent form of use control technology is a DRM. As we have seen, a DRM consists of two components: a database containing information which identifies the content and rightsholders of a work, and a licensing arrangement which establishes the terms of use for the underlying work.[193] DRMs often include digital rights language software such as XrML. Use control technologies such as XrML have the ability to set licensing terms and the technological capability of controlling the uses of a work well beyond the boundaries of the copyright regime. DRMs may present the most significant problem in maintaining a balanced copyright regime. As Burk and Cohen observe:

> The copyright industries also have succeeded in obtaining extremely broad legal protection for rights management systems...
>
> The development of rights management systems powerfully demonstrates the ability of technology to regulate behaviour.... But as Larry Lessig and Joel Reidenberg have pointed out, technical standards are within the control of the designer and so confer upon the designer the power to govern behaviour with regard to that system...
>
> The design of technological rule sets, however, is not the sole provenance of the state; indeed, it is more often left to private parties. In the case of rights management systems, copyright owners determine the rules that are embedded into the technological controls. By implementing technical constraints on access to and use of digital information, a copyright owner can effectively supersede the rules of intellectual property law...

---

190. Use control TPMs are described in detail in Part II.C.
191. Use control TPMs also protect against other uses of a work such as the right of public performance or the right of distribution.
192. That is, whether it is subject to copyright.
193. See Gervais, *Collective Management*, *supra* note 72 at para. 10.

> The implications of these developments are stark: Where technological constraints substitute for legal constraints, control over the design of information rights is shifted into the hands of private parties, who may or may not honor the public policies that animate public access doctrines such as fair use. [194]

DRMs present formidable ways for copyright holders to control both the access to and use of their materials, even when users would be entitled to access works without infringing copyright. While it may be true that some users entitled to access digital works will be capable of circumventing DRMs, the vast majority of users do not have the inclination to circumvent such TPMs, nor do they possess the technical savvy. The potential power that copyright holders could have is practically unprecedented.

Use control measures additionally raise a number of privacy issues.[195] In Canada, as is the case elsewhere, some private copying is tolerated. This is largely because, in a free and democratic society, we do not wish our police to perform general monitoring of private activity. In the digital era, the concern is not with the police or government monitoring of private activity so much as it is with private industry monitoring activity through DRMs and other use control technologies. In some instances, use control technologies utilize surveillance or tracking means to monitor how a work is used as well as personal information about those who use a work. A legal prohibition of the circumvention of use control TPMs could potentially cause a serious intrusion into the privacy of individuals since the prohibition would make it illegal for a person to choose to disable mechanisms that track the usage of works in order to collect and transmit information about the personal attributes of users of such works.[196]

At the same time, privacy-enhancing technologies may be used to reduce or eliminate the collection of personal data.[197] The use of privacy-enhancing technologies to safeguard user privacy could in some instances be construed as an act of circumvention. Although any class of legal protection afforded to TPMs will have to be reconciled with privacy interests, the need for reconciliation would be amplified in the case of use control measures.

DRMs often incorporate use control technologies within their infrastructure. Many authorities believe that DRMs are becoming an industry standard, if they have not already become one.[198] The WIPO Treaties contain separate

---

194. Burk & Cohen, *supra* note 166 at 49–51 [footnotes omitted].

195. Lee A. Bygrave & Kamiel J. Koelman, "Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems" in Hugenholtz, Copyright Management, *supra* note 10 at 59.

196. It has been argued that the United States Constitution protects the right to read anonymously. See Julie E. Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace" (1996) 28 Conn. L. Rev. 981. For a general discussion of online anonymity in the Canadian context, see Ian R. Kerr, "The Legal Relationship Between Online Service Providers and Users" (2001) 35 Can. Bus. L.J. 419.

197. Bygrave & Koelman, *supra* note 195 at 95–97.

198. See Einhorn, *supra* note 86. See also Kaestner, *supra* note 86 at 39. This is a study prepared for the European Union. The author discusses many standardization activities in copyright protection. One initiative is the Document Objective Identifier (DOI). The DOI is an effort undertaken by 40 international publishing organizations, Association of American Publishers and the Alliance of European Music Rights Societies, to promote a standardized DRM.

obligations with respect to DRMs. Article 12 of the *WCT*[199] and article 19 of the *WPPT*[200] address the obligations of contracting states in the area of rights management information.

The purpose of these provisions is to prohibit the removal of DRM information from works, as well as the trafficking in works that have had DRM information removed or altered without authorization. When DRMs incorporate TPMs within their infrastructure, such as digital rights language software, they become, in effect, an advanced form of a TPM.[201] Thus, the legal protection of use control technologies may make DRMs subject to redundant protection.

It may be desirable to limit the scope of protection afforded to DRMs regardless of the type of anti-circumvention measure adopted. This could be done through either a narrow definition of a TPM, a narrow definition of a DRM, or a combination of these principles.

D. ANTI-DEVICE MEASURES

All of the legal measures discussed above prohibit the *act of circumvention* in one form or another. An anti-device measure, on the other hand, is a prohibition, usually of the manufacturing, distribution, and sale of devices that circumvent TPMs. Such measures are promulgated as a means of providing a higher-order deterrent

---

199. The provision reads:
(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:
(i) to remove or alter any electronic rights management information without authority;
(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.
(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

200. The provision reads:
(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty:
(i) to remove or alter any electronic rights management information without authority;
(ii) to distribute, import for distribution, broadcast, communicate or make available to the public, without authority, performances, copies of fixed performances or phonograms know ing that electronic rights management information has been removed or altered without authority.
(2) As used in this Article, "rights management information" means information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a fixed performance or a phonogram or appears in connection with the communication or making available of a fixed performance or a phonogram to the public.

201. Koelman & Helberger, *supra* note 10 at 169. According to these authors, "Advanced TMs of the latter type [control use technologies] may be qualified as full-blown 'Electronic Copyright Management Systems' (ECMSs). The term ECMS normally covers more than measures merely preventing access or use.... An ECMS would provide the complete infrastructure necessary for rights-holders to license directly users of copyrighted works."

to infringement. Not unlike the approach taken in the so-called 'War on Drugs'—which focuses on dealers and distributors rather than users—the prohibition of the manufacturing of and trade in devices that circumvent technological mechanisms operates on the premise that sanctioning acts of circumvention on a case-by-case basis is costly and ineffective. Consequently, some have argued that the only effective way to enforce the circumvention of TPMs is through a prohibition of circumvention devices.

Proponents of a broad prohibition of circumvention devices would argue that anything less than an absolute prohibition would be meaningless. Some have suggested more modest alternatives. Taking a narrower approach to prohibition, one might prohibit only the commercial sale of devices, the primary purpose of which is infringement. Alternatively, one might allow the sale of devices so long as a personal declaration has been made that the circumvention device is being sold for a non-infringing use. Proponents of an absolute ban have criticized this latter alternative as ineffective and tantamount to an honour system to prevent digital copyright infringement. They would say that one need look no further than the Napster phenomenon[202] to illustrate the futility of honour system approaches to copyright management. On the other hand, cases like Napster demonstrate a growing tendency on the part of government and our judiciary to legislate, prosecute, and resolve disputes against the social norm.[203] When a social norm is prevalent amongst the public, will legislation or a court decision ever be an effective method of promoting change? Essentially, legislators and courts face a difficult question as to how they wish to approach circumvention device prohibitions. Do they wish to rely on the honour system or adopt a common thief view of the public and enact restrictive legislation?

There are several other problems inherent in an anti-device measure. As indicated above, since the majority of the public does not possess the technical ability to circumvent TPMs, the right to circumvent a TPM under a fair dealing exception would be rendered empty. Another problem is that some devices subject to prohibition will also have legitimate and important functions unrelated to circumvention. A stethoscope can be used to monitor a heart in crisis or to crack a safe. Software devices can also serve dual or multi-purposes. From the perspective of policy, it is important to recognize that the prohibition of circumvention devices could also discourage capital flow to innovative technology, thereby impeding one of copyright law's primary goals, which is to secure and encourage innovation. Finally, and perhaps most important of all, a prohibition of the manufacturing of circumvention devices could have devastating implications for research and development and for national security. Prohibiting the making of such devices is sure to stifle research in the field of cryptography and other

202. *A&M Records, Inc. v. Napster, Inc.*, 239 F. 3d 1004 (9th Cir. 2001), 57 U.S.P.Q.2D (BNA) 1729.

203. Posner discusses the difficulty in enacting legislation that goes against accepted societal practices through an analysis of why people abide by tax law. See Eric A. Posner, "Law and Social Norms: The Case of Tax Compliance" (2000) 86 Va. L. Rev. 1781.

sciences that promote innovation. It will also stifle the research of various security applications.[204]

E. EFFECTIVE REMEDIES

The *WCT* and *WPPT* do not mandate whether implemented legislation must include civil or criminal sanctions in order to meet the "effective remedies" requirement. As discussed above, this affords substantial leeway as to how WIPO obligations may be fulfilled. Canada could therefore choose to limit its sanctions to civil remedies of the sort traditionally available to copyright litigants, such as injunctive relief,[205] compensatory damages,[206] punitive damages,[207] or statutory damages.[208] Alternatively, Canada could introduce quasi-criminal provisions to the *Copyright Act* through an anti-circumvention or anti-device measure. Another option would be to amend the relevant *Criminal Code* provisions, making circumvention a computer crime.[209] A combination of any of the above remedies is also a possibility. Some possibilities make more sense for anti-circumvention measures, while other possibilities make more sense for anti-device measures.

