CHAPTER TEN

The Protection of Rights Management Information:

Modernization or Cup Half Full?

Mark Perry*

In the SAVOY:

Printed by *Henry Lintot*, Law-Printer to the King's most excellent Majesty; for D. Browne at the *Black Swan*; J. Worrall at the *Dove*, both near *Temple-Bar*; and A. Millar at *Buchanan's Head* opposite *Catherine Street* in the *Strand*, 1757**

A. AN INTRODUCTION TO RIGHTS MANAGEMENT INFORMATION

Many papers in this collection discuss the history and development of Bill C-32, *An Act to Amend the Copyright Act*,[1] introduced into the Canadian Par-

* Thanks to Michelle Alton and Ambrese Montague (UWO law class of 2007) and Dan Hynes and David Morrison (law class of 2012) and Thomas Margoni (Post Doctoral Fellow) for their research assistance.

** This "RMI" is from the front of Lord Chief Baron Gilbert, "A treatise of Tenures in Two Parts" 1757. Lintot and Millar were well known publisher/booksellers in London at the time. The same Andrew Millar was party to *Millar v. Taylor* (1769), 4 Burr. 2303, 98 E.R. 201, with the erroneous judgment proclaiming common law copyright. For more on the latter, denying the existence of common law copyright, see Mark Perry, "Acts of Parliament: Privatization, Promulgation and Crown Copyright—Is there a Need for a Royal Royalty?" (1998) 1993:3 N.Z. L. Rev. 493.

1 Bill C-32, *An Act to Amend the Copyright Act*, 3rd Sess., 40th Parl., 2010 (First reading 2 June 2010), www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4580265&file=4 [Bill C-32].

liament on 2 June 2010, so that analysis will not be duplicated here. Among the failures of copyright reform has been the lack of addressing the required "balancing" of proprietary rights on the one hand, with user rights and the public domain on the other. Rights Management Information (RMI) can aid in this balancing. The RMI of a work[2] is simply data that provide identification of rights related to that work, either directly or indirectly.[3] Although the Bill aims to address the perceived lack of compliance with the World Intellectual Property Organization (WIPO) Treaties,[4] the drafters may not have seen WIPO's own Scoping Study,[5] which recommended:

> Legal means should be found to prevent the recapture of exclusivity in works that have fallen into the public domain, whether through another intellectual property right (trademark or right in databases), property rights, other legal entitlements or technical protection, if such exclusivity is similar in scope or effect to that of copyright or is detrimental to non-rivalrous or concurrent uses of the public domain work.
>
> The 1996 WIPO Treaties should be amended to prohibit a technical impediment to reproduce, publicly communicate or making available a work that has fallen into the public domain. There is no legal basis for the enforcement of technical protection measures applied to the public domain, as public domain status should guarantee the right to make re-use, modification, reproduction and communication. It could also be clarified that only technological measures protecting copyrighted works that form a substantial part of the digital content to which they apply will be protected against circumvention. Technological measures mainly protecting public domain works, with an ancillary and minimal presence of copyrighted works, should not enjoy legal protection. [6]

Bill C-32 addresses Rights Management Information (RMI) specifically.[7] Although digital works are typically the subject of RMI protection, in

---

2 The term "work" is being used here in the sense given by copyright jurisprudence, so as to restrict this discussion to RMI in data that may be appropriate subject matter for copyright.

3 For example, "by Mark Perry" indicates the authorship of this paper, which may lead to assumptions regarding moral rights or economic rights in the absence of other more detailed indications.

4 Below note 29 with discussion in text.

5 From the World Intellectual Property Organization, *Scoping Study on Copyright and Related Rights and The Public Domain by Séverine Dusollier* (30 April 2010), www.wipo.int/ip-development/en/agenda/pdf/scoping_study_cr.pdf [Scoping Study].

6 *Ibid.*, at 68.

7 Bill C-32, above note 2, s. 41.22.

its plain vanilla form RMI predates the digital content era. The breadth of RMI's impact is now much wider than the simple protection given to pre-digital works by moral rights. For example, the removal of a title and copyright information from a novel can be taken as an attempt to remove authorship information. RMI can be seen as a type of meta-data about a work. In the realm of distribution of digital works, it may be seen as akin to the right of attribution within moral rights jurisprudence, or rights of access in permissions on files in a computer operating system such as Unix.[8] Since the beginning of time, or at least since the beginning of the creation of artistic works, authors and owners of works have wished to be identified, and so have put their name with the title on the front cover, as well as the inside of the book, signed their paintings and pottery, and in some markets, used state authorized marks to authenticate source.[9] In recent centuries, such identifications have typically been accompanied by information specifically related to the rights in the works, such as by the insertion of copyright notices, publishers' information, dates, disclaimers, permissions, International Standard Book Numbers, acknowledgements and so forth, which are typically inserted on the verso of the title page inside the work in printed volumes. An early example can be seen above in the *leader* to this paper. Over the last two decades, the growth in the digital market has led to increased variety in the types of RMI accompanying works, and some would even say that RMI only became meaningful in the digital era. Herein is addressed the application of the technologies that are being used to attach RMI to digital works and the implementations of RMI-related treaty obligations in other jurisdictions, as well as examining the parts of Bill C-32 that deal with RMI.