One of the chief conceptual difficulties in devising a scheme of effective remedies is the fact that the act of circumventing a TPM is usually distinct from the act of infringing the copyright it seeks to protect.[210]

In the context of civil sanctions, it is unclear what the appropriate remedy should be for circumventions unrelated to infringement since it is unclear whether any damages would be suffered. Presumably, some form of statutory damages would therefore be made available. It is unclear what goals such a sanction would achieve other than serving as a specific or general deterrent.[211] Given that the entire impetus of the relevant provisions of *WCT* and *WPPT* is to provide effective remedies to copyright owners whose TPMs have been undermined (at least it is in the civil context), it is unclear the extent to which non-remedial sanctions are appropriate. In any event, such a remedy is an unlikely choice given that we will suggest that anti-circumvention measures cannot be justified unless they are tied to infringement. Where the circumvention is tied to infringement, a different kind of conceptual problem arises. Given that the victim of a circumven-

---

204. *Universal v. Reimerdes*, *supra* note 28 (Brief of Amici Curiae at para. 1), online: Open Law <http://eon.law.harvard.edu/openlaw/DVD/crypto-amicus.html>: "The amici curiae are cryptographers, individuals whose work or hobby involves research, design, analysis, and testing of encryption technologies. *Amici* are concerned that Section 1201 of the *Digital Millennium Copyright Act* ("*DMCA*"), as construed by the District Court ... would deprive cryptographers of the most effective language in which to communicate their research and its results, with the effect of weakening security systems and technological protection of data for the public."
205. Injunctive relief aims at stopping ongoing acts of circumvention.
206. Compensatory damages aim at restoring the loss suffered as a result of circumvention/infringement.
207. Punitive damages aim at punishing the wrongdoer in a civil context.
208. Statutory damages aim at deterring wrongdoers from prohibited acts irrespective of or in lieu of actual damages.
209. R.S.C. 1985, c. C-46 (see *e.g.*, ss. 342.1, 342.2).
210. Setting aside, for the moment, the complex (and for the most part unrelated) issue of whether the process of circumvention infringes the copyright of the software code in the circumvented TPM (as opposed to infringing the copyright of the content that TPM was meant to protect).
211. Given that most circumvention of effective TPMs could not be accomplished by lay persons, circumventors would usually either be legitimate researchers and security analysts, or hackers motivated by illegitimate purposes.

tion that results in infringement is *already* entitled to remedies pursuant to copyright law and, in many instances, under the law of contract (pursuant to a licence), what need is there for an additional sanction?[212]

It has been suggested that sanctions be directed at the level of commercial rather than individual circumvention. This is a useful suggestion, not only from a deep pockets perspective but also because it might reduce the likelihood of cases such as *Sklyarov*, the Russian computer scientist who was thrown into an American jail for nearly five months after he was charged with trafficking in, and offering to the public, a software program that could circumvent technological protections on works subject to copyright when he arrived in the U.S. to deliver an article at a conference.[213]

In the Canadian context, it would likewise be possible to introduce a quasi-criminal provision. Such a provision could bear similarity to section 42 of the *Copyright Act*.[214] Alternatively, it could parallel the anti-circumvention provisions contained in sections 9 and 10 of the *Radiocommunication Act*.[215] Under this approach, the unauthorized trafficking in circumvention devices would be a criminal offence. Again, as a matter of policy, prosecutions could occur at the commercial level and not at the level of individual use of devices by individuals.[216]

A circumvention and anti-device provision could also be promulgated through the *Criminal Code* by amending the computer crime provisions. For example, an amendment could be made to the provisions on "unauthorized use of a computer,"[217] broadening the scope of this provision from "computer service" and "computer system" and extending it to include tampering with TPMs. In the *Consultation Paper on Digital Copyright Issues*, it was suggested that, "[i]n certain cases with commercial motivations, where the scale of circumvention has consequences for the copyright sectors as a whole, there should be appropriate criminal sanctions."[218] While it may be desirable to prevent the circumvention of TPMs where there are significant commercial implications, what would be an appropriate threshold for "commercial motivation" and "consequences for copyright sectors as a whole"? These are broad and vague statements that may not withstand constitutional scrutiny.

Criminal and quasi-criminal provisions raise a number of other particular concerns. For example, what level of *mens rea* would be required? The "knowingly" standard found in section 42 of the *Copyright Act* seems like an appropriate point of departure. But what exactly must be known? For an anti-circumvention

---

212. Perhaps there is the exception of additional injunctive relief in situations in which there are ongoing acts of circumvention.

213. It is, however, arguable that this kind of event could happen just as easily in a commercial context since Sklyarov's so-called illicit conduct was conducted in the course of his employment as will be the case with most research scientists. Sklyarov's case is discussed in detail in Part X.D.1 below.

214. *Supra* note 157, s.42.

215. R.S.C. 1985, c. R-2. S. 10(b) makes the trafficking in equipment that is used for the purpose of decrypting encrypted subscription programming signals without the authorization of the lawful distributor of the signal or feed a criminal offence. Ss. 9(b), (c), and (d) contain various prohibitions relating to unauthorized decryption. S. 18 provides a civil remedy as well.

216. This is the existing strategy for current prosecutions with respect to satellite and cable-TV descramblers. See generally *Radiocommunication Act*, *ibid.*

217. *Supra* note 209.

218. *Supra* note 173 at 24.

provision, is the required *mens rea* simply a knowledge requirement that X "knowingly circumvents a TPM"? Or is it a specific intent offence, that X "knowingly circumvents a TPM for the purpose of an infringing use..."? Of these possibilities, it is suggested that the latter is preferred as it ties the circumvention to infringement and offers a clear defence for scientific researchers as well as those permitted to gain access to the work under copyright law exceptions.

What about for an anti-device provision? Is the relevant offence the manufacture, trade (etc.) of a device, the purpose of which is to circumvent a TPM? Or is it the manufacture, trade (etc.) of a device, the purpose of which is to infringe copyright through the circumvention of a TPM? The problem with the former approach is that it is not tied to infringement. The problem with the latter approach is that legitimate manufacturers and distributors selling products with substantial non-infringing uses might be caught by such a provision if the TPM can also be used for infringing purposes. Even worse, illegitimate manufacturers and distributors might not be caught by such a provision if they are able to demonstrate that their products can be used for non-infringing purposes. As stated above, a stethoscope can be used to monitor a heart in crisis or to crack a safe. Software devices can also serve dual or multi-purposes.

If the purpose of a criminal provision is to deter members of society from infringing copyright, will a criminal prohibition against circumvention or trafficking in circumvention devices achieve this end? When one considers the recent Napster controversy and the continuing proliferation of satellite black boxes, the very idea of relying on criminal offences to achieve a deterrent effect for doing something that so many members of society do not believe is wrong raises difficulties, including a decrease in public respect for the law and an increase in the rate at which the law is transgressed.

One further consideration is the impact that criminal sanctions may have on the development of innovative technology. The potential stigma of a criminal charge may act to discourage capital flow from innovative technology and may deter new and important forms of computer programming, such as the development of open-source software.[219] It could also prevent high quality researchers from coming to Canada.

All of the above considerations lead to the suggestion that criminal sanctions ought to be avoided. Although they have the salutary effect of requiring more onerous proof of an intent to infringe and ought therefore to result in fewer legal actions, as discussed in further detail in Part VII, above, such provisions are subject to misuse, often resulting in a chilling effect on various important forms of social participation.

Policy makers should take into account that whatever measures are chosen, they should be mindful of the possible differences between what such policy measures purport to achieve and what they will *actually* achieve.

---

219. Software programs are often circumvented, analysed and modified so as to make them compatible and operable with different operating systems such as Linux. Such acts are currently permissible under the *Copyright Act*.

x. Legislative Responses in Other Jurisdictions

A NUMBER OF COUNTRIES have enacted legislation to implement their obligations under the WIPO Treaties, including Australia, Japan, the European Union, and the United States. These legislative regimes offer a variety of methods for implementing the *WCT* and *WPPT*. We will take a brief look at the legislative measures adopted in Australia, Japan and the European Union, and a more detailed review of the measures adopted in the United States.[220]

A. AUSTRALIA

Australia has implemented its WIPO Treaty obligations with respect to TPMs in a manner that favours the use of protected works.[221] Australia's amendments are contained in the *Digital Agenda Act*,[222] which amends the *Copyright Act of 1968*.

The *DAA* only prevents the trafficking in circumvention technologies.[223] Individuals who use such technologies are not targeted, nor is the act of circumvention itself.[224] However, the trafficking activities that are targeted include making a "circumvention device available online to an extent that will affect prejudicially the owner of the copyright."[225]

A limited number of exceptions to the anti-device provision exist. These exceptions include: reproducing computer programs to make interoperable products;[226] reproducing computer programs to correct errors;[227] reproducing computer programs for security testing;[228] copying by Parliamentary libraries for members of Parliament;[229] copying by libraries and archives for users;[230] copying by libraries or archives for other libraries or archives;[231] copying of works for preservation and other purposes;[232] and use of copyright material for the services of the Crown.[233] Interestingly, this is a closed list and does not include all possible uses falling under the fair dealing exception to copyright.[234]

In order to make sure that a circumventing device or service is really used for a permitted purpose, a person wishing to make such a use must provide the supplier of the device or service with a signed declaration containing information,

---

220. For a comprehensive analysis of the measures adopted by these nations see de Werra, *supra* note 11.
221. Pierre Sirinelli, "The Scope of the Prohibition on Circumvention of Technological Measures: Exceptions," trans. by Jane C. Ginsburg (General Report presented to the ALAI Congress, June 2001) [unpublished], online: ALAI 2001 Congress <http://www.law.columbia.edu/conferences/2001/3_reports_en.htm>.
222. *Copyright Amendment (Digital Agenda) Act 2000* (Cth.) No. 110, 2000 came into force on March 4, 2001 [*DAA*].
223. S. 10(1).
224. However, the *DAA* does prohibit attacks on TPMs concerning copyright management information if the work is copyright protected. See Sirinelli, *supra* note 221 at 11.
225. S. 116A(1)(b)(vi).
226. S. 47D.
227. S. 47E.
228. S. 47F.
229. S. 48A.
230. S. 49.
231. S. 50.
232. S. 51A.
233. S. 183.
234. Sirinelli, *supra* note 221 at 16.

such as the person's name and address, the basis of the exemption claimed, the name and address of the supplier, a statement that the device or service is to be used for a permitted purpose and identification of that purpose by reference to a specific section of the *Copyright Act*. "The declaration must also include a statement that the work or other subject-matter in relation to which the device or service is required is not readily available in a form not protected by a [TPM]."[235]

The Australian system is unique, but it is not yet clear if it will be workable since "[e]verything depends on the user's declarations."[236] Assuming the Australian approach is workable, it does have two significant limitations. First, there is no general exemption for fair dealing, so this mechanism does not solve the problem of users being able to circumvent in order to deal fairly with works for which they may well have lawfully obtained initial access. Second, this kind of a national verification system has severe limitations in a global environment. It can be expected that most devices for the circumvention of digital works will be made available primarily, if not exclusively, over the internet by entities that may be situated anywhere in the world. The automated methods used to obtain such devices are unlikely to accommodate the verification requirements of the Australian system. The net effect is that Australians may only be able to obtain such devices lawfully from Australian sources, thereby severely limiting the range of devices that can be acquired and, hence, the range of TPMs that can be circumvented.

B. JAPAN

Japan has amended two statutes to address the circumvention of TPMs for the purpose of complying with the WIPO Treaties. The two statutes are the *Japanese Copyright Law*[237] and the *Japanese Anti-Unfair Competition Law*.[238] The amendments to the *JCL* focus on the circumvention of TPMs protecting works subject to copyright, whereas the amendments to the *JAUCL* focus primarily on the circumvention of access control technologies.[239]

---

235. de Werra, *supra* note 11 at 39.
236. Sirinelli, *supra* note 221 at 16. The International Intellectual Property Alliance has also criticized the DAA on similar grounds and has sought to have Australia maintained on the U.S. Special 301 Watch List. See *International Intellectual Property Alliance 2000 Special 201 Report, Executive Summary*, online: International Intellectual Property Alliance <http://www.iipa.com/rbc/2000/AUSTRALIA_2000.PDF>. The Special 301 Watch List contains the names of those countries that, in the opinion of U.S. authorities, deny adequate and effective protection for intellectual property rights, or deny fair and equitable market access for persons that rely on intellectual property protection resulting in (actual or potential) adverse impact on relevant U.S. products. Countries on the list are potentially subject to investigation and trade retaliation on the part of the U.S. See 1994 Annual Report, Special 301, online: Office of the United States Trade Representative <http://www.ustr.gov/html/1994_special301.html>.
237. See the *Japanese Copyright Law*, Law No. 48, promulgated on May 6, 1970 as amended by Law No. 77, June 15, 1999 [*JCL*].
238. *Japanese Anti-Unfair Competition Law*, Law No. 47, promulgated on May 19, 1993 as amended by Law No. 33, April 23, 1999 and Law No. 160, December 22, 1999). See de Werra, *supra* note 11 at 33–34. The amendments made to the *JCL* and to the *JAUCL* both came into force on October 1, 1999.
239. However, the *JAUCL* does also implement technological measures controlling the use of the works (i.e. copy control).

The *JCL* does not outlaw the act of circumvention;[240] it prohibits trafficking in circumventing technology.[241] The only legal remedy provided for a violation is criminal. The test relating to the function of the device used for circumvention is based on whether or not the device has a "principal function for the circumvention of technological protection [measures.]"[242] Such a test, like its Australian counterpart, might be difficult to apply. The *JCL* anti-device measure only prohibits trafficking in anti-copy devices and related businesses.[243] Interestingly, the manufacturing of such equipment does not appear to be prohibited. The *JCL* does not address access circumvention at all. Thus, for example, selling a pay-TV decoder will not attract any liability under the *JCL*. That is something that the *JAUCL* addresses instead.[244]

The *JAUCL* includes only anti-device measures and does not prohibit the act of circumvention itself.[245] Interestingly, once again, the manufacturing of circumvention equipment does not appear to be prohibited.

Japanese law strives to keep access and copying separate as much as possible. So far this has occurred in two ways: firstly, the interactive transmission of material subject to copyright *via* the Internet, is treated as a transmission by the person who transmits the work and not as an acquisition (or access) of customized information by the public.[246] Second, the Tokyo District Court has held that temporary or ephemeral storage, such as that which occurs in a computer's random access memory, is not a reproduction in tangible form since it is not a reproduction that will be used repeatedly in the future.[247]

240. See *JCL*, art. 2.
241. de Werra, *supra* note 11 at 34.
242. *Ibid.*
243. Naoki Koizumi, "The New or Evolving 'Access Right'" (Paper presented to the ALAI Congress, June 2001) [unpublished] at 1, online: ALAI 2001 Congress <http://www.law.columbia.edu/conferences/2001/1_program_en.htm>.
244. *Ibid.* at 2.
245. *JAUCL*, *supra* note 238, art. 2.
246. *Ibid.*, art. 3.
247. *Ibid.*

C. THE EUROPEAN UNION

The European Union (EU) adopted its *Directive on the harmonization of certain aspects of copyright and related rights in the information society*[248] in order to implement most of the provisions of the *WCT* and *WPPT*. In reviewing the *Copyright Directive*, it is important to remember that the role of EU Directives is to harmonize the national laws of Member States by setting objectives without imposing means.[249] The means employed are left to each Member State. Therefore, it is not surprising that the *Copyright Directive* is not nearly as detailed in its drafting as say, the American legislation.[250] Nevertheless, the *Copyright Directive* remains a convoluted document.[251]

The European definition of TPMs outlines what are essentially two major requirements: i) that the measure be designed to *prevent copyright infringement*, and ii) that the measure be *effective*.[252] The *Copyright Directive* prohibits the act of circumvention.[253] Unlike the U.S. approach, discussed below, contravention of the above provision requires an element of intention. Due to the fact that it is

248. EC, *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society*, [2001] O.J.L. 167/10 [*Copyright Directive*]. This directive was adopted by the European Parliament on February 14, 2001 and subsequently by the Council of Europe on April 9, 2001, followed by a consolidated version of the *Copyright Directive* released on May 22, 2001. It came into force on June 22, 2001 and EU Member States have 18 months from that date to implement it into national legislation. See also de Werra, *supra* note 11 at 25 (including notes 122, 123 and 124) and Maria Martin-Prat, "The Scope of the Legal Protection of Technological Measures (Access Control/Rights Control) in the EU Directive on Copyright and Related Rights in the Information Society: The Relationship Between Such Protection and Exceptions to Copyright and Related Rights" (Paper presented to the ALAI Congress, June 2001) [unpublished] at 1 online: <http://www.law.columbia.edu/conferences/2001/0_entrance_en.htm>. There are two other EU directives that address anti-circumvention of TPMs: (1) EC, *Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs*, [1991] O.J.L. 122/42; and (2) EC, *Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access*, [1998] O.J.L. 328/54. However, it should be noted that neither of these was passed for the specific purpose of implementing the EU's TPM-related obligations under the WIPO Treaties. Therefore, these Directives are not discussed further in this article.

249. Martin-Prat, *ibid.* at 1.

250. de Werra, *supra* note 11 at 26.

251. Martin-Prat, *supra* note 248 at 8. See also P. Bernt Hugenholtz, "Why the Copyright Directive is Unimportant, and Possibly Invalid" (2000) 22 Eur. I.P. Rev. 499 at 500 [Hugenholtz, "Copyright Directive"], where the author describes the *Copyright Directive* "... as a badly drafted, compromise-ridden, ambiguous piece of legislation. It does not increase 'legal certainty,' a goal repeatedly stated in the Directive's Recitals (Recitals 4, 6, 7 and 21), but instead creates new uncertainties by using vague language and in places almost unintelligible language."

252. See *Copyright Directive*, *supra* note 248, art. 6(3). One interpretation of the "effective" requirement is that TPMs that can be circumvented too easily or by accident will not qualify as an "effective" measure and therefore will not be protected against circumvention. See Dusollier, *supra* note 162 at 290. From a different perspective, however, the provision allows for an expansive approach to protected measures. The definition of "effective" does not distinguish between access control and copy control. Thus, both measures that prevent copyright infringement and measures that prevent access *may* fall within the scope of this provision: see Koelman & Helberger, *supra* note 10 at 173. Traditionally, copyright law has not included an access-control right. Note, however, that the definition of "effective" does make reference to copyright. The inclusion of an access-control right in this provision may therefore entail a new right, but it does not necessarily entail the introduction of a new right within the law of copyright. In this respect, the definition is distinctly more expansive than strictly required by the WIPO Treaties and *may* favour copyright holders.

253. *Supra* note 248, arts. 6(1)-(3).

possible to circumvent a technology unknowingly, for example through a deep link,[254] article 6(1) was drafted to exclude innocent contraventions. Some authors have suggested that an intention requirement is unnecessary because innocent circumvention is unlikely to occur where a TPM is effective.[255]

The *Copyright Directive* like its American counterpart also prohibits circumvention devices.[256] The *Copyright Directive* differs from the U.S. legislation in one significant way. Contrary to the American legislation, the *Copyright Directive* proposes a voluntary method of addressing exceptions to copyright protection and the interests of users. The provision invites interested parties, such as rights-holders, users, and other interested third parties (*e.g.* producers of consumer electronic goods), to take "voluntary measures" in order to ensure that users can benefit from certain exceptions to copyright law.[257]

This approach, which aims to delegate to private parties the responsibility of safeguarding the public interest, has little chance of achieving the balance that copyright seeks in situations where the bargaining power of the parties is disparate.[258] For example, rights-holders often impose contractual terms on users. As we have seen, the use of DRMs makes this even easier and often forces users to take-it-or-leave-it. Where there is no meaningful opportunity to negotiate, it is unlikely that a voluntary approach will succeed in protecting the balance that copyright law seeks to achieve.

If no agreement is reached between the interested parties, Member States are required to take "appropriate measures" to ensure that right holders:

> ...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.[259]

---

254. See Dave Winer, "Deep Linking" (1999), online: Dave Winer <http://davenet.userl and.com/1999/08/09/deepLin king>: "A deep link is a publicly accessible HTML 'anchor' tag that points to an off-site web page that is not the home page of the site being pointed to." Deep linking is used to route visitors to a specific page of another party's website. Often this is done to save the effort of having to reproduce the particular document or file being offered at that address. When a deep link is offered into a password protected site, users may be circumventing a TPM unknowingly.

255. See *e.g.* Koelman & Helberger, *supra* note 10: "[A] reason not to require proof of knowledge may be that it can be assumed that a person circumventing an 'effective' TM will know he is tampering with a protective measure anyway, and therefore a knowledge test would be redundant." In this situation, "effective" does not refer to whether a TPM meets the formal requirements put forth in art. 6 of the *Copyright Directive*, but, rather, refers to the degree of difficulty with which a TPM may be circumvented. TPMs may, therefore, be categorized as "strong" or "weak" based on their ability to protect an underlying work.

256. *Supra* note 248, art. 6(2).

257. One problem with this regime is that not all Member States will apply the same exceptions. Therefore, what is legal in one Member State will not be legal in another. See *e.g.* Hugenholtz, "Copyright Directive," *supra* note 251 at 500: "What, for example, to make of Article 6.4 (1), a provision that is presumably intended to reconcile the interests of rights owners employing technical protection measures with the interests of users wishing to benefit from copyright limitations? I have read and reread these words several times, but most of it still eludes me. What 'voluntary measures' does the Directive envisage: technical protection measures that automatically respond to eligible users? And what kind of 'agreements between rightholders and other parties' do the framers of the Directive have in mind: collective understandings between right holders and users?"