The basic idea behind RMI for digital works is to include meta-data along with the work that provide information on the rights that are attached to the work. For example, if you play a track on your digital music player, it will typically display the title of the track and the performer on its screen. This is minimal RMI.

B. TECHNOLOGIES

RMI is a cornerstone of systems that are aimed at regulating the rights held in digital works. RMI is often used with watermarking and stegano-

8 This Unix example is used in Jonathan Weinberg, "Hardware-Based ID, Rights Management, and Trusted Systems" in Niva Elkin-Karen & Neil Weinstock Netanel, eds., *The Commodification of Information* (New York: Aspen Publishers, 1999) 343.

9 For example, hallmarking of precious metals began in Britain around 1300AD.

graphy techniques, both of which provide information over and above that contained in the primary work. Although used by technological protection measures that attempt to regulate access or replication of digital materials, the term RMI is used to identify the data *about* the content. Watermarking may use information hidden from all but an intended recipient,[10] whereas other RMI is blatant or reasonably easy (for the technically minded) to find in works, such as those in paper (for example, currency notes) or in digital music tracks (the song title and performer displayed by an MP3 player). Regardless of the technique used, information can be embedded in all types of works. Regrettably, the technology to achieve this is yet to be perfected and may involve, in some cases, the introduction of undesirable artifacts upon reproduction in some cases, for example, a reversed pixel in a photograph.[11]

There are many technologies commercially used to embed RMI in today's digital content.[12] It is also a fertile research area, both for those attempting to crack watermarking technologies as well as those developing new ones.[13] There are many types of technologies applied to RMIs, but

10 Steganography is not differentiated from watermarking in this paper and watermarking will be used as a generic term for embedded RMI. In practice, steganography is usually used to describe technologies that hide messages intended for particular recipients inside content that is available to anyone. A recent example is that of the Russian spies who put messages in picture on websites; see Caitlin Stier, "Russian spy ring hid secret messages on the web" *New Scientist* (02 July 2010), www.newscientist.com/article/dn19126-russian-spy-ring-hid-secret-messages-on-the-web.html.

11 See Brian Dipert, "Security scheme doesn't hold water (marking)" (21 December 2000) *Electronic Design News* 35, www.edn.com/contents/images/56211.pdf. For a discussion of how must steganalysis (i.e., looking for steganograpy in works) involves searching for artifacts, which give away the presence of a hidden message, see Sathiamoorthy Manoharan, "An Empirical Analysis of RS Steganalysis" in *Proceedings of the 2008 Third International Conference on Internet Monitoring and Protection* 172, (Washington, D.C.: IEEE Computer Society, 2008).

12 Most technologies that are developed by private companies are then put forward to try to get the technique approved as a standard or adopted by a major content supplier. An early standardization attempt, the Secure Digital Music Initiative (SDMI) seemed promising with 200-plus companies and organizations participating to find the answer to the problems posed to music publishers by digital technologies, but environments such as Napster and Gnutella overtook the initiative, as well as inherent weaknesses in the technology. The SDMI website (www.sdmi.org) seems non-functional and the domain name is registered by the Recording Industry Association of America (date last attempted access: 3 July 2010).

13 Over the last three years, there have been around 1,500 research papers on digital watermarking and steganography published by Institute of Electrical and Electronics Engineers and the Association of Computing Machinery.