258. *Ibid.* at 502.

259. *Copyright Directive*, *supra* note 248, art. 4.

However, the *Copyright Directive* provides an exclusion from this requirement for "works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them."[260] Since online applications by their very nature allow members of the public to access works from a place and at a time individually chosen by them, the application of the exceptions to copyright law in the online environment may be defeated by this exclusion.

The *Copyright Directive* has raised a number of concerns. One concern is the uncertain reach of the circumvention provisions, namely whether they are aimed merely at activities that facilitate copyright infringement (use-control) or whether their reach extends to the right to control access to a work (general or limited access-control).[261] What will remain of the public domain if private entities are given the power, both through technological protections and legal measures, to control works to such an extent? Furthermore, there is concern that the approach adopted in the *Copyright Directive* will raise questions of proportionality, since there is doubt as to whether a legal regime is a necessary layer in addition to the technological protections copyright holders may currently employ.[262]

The anti-device prohibition raises additional concerns. As Professor Hugenholtz points out:

> If circumventing as part of exempted copying is permitted, producing the necessary equipment can hardly be prohibited. For similar reasons, photocopying machines, video recorders, personal computers and other reproduction equipment considered suitable for "substantial non-infringing uses," have never been considered illegal.[263]

In conclusion, the EU's *Copyright Directive* raises some serious concerns. For the moment, these concerns are speculative. Until Member States actually implement the provisions of the *Copyright Directive* within their national legislation, we remain unable to measure the possible effect on the public interest. Even then, it will to some extent depend on the European Court's interpretation of these legislative provisions once they enter into force. It may be that the Courts will narrowly interpret the impugned provisions so as to alleviate many of these concerns. Conversely, a broad interpretation of the provisions could prove more detrimental than originally forecast, thereby raising new and pressing concerns. Moreover, as Hugenholtz speculates, the *Copyright Directive* may be invalid and could potentially be annulled:

---

260. *Ibid.*

261. See Koelman & Helberger, *supra* note 10 at 205 where the authors comment on the nature of protection of technological measures: "... one could say that the protection of rights-protecting measures merely boosts existing copyright protection, whereas the protection of access-controlling measures, arguably, constitutes a new exclusive right." The authors further note that in the case of the European Union: "... the proposed Directive suggests that the act of circumvention constitutes copyright infringement ... [h]owever, Article 6 CD does not expressly require Member States to grant an exclusive right [of access], nor does it specify in which area of the law TM protection and remedies may be introduced" (*ibid.* at 207).

262. Hugenholtz, "Public Domain", *supra* note 70 at 89.

263. *Ibid.* at 86.

> In a case brought before the European Court of Justice, Germany has challenged [The Tobacco Advertising Directive's] legal basis and requested its annulment, pursuant to article 230 (ex 173) of the Treaty... The Court notes that the Directive does not facilitate the free movement of goods or the freedom of services, and does not remove distortions to competition. In sum, the Directive lacks a proper legal basis, and should be annulled. The European Court's decision raises the intriguing prospect of one or more disgruntled Member States challenging the validity of the *Copyright Directive*.[264]

At this point in time, it is too early to tell.

D. THE UNITED STATES

While Australia, Japan, and the EU have enacted legislation in compliance with their obligations under the *WCT* and *WPPT*, the U.S. is the only jurisdiction to date with a significant body of decisions demonstrating how such anti-circumvention and anti-device measures have been interpreted by their respective courts. In other words, it is the only country from which concrete conclusions regarding the effect of anti-circumvention measures may be drawn. It is therefore imperative that Canada carefully and critically examine the U.S. situation.

The U.S. response to the obligations of the WIPO Treaties is contained in §1201 of the *DMCA*.[265] The *DMCA* contains prohibitions against both the act of circumvention,[266] and trafficking in circumvention technologies.[267]

Section 1201 is very difficult to navigate. As such, the following outline of the *DMCA* will be used as a guide:

1) Access Control
    (i) Basic Ban
    (ii) Circumvention
    (iii) "Effective" access TPM
    (iv) Prohibition of access circumvention devices
2) Copyright Protection
    (i) Circumvention
    (ii) "Effective" copyright TPM
    (iii) Prohibition of copyright circumvention devices

1) Access Control Measures

(i) Basic Ban

The basic provision is often referred to as the "access provision" or the "anti-access circumvention provision."[268] This basic provision prohibits the circumvention of a TPM that effectively controls access to a work subject to copyright.[269]

---

264. Hugenholtz, "Copyright Directive", *supra* note 251 at 501–2.
265. *DMCA*, *supra* note 31.
266. § 1201(a)(1).
267. § 1201(a)(2) and § 1201(b).
268. Koelman & Helberger, *supra* note 10 at 206–7.
269. Christine Jeanneret, "The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance" (2001) 12 Fordham I.P. Media & Ent. L.J. 157 at 165.

The provision reads:

> No person shall circumvent a technological measure that effectively controls access to a work protected under this title.[270]

In essence, this provision is aimed at prohibiting the circumvention of a TPM that effectively controls access to a work subject to copyright, regardless of whether or not such access would itself amount to an infringement. The basic provision therefore does not protect use control TPMs. The reasoning is that circumvention of a use-control TPM can be dealt with under existing copyright law.[271] Because controlling access is not a right granted in copyright law, it was felt that a new access-control right was necessary in order to provide a means of legal action.[272]

(ii) Circumvention of Access Control TPMs

Circumvention of a technological measure is later defined in a separate provision. This provision reads:

> To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.[273]

This provision is general. The incorporation of access-control and copyright protection were not asserted in this definition. This provision is merely descriptive of the attributes of an act of circumvention.[274]

(iii) "Effective" Access TPM

The *DMCA* distinguishes between TPMs that effectively control access and TPMs that effectively protect copyrights. An effective access TPM is defined as:

> A technological measure 'effectively *controls access* to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain *access to the work.*[275]

(iv) Prohibition of Access Control Circumvention Devices

The *DMCA* circumscribes the trafficking in both access and copyright circumvention devices:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in technology, product, service, device, component, or part thereof which circumvent TPMs.[276]

---

270. § 1201(a)(1)(A).
271. See Koelman & Helberger, *supra* note 10 at 180.
272. *Ibid.* at 179.
273. § 1201(a)(3)(A)
274. Koelman & Helberger, *supra* note 10 at 180.
275. § 1201(a)(3)(B) [emphasis added].
276. § 1201(a)(2).

The above provision does not apply to every conceivable TPM. Rather, it only applies to access control TPMs and requires that one of three following conditions are met:

1) The TPM is "primarily designed or produced for the purpose of circumventing" an access control TPM;[277] or

2) The TPM "has only limited commercially significant purpose or use other than to circumvent" an access control TPM;[278] or

3) The TPM is "marketed by" the person who traffics in the circumventing technology or "by another acting in concert with that person with that person's knowledge for use in circumventing" an access control TPM.[279]

As indicated in our above discussion of the legislation implemented in other countries, the problem with these conditions is that they are rather vague and ambiguous. Practically every technology known to humanity can be used for legitimate or illegitimate purposes. As such, it may be difficult to determine whether a particular technology under investigation satisfies the first two of the three conditions set out above.[280] This could create significant uncertainty for manufacturers and distributors of consumer electronics, telecommunications, computing equipment, and commercial software.

2) Copyright Control Measures

Recall that the basic provision[281] does not prohibit the circumvention of use control TPMs, but rather, is restricted to those technologies that control access. This does not mean, however, that TPMs that protect the uses of works subject to copyright are left unprotected under the *DMCA*. As previously mentioned, rightsholders may still take action for copyright infringement pursuant to existing copyright legislation. Furthermore, the *DMCA* provides additional protection for copyright TPMs.[282]

(i) Circumvention of Copy Control TPMs

This provision, which is the same provision used to protect against circumvention of access control TPMs, is merely descriptive of the attributes of an act of circumvention.[283] Again, the provision reads:

> To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.[284]

---

277. § 1201(a)(2)(A).
278. § 1201(a)(2)(B).
279. § 1201(a)(2)(C).
280. de Werra, *supra* note 11 at 22. See also Dusollier, *supra* note 162 at 28. As indicated above, the European Union *Copyright Directive* utilizes similar criteria.
281. *DMCA*, *supra* note 31, § 1201(a)(1)(A).
282. § 1201(b)(2)(B).
283. Koelman & Helberger, *supra* note 10 at 180.
284. § 1201(a)(3)(A).

(ii) "Effective" Use Control TPM

Whether or not a TPM is deemed "effective" depends on the characteristics of the technology in question. As outlined above, the requirement for an effective access control TPM is governed by § 1201(a)(3)(B). Use control TPMs are subject to a different set of conditions:

> A technological protection measure 'effectively *protects a right of a copyright* owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner.[285]

As written, the above provision covers only those TPMs that protect the rights of a copyright owner within the ambit of copyright law. It is crucial to note that a literal interpretation of this provision would therefore exclude from coverage TPMs that prevent fair use or acts otherwise permitted to users under the law of copyright.[286] Likewise, TPMs that protect materials that are not subject to copyright are excluded from protection.[287]

(iii) Prohibition of Use Control Circumvention Devices

The *DMCA* circumscribes the trafficking of both access and copyright circumvention devices:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in technology, product, service, device, component, or part thereof which circumvent technological protection measures.[288]

As is the case with access control TPMs, this provision does not apply to every conceivable TPM. Rather, it only applies to use control TPMs and requires that one of three following conditions be met:

1) The TPM is "primarily designed or produced for the purpose of circumventing" a TPM used to protect copyright;[289]

2) The TPM "has only limited commercially significant purpose or use other than to circumvent" a TPM used to protect copyright;[290] or

3) The TPM is "marketed by" the person who traffics in the circumventing technology; or by "another acting in concert with that person with that person's knowledge for use in circumventing," a TPM used to protect copyright.[291]

---

285. § 1201(b)(2)(B) [emphasis added].
286. Koelman & Helberger, *supra* note 10 at 175.
287. *Ibid.*
288. § 1201(b).
289. § 1201(b)(1)(A).
290. § 1201(b)(1)(B).
291. § 1201(b)(1)(C).

3) Exemptions

While the Library of Congress was at liberty to address the concerns expressed by critics of the *DMCA*—having the power to grant a range of exemptions—it chose to adopt an extremely narrow three-year exemption to only two "classes of works": compilations consisting of lists of websites blocked by filtering software applications and literary works protected by access control mechanisms that fail to permit access because of malfunction, damage, or obsoleteness.[292]

In addition to the "classes of works" exemption, the *DMCA* contains seven other specific exceptions allowing the circumvention of TPMs in particular cases. These exceptions involve: nonprofit libraries, archives, and educational institutions;[293] law enforcement, intelligence, and other government activities;[294] reverse engineering;[295] encryption research;[296] exceptions regarding minors;[297] protection of personally identifying information;[298] and security testing.[299]

Many scholars have pointed out that a number of these exceptions are written so narrowly that they are not useful as a matter of practice.[300] For example, four of the above exemptions neglect to indicate whether tool-making is permitted as a privileged circumvention.[301] This raises serious doubt as to the true availability of these exemptions, since many of them simply cannot be exercised without the use of circumvention tools.

4) Some Effects of the Digital Millennium Copyright Act

Although rightsholders enjoy benefits under the *DMCA*, nonetheless, the manner in which the *DMCA* has been judicially interpreted has further restricted the availability of the exemptions provided by it.

Some of the more serious criticisms associated with the application of the *DMCA* include: the impairment of the fair use doctrine under U.S. law; prior restraint on freedom of speech as guaranteed by the First Amendment to the U.S. Constitution; the enclosure of the public domain through digital lock-up; a skewing of the balance that copyright policy has traditionally aimed to achieve between private rights and the public interest; the inadequate privacy protection afforded to individuals whose private information may be tracked through the use of TPMs; the chilling effect on scientific research; and the extent to which such a complex maze of prohibitions and exemptions is workable.

---

292. 65 Fed. Reg. 64556 (2000) (to be codified at 37 C.F.R. § 201).
293. § 1201(d).
294. § 1201(e).
295. § 1201(f).
296. § 1201(g).
297. § 1201(h).
298. § 1201(i).
299. § 1201(j). A description of the various exceptions is provided at Michael N. Schlesinger, "Exceptions and Limitations on the Prohibition of Circumvention Access Controls, and on the Prohibition on Circumvention of Technological Measures Protecting Traditional Rights Under Copyright" (Paper presented to the ALAI Congress, June 2001) [unpublished].
300. See *e.g.* Samuelson, "U.S. Digital Agenda," *supra* note 102. See also Nimmer, *supra* note 62.
301. Samuelson, *ibid.* at 1.

A number of examples illustrate some of the concerns expressed regarding the *DMCA*.[302]

(i) US v. Sklyarov[303]

Dmitry Sklyarov, a Russian programmer, was arrested in Las Vegas on July 16, 2001, when he arrived there to give a speech at a conference. He was charged with trafficking and offering to the public a software program that could circumvent technological protections on works subject to copyright law, contrary to *DMCA* § 1201(b)(1)(A). The software program in question was the "Advanced eBook Processor" (AEBPR), owned by ElcomSoft Co. Ltd. (ElcomSoft), Sklyarov's Russian employer. AEBPR is alleged to be capable of removing the technological protection from eBooks in Adobe's eBook format. It further allows the AEBPR to be converted to Adobe's Portable Document Format (PDF) and other similar readers without the restrictions against copying, printing and text-to-speech processing. Normally, publishers of eBooks in Adobe's eBook format can choose to activate such controls as part of their DRMs. Sklyarov was held in jail until August 6, 2001, when he was released on bail of US$50,000 on the condition that he remain in northern California. On August 28, 2001, a grand jury indicted Sklyarov and ElcomSoft on five counts under the *DMCA*. The charges were related to allegations that Sklyarov had developed algorithms on which the AEBPR program is based; that the program was available for purchase on a website in Issaquah, Washington; and that a partially functional version of the program was available on a web server in Chicago, Illinois. If convicted of all counts, he could face 25 years in prison and a fine of up to US$2,250,000. ElcomSoft could face a fine of up to US$2,500,000. On December 13, 2001, Sklyarov was released from custody and allowed to return to Russia as part of an agreement between him and the U.S. government.[304] The manufacturing of a tool such as AEBPR is not illegal in Russia and, apparently, Sklyarov had no role in distributing the program in the U.S. The AEBPR software can be used to allow people access to copies of eBooks that they have acquired for legitimate purposes protected by the fair use defence.

(ii) Felten

A second example involves an action brought by Professor Edward Felten, his research team and Usenix (a technical conference organization) for a declaratory judgment against the *DMCA*. The issue was the publication and presentation of research work done by Professor Felten and his colleagues concerning their success at breaking the "digital watermark" copy prevention on music files. The circumvention activity was actually performed at the invitation of the recording industry. As part of the 'Hack SDMI Challenge,' the recording industry challenged the public to test the security of proposed SDMI copy prevention systems.

---

302. Several American universities have collaborated to create the website "Chilling Effects." This site is dedicated to providing examples that illustrate some of the potential problems and consequences of the *DMCA*, online: Chilling Effects ClearingHouse <http://www.chillingeffects.org>.

303. For a list of the scheduled court dates concerning bail hearings and indictments see online: Slash Dot <http://www.slashdot.org/yro/01/08/06/1941228.shtml>.

304. A summary of this case and other related information is available online: Electronic Frontier Foundation <http://www.eff.org/IP/*DMCA*/US_v_Elcomsoft/us_v_sklyarov_faq.html>.

Felten's team circumvented a number of the SDMI protection mechanisms. In order to claim a prize for successfully breaking these codes, Felten and his team would have had to agree not to disclose the technical details of their circumvention solutions. The Felten team decided not to take the prize, opting instead to publish their results. The SDMI member companies sent Felten's team a letter threatening action under the provisions of the *DMCA*. Concerned that it could be subject to criminal liability if it allowed the Felten paper to be presented at its security conference, the Usenix technical conference organization became involved. There was some discussion whether the paper ought to be presented. Finally, after receiving an incredible amount of negative publicity, the recording industry withdrew its opposition prior to the conference on August 15, 2001, and allowed Felten and his team to submit their paper.[305]

(iii) Ferguson

A third example of the effect that the *DMCA* is having on the scientific research community is illustrated by the case of Niels Ferguson, a professional cryptographer who found a fatal flaw in a cryptographic system called High-Bandwidth Digital Content Protection (HDCP). HDCP encrypts video on the DVI bus used to connect digital video cameras and DVD players with digital TVs and other devices. Exploitation of the flaw in HDCP can result in the decryption of movies, impersonation of any HDCP device and even the creation of new HDCP devices that will work with legitimate ones. Ferguson wrote a paper containing the results of his research. In the normal course, his paper would have been published so that the mistakes could be fixed and others could learn from the paper. However, Ferguson was afraid to publish his paper for fear of prosecution under the *DMCA*. Although Ferguson lives in the Netherlands, he is concerned that his paper may contravene the *DMCA*. Part of his concern is based on the fact that he travels to the United States regularly. Ferguson makes a strong case that the *DMCA* actually protected flawed systems such as HDCP rather encouraging the repair of such flaws prior to their mass adoption in the manufacture of electronic products. He also condemns the *DMCA* on the basis of its interference with free speech.[306]

Given the experiences of Sklyarov and Felten, Ferguson's concerns may be legitimate and far from unique. One illustration of the extent to which the *DMCA* has had a chilling effect on the science community is that of a contractual clause found in the standard Copyright Form of the Institute for Electrical and Electronic Engineers (IEEE).[307] The IEEE is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. According to its website, the IEEE claims to produce thirty percent of the world's published literature in electrical engineering, computers and control technology; holds annually more than 300 major conferences; and has more than 860 active standards with 700

305. A summary of this case and other related information is also included online: Electronic Frontier Foundation <http://www.eff.org/IP/*DMCA*/Felten_v_RIAA>.

306. Ferguson, *supra* note 68.

307. Online: Institute for Electrical and Electronic Engineers <http://www.ieee.org/about/documentation/copyright/cfrmlink.html>.

under development.[308] Until very recently, the IEEE Copyright Form–which all authors must sign as a condition of publication in any IEEE related books, journals, or conference proceedings–had required all authors to warrant that the publication or dissemination of the work shall not violate any proprietary right or the *DMCA*.[309] As one anonymous observer recently stated in an online discussion, "the IEEE's decision to require authors to adhere to the *DMCA* has the potential to restrict research and discussion of security matters worldwide."[310] As a result of extreme pressure both internal and external to the organization, the IEEE decided to remove the contractual warrant.[311]

(iv) RealNetworks v. Streambox

The first of the reported decisions that interpreted the provisions of the *DMCA* was *RealNetworks, Inc. v. Streambox, Inc.*[312] RealNetworks developed the copy control format "Real Media" which provides a series of security mechanisms to prevent unauthorized downloading of streamed audio and video content over the internet. This copy format works as a "secret handshake"/"copy switch" by authenticating the destination of the file. Streambox made a series of products, which facilitated various uses of content streamed from RealNetworks products. Such products allowed the user to bypass the "secret handshake"/"copy switch" and access the underlying content by converting the files from Real Media format to other formats. RealNetworks brought a suit against Streambox alleging that they had violated the trafficking provisions of the *DMCA*.

The Court found that Streambox had likely violated the trafficking in circumvention devices provisions, both with respect to access and copy control, and thereby granted the preliminary injunction preventing Streambox from manufacturing, importing or selling its products.

(v) Universal City Studios v. Reimerdes

The second case worth noting is *Universal City Studios, Inc. v. Reimerdes*.[313] Universal Studios and five other movie studios filed suit against the three defendants (affiliated with the online computer magazine "2600") who posted on the internet copies of a software program, DeCSS, that cracks the security system, CSS. Recall that CSS prevents the unauthorized copying of DVDs. The plaintiffs alleged that CSS is a technical measure that controls access to copyrighted works and that DeCSS circumvents that measure. Universal alleged that the defendants had violated the trafficking ban on circumvention devices through the posting and providing of weblinks to DeCSS. The court granted a preliminary injunction bar-

308. Online: Institute for Electrical and Electronic Engineers <http://www.ieee.org/about>.

309. Ironically, the text of the actual copyright form refers to it as the "Digital Copyright Millennium Act (the 'DCMA')." Apparently, Professors Nimmer and MacKaay are not the only ones to find this statute confusing, see text accompanying note 321, below.

310. The fact that the author of this message felt the need to send it anonymously is itself further evidence of the chilling effect that the *DMCA* is having on the scientific community.

311. Lisa M. Bowman, "IEEE backs off on copyright law" ZD Net News (16 April 2002), online: IEEE <http://zdnet.com.com/2100-1106-884288.html>.

312. 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 18 Jan. 2000) (Lexis) [*Streambox*].

313. *Universal v. Reimerdes, supra* note 28.

ring the defendants from posting the DeCSS program or any other technology that circumvents CSS. The court further held that offering access to DeCSS on a website violated the trafficking ban of the anti-circumvention measures by providing a means to circumvent an access control measure.

The *Universal v. Reimerdes* decision was appealed. The U.S. Court of Appeals dismissed the appeal.[314] In dismissing the appeal, the Court made the following important determinations: i) circumvention of encryption technology protecting copyrighted materials is not permitted even when the material will be put to "fair uses" exempt from copyright liability;[315] ii) the protection afforded to copyright owners in the *DMCA* is not to be construed narrowly;[316] iii) while a person who buys a DVD is permitted to view the DVD, the right to do so does not include a right to circumvent encryption technology to support use on multiple platforms;[317] iv) "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code;"[318] v) computer programs are not exempted from the category of speech protected by the U.S. Constitution simply because their instructions require the use of a computer;[319] vi) computer code contains both speech (*i.e.* expressive) and non-speech (*i.e.* functional) elements;[320] vii) the *DMCA* and the posting and linking prohibitions on DeCSS are applied to DeCSS because of its functional ability to instruct a computer and not because of the content of DeCSS; and viii) this form of regulation is content-neutral and passes constitutional scrutiny.[321] Furthermore, it has been suggested that this case does not really address the fair use exception and, in any event, that the fair use doctrine has never been held out as a guarantee of access to copy a work, nor as a guarantee that a person claiming fair use can copy the work in question according to his or her preferred technique or, for that matter, in the format of the original.[322]

A number of interesting and troubling possibilities arise from the decisions in *Streambox* and *Universal v. Reimerdes*.

First, the de-coupling of the inquiry into the uses of circumvention from prohibitions on circumvention devices might have the effect of extending a copyright holder's authority over the use of a work to include access control as well, when the technological systems are designed to protect both.[323] As TPMs often incorporate both access-control and copy-control technologies, and as there is no fair use defence for the circumvention of an access-control measure, this could

---

314. *Universal v. Corley*, *supra* note 28.

315. *Ibid.* at 443. Notice that this holding contravenes the definition of an effective TPM which, as discussed above in Part X.D.2.iii, expressly includes only TPMs that "prevent, restrict, or otherwise limit the exercise of a right of a copyright owner." Here, the TPM prevented a user from using a work in spite of the availability of the fair use exception. In other words, the TPM did not prevent the exercise of a right of a copyright owner and therefore, the technology used to restrict use should arguably have fallen outside the scope of protection set out in the *DMCA* as drafted.

316. *Ibid.* at 444.

317. *Ibid.*

318. *Ibid.* at 445.

319. *Ibid.* at 447.

320. *Ibid.* at 451.

321. *Ibid.* at 454 ff.

322. *Ibid.* at 458–459.

323. Eddan E. Katz, "*Realnetworks, Inc. v. Streambox, Inc. & Universal City Studios, Inc. v. Reimerdes*" (2001) 16 Berkeley Tech. L.J. 53 at 64.

effectively remove the fair use defence for copyright infringement. Thus, for example, Streambox technology might not be lawfully used even to download video works that are in the U.S. public domain, such as court proceedings, even if such videos are only available for a short time on a website.[324]

Second, the District Court in *Universal v. Reimerdes* held that the reverse engineering exemption in the *DMCA* does not allow for the public dissemination of a software developer's work, but rather permits the developer only to share that information with individuals collaborating on the inter-operability project.[325] This narrow interpretation of the exemption has potentially devastating implications for the future of innovation as it adversely affects the developmental structure of open source software that relies on collaborative projects within a particular community while being open to all internet users.[326] As Katz notes:

> This type of product development has been an integral element in the success of Linux in the computer industry. The further acceptance of Linux in the consumer market as a practicable operating system alternative to Windows depends on the ability of users to utilize the same mainstream applications, including the ability to view DVD movies.[327]

Finally, there is something unsettling in the decision in *Universal v. Reimerdes*, holding that the anti-device provisions of the *DMCA* do not result in an unconstitutional interference with freedom of speech. How is one to reconcile the U.S. constitutional theory applied in this case with the claims of legitimate cryptographers, like Ferguson, who purport that they are afraid of publishing the results of their work for fear of prosecution under the *DMCA*?

(vi) Church of Scientology Cases

The Church of Scientology has routinely sued for copyright infringement to restrain critiques of Scientology.[328] The Church of Scientology has recently employed the *DMCA* to control the use of their publications. On March 21, 2002, Google, the leading search engine on the Internet, made the decision to ban a site critical of the Church of Scientology.[329] The blocked site, xenu.net, is located in Norway and posts comments critical of the Church of Scientology. Using the *DMCA*, Scientology lawyers claim that Google may no longer include anti-Scientology sites that allegedly infringe upon the church's intellectual property. The net-effect is that a search for the term 'Scientology' will only yield links to sites that are controlled by the church itself.

---

324. *Ibid.* at 65–66.
325. *Supra* note 28 at 320.
326. Katz, *supra* note 323 at 68.
327. *Ibid.*
328. See *e.g. New Era Publications, APS v. Key-Porter Books* (1988), 17 F.T.R. 300, (1987), 18 C.P.R. (3d) 562 (F.C.T.D.); *New Era Publications International, APS v. Carol Publishing Group* 904 F.2d 153, 14 U.S.P.Q.2d 2030 (2d Cir. 1990).
329. See *e.g.* Declan McCullagh, "Google Yanks Anti-Church Sites" (21 March 2002), online: Wired News <http://www.wired.com/news/politics/0,1283,51233,00.html>; and Harry Rider, "Google Caves to Church's Legal Pressure" (26 March 2002), online: osOpinion <http://www.osopinion.com/perl/story/16938.html>. A number of web sites have posted comments on Google's removal of xenu.net.

The *DMCA* contains a provision for copyright violations and on-line intermediary liability, more commonly referred to as the "notice and takedown" provisions. Scientologists claimed that their rights were being infringed and sent a notice to Google, under the *DMCA*, demanding the removal of the web-link from the search engine. If Google had not complied, it could have been held liable for contributory copyright infringement. After much media criticism, Google restored the xenu.net site to its search engine, thus exposing itself to liability.[330] Despite the fact that it was only removed temporarily, the removal of the xenu.net site and the actions of the Church of Scientology raise alarming free speech issues.

Although the Google–Church of Scientology scenario is not in itself illustrative of the effects of the anti-circumvention provisions in the *DMCA*, it is important to note that the Church of Scientology could have used an access-control or use-control technology to achieve the same effect. Benkler, in commenting on the case *Religious Technology Center v. Netcom On-line Communications Services*,[331] illustrates how anti-circumvention measures could be used in an abusive manner to significantly curtail freedom of expression and enclose the public domain. By way of background, the Church of Scientology brought charges of copyright infringement against Dennis Erlich, a former Scientology minister turned avid critic of the Church of Scientology. Erlich posted critical commentary and Church documents on an Internet newsgroup website. The Court concluded that Erlich had infringed the Church of Scientology's copyright in several of the posted documents. Under order of the Court, Erlich's home was searched, and his computer disks, working papers, and portions of his hard disk drive were copied onto floppy disks and the infringing materials were erased. Benkler demonstrates how a claim using the *DMCA*'s anti-circumvention provision would have impacted this case:

> After the court issues the TRO and Erlich's computer, disks, and documents were seized, the court ordered some of the materials returned. These pertained to his posting of documents that had fallen into the public domain. But if the same documents had been protected by encryption, and even though Erlich would have been perfectly privileged under copyright law to use them to criticize the church, he would have remained under a court order prohibiting him from reading, let alone distributing, the materials that he wished to criticize. To publish these materials on the Internet, Erlich would have had to remove the code that protected them. And that removal, despite any privilege he might have to use the underlying materials, would expose him to civil sanctions and to seizure of his computer.[332]

Benkler's example illustrates the potential violation of freedom of expression and the ability of copyright holders to enclose works in the public domain through the use of an anti-circumvention measure.

---

330. See "Google pulls, replaces Web page critical of Scientology" Reuters (22 March 2002), online: Philly.com <http://www.philly.com/mld/philly/business/technology/2910195.html>.

331. 923 F. Supp. 1231, 37 U.S.P.Q.2d 1545 (N.D. Cal. 1995).

332. Yochai Benkler, "Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain" (1999) 74 N.Y.U.L. Rev. 354 at 419.

5) Academic Reactions to the Digital Millennium Copyright Act

The events discussed in the preceding sections have resulted in strong reaction from the academia. The *DMCA* has been subjected to the following academic criticisms: the statute is drafted in a very convoluted manner that is hard to follow;[333] the prohibitions contained in the *DMCA* go far beyond what the WIPO Treaties require with respect to the legal protection of TPMs;[334] the *DMCA* creates an access-control right for copyright owners that was not previously part of copyright law;[335] the *DMCA* will lead to a pay-per-use society;[336] the exemptions contained in the *DMCA* favour significantly and unjustifiably the rights of copyright owners as compared to users;[337] no general purpose exception has been included to give courts some leeway in making exceptions for circumstances that Congress has not considered;[338] there is a need for periodic reviews of the anti-circumvention provisions;[339] there is a potential for the use of TPMs coupled with legal protection to leverage "thin" copyright in information that was previously in the public domain;[340] it is not yet clear that consumers will accept access controls;[341] if the operation of the *DMCA* is not seen to be reasonable, it will invite civil disobedience;[342] and the *DMCA* is not the most effective means of achieving its objectives given that potential defendants (against whom injunctions are sought) can be situated anywhere in the world and can use various technologies to shield their identities.[343]

One of the few favourable academic reviews of the *DMCA* has come from Ginsburg, who has suggested that maintaining a high degree of control over works in authors' hands will actually increase the prospect of remuneration for authors. This, she claims, makes the prospect of self-publication more realistic and improves the likelihood of "an increase in the volume and diversity of works of authorship, as authors will be able to bypass the gatekeeping functions of publishers and other intermediaries."[344]

In spite of Ginsburg's optimism, it would seem, on balance, that the difficulties posed by the *DMCA* provide a number of reasons for policy-makers in Canada to proceed cautiously when considering how best, if at all, to implement Canada's TPM-related obligations under the WIPO Treaties.

---

333. Nimmer, *supra* note 62 at 675. See also MacKaay, *supra* note 8 (MacKaay aptly describes the *DMCA* as, "blissfully unreadable").
334. Pamela Samuelson, "Towards More Sensible Anti-Circumvention Regulations" (Paper presented to Financial Cryptography 2000 Conference, February 2001) [unpublished] at 7–9, online: Sims School of Information Management and Systems University of California Berkeley <http://www.sims.berkeley.edu/~pam/papers/fincrypt2.doc> [Samuelson, "Anti-Circumvention Regulations"]; Lipton, *supra* note 142 at 339.
335. de Werra, *supra* note 11 at 19.
336. Nimmer, *supra* note 62 at 710.
337. Samuelson, "Anti-Circumvention Regulations," *supra* note 334. See also Guibault, *supra* note 156 at 159–60.
338. Samuelson, *ibid.* at 5–7.
339. Samuelson, "Intellectual Property," *supra* note 130 at 561–62.
340. Jane C. Ginsburg, "Copyright and Control over New Technologies of Dissemination" (2001) 101 Colum. L. Rev. 1613 at 1635.
341. Jessica Litman, "The Breadth of the Anti-Trafficking Provisions and the Moral High Ground" (Paper presented to the ALAI Congress, June 2001) [unpublished] at 9, online: ALAI 2001 Congress <http://www.law.columbia.edu/conferences/2001/1_program_en.htm>.
342. *Ibid.* at 7.
343. Lipton, *supra* note 142 at 366–67.
344. Ginsburg, *supra* note 340 at 1646–47.

XI. Concluding Remarks

SHOULD CANADIAN POLICY-MAKERS choose to let TPMs flourish or fail on their own merit? Or should they confer some particular form of extra legal protection for the legitimate use of TPMs, inspired by the relevant provisions of *WCT* and *WPPT*? The former option runs the risk of enabling the mass infringement of digital works and thereby threatens the very existence of key cultural industries, such as book and music publishing, record production, computer software, film production, media, sports and entertainment. The latter choice, on the other hand, runs the risk of skewing copyright's delicate balance, interfering with personal privacy, chilling expression, stifling important scientific research, shrinking the public domain, undermining the public's ability to access information and perhaps even threatening national security. Given the serious implications of either choice, it is suggested that Canadian policy-makers must be guided not by speculation, but by what is known.

Currently, there is a paucity of empirical data indicating a clear need to adopt legal measures. To the contrary, much of the existing literature focuses instead on the recent advent of DRMs and their promise to secure copyright owner control over digital works. TPM-enabled DRMs currently offer copyright owners three layers of protection: TPMs, copyright law and contract law.

Another existing source of empirical data is the judicial application and its aftermath of US enacted legislation. As we have seen, the application of the *DMCA* provides ample warning of the possible effects of anti-circumvention measures and demonstrates that the implementation of similar policies must be approached with tremendous caution. The application of the *DMCA* also reveals the tension between what is theoretically desirable and what is practically achievable. As summarized by Lipton:

> It is important that those engaging in debates about the appropriate balance of rights in the digital era do not forget the need to strike a balance between ownership of intellectual property and the need for free debate and expression in a democratic society. However, it is equally important that practical imperatives are not forgotten. There is little point in resolving the political issues only to find that effective legislation is impossible in practice. It would be a regrettable and somewhat paradoxical outcome if new copyright legislation had the effect of preventing access to copyright works and other materials by those with a legal right to use them, but lacked the technical skills to access them, while at the same time failed to prevent or effectively redress activities of those with no legal right to the material in question but with the necessary technical skills to gain access.[345]

Until the market for digital content and the norms surrounding the use and circumvention of TPMs (and their implications for that market) become better known, it is simply premature to try to ascertain what the appropriate *practical* legal response should be. As indicated in several points throughout this article, making policy decisions without such knowledge could result in great harm to the public interest. Consequently, we suggest that Canada should not implement any new legal measures to protect TPMs at this time. At the moment, it is far from

345. Lipton, *supra* note 142 at 368–69.

certain that new legislation designed to protect the legitimate use of TPMs is necessary to meet the TPM-related requirements of the *WCT* and *WPPT*.[346]

Should there come a time when it is evident that such legislation is necessary, several options might be considered. One option would be to create a legislative regime that comports with Canada's domestic copyright policy without regard to the requirements set out in the *WCT* and *WPPT*. The effect of this would, of course, be to deprive Canada of the benefit of reciprocal enforcement of a number of areas covered by the treaties. In addition, a number of Canada's trading partners might be upset with Canada and seek some form of trade-related retaliation.

A second option would be to adopt a policy approach that aims to create as little legal change as possible in meeting the threshold of "adequate legal protection" pursuant to the WIPO Treaties. Under this approach, the measures adopted in Canada would incorporate a healthy range of exceptions aimed at maintaining the balance promoted by Canadian copyright legislation prior to digital copyright reform. To the greatest extent possible, these measures would be crafted in a manner that protects free expression values, safeguards privacy and maintains a robust public domain. If Canada were to take this course, further study would be useful in determining the minimal level of legal protection, in order to ensure compliance with the *WCT* and *WPPT*.

A third option would be for Canada to follow the lead of other WTO countries and opt for strong legal protection of TPMs. If Canada pursues this option, this article reveals that the details of such a regime *must* be crafted carefully in light of the practical problems that have been identified in this article with other national regimes of this nature. In particular, until such a time as TPMs are capable of distinguishing between infringing and non-infringing uses of digital works,[347] the measures that are ultimately adopted must go to great lengths *not* to introduce an access-control right. Such a right has the potential to undermine the philosophical foundations of copyright law and policy. To the extent that the *sui generis* creation of such a right is an indirect and unavoidable consequence of the adopted measures, the measures that are ultimately adopted must absolutely incorporate a healthy range of exceptions aimed at restoring the balance originally promoted by Canadian copyright law.

Canadian copyright law currently contains a "fair dealing" exception to copyright when a work is used for the purpose of private study, research, review, criticism, or news reporting, and the manner of the use is fair.[348] A fairly long list

---

346. The above suggestion is offered with full awareness of the fact that there are perhaps a number of persuasive political reasons in favour of implementing WIPO-compliant legislation of the sort not appropriate for analysis in this article. To mention just two examples, perhaps policy makers will be forced to measure the potential harm to the public interest set out in this paper against other possible harms that could result if Canada upsets a number of its usual trading partners by refusing to enact new legislation; or perhaps policy makers will want to measure the effect of enacting some minimally compliant legislation now versus succumbing to political pressure to adopt *DMCA*-like legislation down the road.

347. As David Nimmer recently suggested at the Duke Law Conference on the Public Domain, the day when software is sufficiently capable of drawing such a distinction could be a longtime-coming, especially since appellate courts are not yet sophisticated enough to do this in a coherent and consistent manner. See online: 2001 Duke Law School Conference on the Public Domain <http://www.law.duke.edu/pd/realcast.htm>.

348. *Copyright Act*, *supra* note 157, ss. 29–29.2 as am. by S.C. 1997, c.24, s.18.

of other specified exceptions to copyright exist in Canada in order to protect access for educational institutions;[349] libraries, archives and museums;[350] and individuals to computer programs;[351] incidental inclusions;[352] ephemeral recordings,[353] and sound recordings.[354] As indicated in this article, it is absolutely crucial to note that *the exercise of any of the exceptions enumerated above is premised on the ability to gain access to the work in question.* Consequently, to the extent that the *sui generis* creation of an access-control right is an indirect and unavoidable consequence of the adopted measures, we have revealed that such legal measures must include a positive obligation on the copyright holder to ensure that alternative means of obtaining access to a work remain available—a "*copy-duty*," as Lessig has called it.[355] In other words, any newly introduced access-control right must be counter-balanced by a newly introduced access-to-a-work right.[356] Under this approach, copyright owners would have a positive obligation to provide access-to-a-work when persons or institutions fall within an exception or limitation set out in the *Copyright Act*. Such an obligation might entail the positive obligation to allow access-to-works in the public domain, or to provide unfettered access-to-works to educational institutions and other organizations that are currently exempted from a number of the provisions in the *Copyright Act*.[357]

The above suggestion is not merely the passing fancy of wishful academics. It has its basis in Canadian constitutional law, and is already supported in principal by the Supreme Court of Canada, as illustrated by the following passage from *Haig v. Canada*:

> ... a situation may arise in which, in order to make a fundamental freedom meaningful, a posture of restraint would not be enough, and positive governmental action might be required. This might, for example, take the form of legislative intervention aimed at preventing certain conditions which muzzle expression, or ensuring public access to certain kinds of information. [358]

An application of the *Haig* principle to the TPM issue raises an interesting question. Might the failure to provide a *copy-duty*, *i.e.*, a failure to ensure public access to certain kinds of information, result in a court mandating governmental action to preserve free expression or to otherwise ensure access-to-a-work? Perhaps, in the digital age, the public needs to be safeguarded through a legally protected right to access digital information.[359] Such thinking provides a reason-

---

349. Ss. 29.3–30 as am. by S.C. 1997, c.24, s.18.
350. Ss. 30.2, 30.3–30.5 as am. by S.C. 1997, c.24, s.18; ss. 30.1, 30.21 as am. by S.C. 1999, c.31, s.59(e).
351. S. 30.6 as am. by S.C. 1997, c.24, s.18.
352. S. 30.7 as am. by S.C. 1997, c.24, s.18.
353. Ss. 30.8, 30.9 as am. by S.C. 1997, c.24, s.18.
354. Ss. 80–81 as am. by S.C. 1997, c.24, s.50.
355. Lessig, *Code*, *supra* note 66 at 127. See also Koelman, *supra* note 99.
356. An example of such a measure is the creation of a digital lending right that could serve to maintain fair dealing. See Joshua Foley, "Comment: Enter the Library: Creating a Digital Lending Right" (2001) 16 Conn. J. Int'l L. 369 at 389.
357. *Supra* note 157, ss. 29–30. In one variant of this approach, a trusted third party, who holds a copy of the digital work in escrow, could be tasked with resolving access disputes: Burk and Cohen, *supra* note 166 at 63.
358. [1993] 2 S.C.R. 995 at 1039.
359. Julie E. Cohen, "Intellectual Privacy and Censorship on the Internet" (1998) 8 Seton Hall Const. L.J. 693 at 700.

able response to those critics who justify access-control measures on the basis that copyright law "has neither compelled copyright owners to make a general disclosure of their works, nor traditionally obliged right holders to make their works, once disclosed, available in a way that would facilitate either access or copying, even for fair use purposes."[360]

This article would be incomplete, if not totally remiss, if it concluded without at least mentioning a possible error in the approach that Canada's copyright consultation process has taken with respect to TPMs. In particular, it is worth taking note of the manner in which the TPM issue continues to be framed. Consider the following example from the *Consultation Paper on Digital Copyright*: "The issue arises whether and under what circumstances copyright legislation ought to provide sanctions against persons who engage in activities related to the circumvention of these protective measures."[361]

In addressing the above question, it is perhaps useful to remember that there are other questions that come *logically prior* to this one. Before asking whether and under what circumstances copyright legislation ought to protect TPMs, it is necessary to first ask *whether and under what circumstances TPMs should be permitted to flourish.*[362] As indicated throughout this article, the waters are mostly uncharted. Still, given the increasing body of literature that is critical of proprietary software and architectures of control that has been referred to and discussed throughout this article, it is at least possible that the recent focus on the legal protection *of* TPMs is misdirected. It may well turn out that it is the public and not the private interest groups that will require legal protection. As suggested above, legal protection may become necessary to ensure that the public is afforded reasonable access to materials that might otherwise be unavailable to them because of contract or TPM restrictions. The internet's early architectures of freedom certainly did allow users of digital content to thwart copyright enforcement with relative ease, and it was precisely this that led many stakeholders to view legal protection of TPMs as necessary. However, it is extremely important to recognize that those early architectures continue to evolve.[363] As TPMs and DRMs gain presence online, not only might the legal protection *of* TPMs quickly become unnecessary, it could turn out that what is needed is legal protection *from* TPMs. As Hugenholtz notes:

> In a pessimistic vision of the future, the Internet will gradually lose much of its open character. Encrypted information products and services will enforce their own pre-programmed conditions of use automatically. Code will rule the Internet with iron logic. In a worst case scenario, only a new body of public information law, that can secure a right of access to "important" information will be able to safeguard the public domain.[364]

---

360. Ginsburg, *supra* note 340 at 1635.

361. Industry Canada & Canadian Heritage, *supra* note 173 at Part 4.2.

362. Interestingly, although the consultation issue was, once again, framed in terms of "whether and under what circumstances copyright legislation ought to protect TPMs," the *unstated* preliminary question of "whether and under what circumstances TPMs should be permitted to flourish" was raised over and over again, and received the most attention from the participants at the Canadian Heritage consultation held in Ottawa on April 11, 2002.

363. Lessig has referred to the fallacy of assuming that the internet has a fixed essence as "the IS-ism." See Lessig, *Code*, *supra* note 66 at 24–29.

364. Hugenholtz, "Public Domain," *supra* note 70 at 89–90.

The above remarks are not meant to suggest that legal protection should *never* be afforded to TPMs, nor that the public ought to be legally protected *now* from TPMs. Rather, they are intended to point out that policy makers may be tempted to rush too quickly ahead and attempt to resolve issues that are not yet fully formed or understood. Policy makers should not proceed with the passage of new legislation in this area without a more careful consideration of the concerns expressed herein. As stated above, until the market for digital content and the norms surrounding the use and circumvention of TPMs, and their implications for that market, become better known, it is simply premature to try to ascertain the appropriate *practical* legal response. Given this practical reality, as well as important policy implications that follow from a decision to implement new, WIPO-compliant legislation, it is reiterated that Canada ought to refrain from affording legal protection to TPMs at this time.

As a final remark, when examining these issues, it is useful to remember one of the hallmark principles of electronic commerce and internet law: *the doctrine of technological neutrality*. In essence, this principle:

> refers to statutory tests or guidelines that do not depend upon a specific development or state of technology, but rather are based on core principles that can be adapted to changing technologies. Since technological change is constant, standards created with specific technologies in mind are likely to become outdated as the technology changes.[365]

Consequently, the pursuit of technological neutrality as a policy objective tells us that we ought to guide our laws not by the technological flavour of the month but on the basis of sound legal judgments about the underlying functions that the various relevant technologies aim to achieve.

While policy-makers in the technology law field have generally been quite successful in relying on this doctrine to date,[366] it is instructive to consider why the doctrine is not wholly applicable to the issues currently under consideration. Although anti-circumvention and anti-device provisions, if adopted, could and should be drafted so that they are not technology specific,[367] the very impetus in favour of or against adopting anti-circumvention legislation is to some extent technologically dependent rather than technologically neutral.

Where technological neutrality is applicable, the validity of the law in question does not depend on the existence of the technologies it governs. Clearly and

---

365. Michael A. Geist, "Is There A There There? Towards Greater Certainty for Internet Jurisdiction" (2001) 16:3 Berkeley Tech. L.J. 1345 at 1359 [footnotes omitted], online: Berkeley Technology Law Journal <http://law.berkeley.edu/journals/btlj/articles/vol16/geist/geist.pdf>
See also Gerald Herrmann, Secretary of United Nations Commission International Trade Law (UNCITRAL),"Establishing a Legal Framework for Electronic Commerce: the Work of the United Nations Commission on International Trade Law"(Paper presented to the International Conference on Electronic Commerce and Intellectual Property (WIPO), September 1999) [unpublished], online: World Intellectual Property Organization <http://ecommerce.wipo.int/meetings/1999/papers/pdf/herrmann.pdf/>.

366. See *e.g.* UNCITRAL *Model Law on Electronic Commerce With Guide to Enactment* (1996), online: United Nations Commission on International Trade Law <http://www.uncitral.org/en-index.htm> and its Canadian counterpart, the *Uniform Electronic Commerce Act*, online: Uniform Law Conference of Canada <http://www.law.ualberta.ca/alri/ulc/current/euecafin.htm>.

367. That is, they should not be designed to apply only to particular device types such as CSS or SDMI.

without question, this is *not* the case with legislation that might be implemented to protect TPMs. In the case of TPMs, if the technologies embraced by the general public change, then the need for or against implemented legislation of this sort might also change. Thus, it is impossible for anti-circumvention and anti-device legislation to completely invoke the principle of technological neutrality in any pure sense, since the very motivation for implementing TPM legislation is governed by a view that is not technologically neutral but precisely the opposite.[368]

This illustrates the special challenge faced by those compelled to implement WIPO-compliant TPM legislation, who are forced to carve into stone rules surrounding technologies that are not yet carved into silicon. By comparison, such challenges are more easily achieved in other areas of legislation that are less technology-dependent and less value-laden, for example online contract formation. Although intelligent agent technologies raise a number of interesting questions that require a clarification of the rules for contract formation in the online setting,[369] the state of the art and the particular features of any given agent-based technology do not drive the policy objectives. In the case of online contracting, the objective of legislative reform is quite straightforward; namely, to choose a coherent set of rules that provides clarity and fosters business certainty. One enormous difference between online contracting and digital copyright reform is that, in the case of online contracting, the creators of the relevant automation technologies and the businesses that use them are utterly indifferent to the substance of the rules adopted, so long as the rules implemented achieve the policy objective, *which is itself neutral as between the creators and users* of the relevant technologies.

The issues encountered in the digital copyright area are challenging precisely because the policy objectives underlying the legal protection of TPMs are not value-neutral. Likewise, and this point all-too-often goes unnoticed, *the technological measures* used by copyright owners in digital rights management systems are not themselves value neutral. As Postman so eloquently put it:

---

368. For an excellent comprehensive study of the impossibility of achieving technological neutrality in the context of reforming copyright legislation see Ysolde Gendreau, "A Technologically Neutral Solution for the Internet: Is It Wishful Thinking?" in Paul Torremans & Irini Stamatoudi, eds., *Copyright in the New Digital Environment: The Need to Redesign Copyright* (London: Sweet & Maxwell, 2000) at 1–16; see also Service de la formation permanente du Barreau du Québec, ed., *Développements récents en droit du divertissement* (Cowansville: Éditions Yvon Blais, 2000) at 17–35.

369. See Ian R. Kerr, "Spirits in the Material World: Intelligent Agents as Intermediaries in Electronic Commerce" (1999) 22 Dal. L.J. 189–249; Ian R. Kerr, "Providing for Autonomous Electronic Devices in the *Uniform Electronic Commerce Act*" (Paper presented to the Annual Proceedings of the Uniform Law Conference of Canada, Ottawa, 2000)[unpublished], online: Uniform Law Conference of Canada <http://www.law.ualberta.ca/alri/ulc/current/ekerr.htm>; Ian R. Kerr, "Ensuring the Success of Contract Formation in Agent-Mediated Electronic Commerce" (2001) 1 Electronic Commerce Research Journal 183–202.

> Embedded in every technology there is a powerful idea, sometimes two or three powerful ideas. Like language itself, a technology predisposes us to favor and value certain perspectives and accomplishments and to subordinate others. Every technology has a philosophy, which is given expression in how the technology makes people use their minds, ...in how it codifies the world, in which of our senses it amplifies, in which of our emotional and intellectual tendencies it disregards.[370]

As the saying goes, "hard cases make bad law."[371] Certainly, the same can be said of hard policy choices. In the area of digital copyright reform, where policy makers are being asked to implement measures that are neither technologically neutral nor value neutral, it is difficult if not impossible to satisfy all of the stakeholders, all of the time. As suggested in this article, the best strategy for maintaining a balanced copyright law is to take an approach that best preserves the *status quo* until such time as the cultural norms surrounding the use of these technologies provide a clear indication of the need for reform, one way or the other.

> With lance braced and covered by his shield, he charged at Rocinante's fullest gallop and attacked the first mill that stood in front of him. But as he drove his lance-point into the sail, the wind whirled it around with such force that it shivered the lance to pieces. It swept away with it horse and rider, and they were sent rolling over the plain, in sad condition indeed.
>
> *–Miguel de Cervantes, 1605*

370. Neil Postman, *The End of Education: Redefining the Value of School* (New York: Alfred A. Knopf, 1996) at 192–3. See also Jerry Mander, *Four Arguments For The Elimination of Television* (New York: William Morrow, 1978) at 350: "Americans have not grasped the fact that many technologies determine their own use, their own effects, and even the kind of people who control them. We have not yet learned to think of technology as having ideology built into its very form."

371. *Northern Securities Company v. United States*, 193 U.S. 197 [1904] at 400–1, 193 U.S. 197, 24 S. Ct. 436 [per Holmes J].