most rely on embedding the meta-data into the supplied content and apply some level of cryptography to limit access to such information. One such is *FairPlay*. Apple iTunes includes *FairPlay* Digital Rights Management,[14] with songs that customers purchase and download, but also claims that it has "[o]ver 13 million high-quality, DRM-free songs."[15] Even though these songs do not include DRM technologies to directly control replication or playback, they do contain RMI within the file that contains the work. The overt part of such information is simple to see within the iTunes application.[16] The user can see information related to the song file, some of which will be stored locally, such as when the track was last played, the name of the work, album, singer, "(p)" owner (presumably the performer's performance), the fact that the song is a "purchased AAC audiofile,"[17] the size, bit and sample rates (of encoding), the account name, purchaser name, purchase date, date modified, number of plays, when last played, and the encoding complexity. However, it is not made clear to the user how much of this information is attached to the music file itself, what other information has been recorded and how much is kept on the local computer. With a little investigation it can be seen that in addition to the information related to the work directly (i.e., titles, copyrights, etc.), also embedded is the name of the user and the user's account identity. There may also be other encrypted information. Sometimes it is difficult to see what is strictly RMI relating to the work *itself* and what is information *about the user*. Obviously, some user information will be relevant to RMI (for example, to whom a license is granted to playback a track), but if the information is obfuscated it is unclear what is needed for RMI and what is there for the benefit of the provider's marketing efforts, rather than managing the rights in the particular work. It should be noted that *FairPlay* is not strictly a "copy protection scheme," but rather more of a "distribution

14 The FairPlay technology is a digital rights management (DRM) technology created by Apple, Inc., based on technology created by the company Veridisc. FairPlay is built into the QuickTime multimedia software and used by the iPhone, iPod, iPad, Apple TV, iTunes, and iTunes Store and the App Store.

15 See "What is iTunes?," Apple Inc., www.apple.com/itunes/what-is. As of 2009, Apple's iTunes had a 26.7% share of the total USA market, double its 2007 share, according to Billboards analysis of market data: Ed Christman, "Digital Divide" (22 May 2010) *Billboard*, www.billboard.biz/bbbiz/content_display/magazine/upfront/e3i12fe2557a93825976711a522cc1cc901.

16 Select a track on your computer from iTunes and "get info."

17 Advanced Audio Coding (AAC) coded was developed as part of the MPEG-4 specification. Details can be found at: "What is MPEG-4?," MPEG Industry Forum, www.m4if.org/mpeg4.

management scheme." For example, even with DRM loaded files, the user can make as many copies of the same work on an individual computer as he or she likes.[18]

The use of *FairPlay* by iTunes is but one common example of the many other RMI systems in place, not only for music, but also for films and video,[19] photographs,[20] software,[21] cloud services[22] — indeed most digital information supplied as content to a user on a commercial basis will carry some kind of RMI.

C. ALTERING OR REMOVING RMI

A range of technologies are used to affix the RMI to the work, from the trivial (such as the author information on this paper's digital file) to the sophisticated (such as Adobe's digital signatures using a certification authority),[23] but there are always those who will attempt to engage in removing or changing RMI. For some electronic works, simply changing the file name or deleting the RMI is an effective evasion strategy.[24] Unless a very sophisticated scheme of RMI locking or embedding is used, digital RMI remains as easy to remove for the technically minded as it is to re-

---

18 There are other aspects of such schemes which go beyond the scope of this paper, such as that they typically rely on a user contract (terms of service must be accepted before permission is granted to access and download from the system) defining the terms of use of the service. There are also some fairly simple means of circumventing such protection schemes for the computer proficient, and software is available online ready-made for those that are not so proficient. For discussion of usage contracts see Stefan Bechtold, "Digital Rights Management in the United States and Europe" (2004) 52:2 Am. J. Comp. L. 323.

19 This includes the classic Content Scrambling System (CSS) used on film DVDs and the more recent Advanced Access Content System (AACS) for Blu-Ray Discs.

20 Such as PixelSafe and PixelLive, two products offered by Celartem Technology, Inc.

21 For instance, Microsoft Office contains its own RMI entitled Information Rights Management (IRM) which allows individuals to control access to documents, workbooks, and presentations through permissions. This helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people. After a permission to a file has been created using IRM, the access and usage restrictions are enforced no matter where the information is because the permission to a file is stored in the document file itself.

22 Such as Adobe LiveCycle Rights Management.

23 For a good introduction, see "A Primer on Electronic Document Security: Technical Whitepaper," Adobe, www.adobe.com/security.

24 Although it should be noted that some word processors, such as Microsoft Word, keep a lot of information in the file without the knowledge of most users that relate to the authorship and editing of any particular work.

move printed RMI from a book by ripping off the cover and tearing out its copyright notice. As fast as technological measures are developed, new means of circumvention arise and there is a cycle of escalation in the types of technologies used. For example, iTunes, concomitant with its popularity as a music source, has undergone rapid development in response to circumvention of the technological protection measures.[25] Strong encryption techniques can slow down circumvention, however strong encryption has its own drawbacks. RMI, whether for a music file or text, which has been encrypted with strong techniques will typically take more processing time to handle, thus requiring more powerful chips or greater allocation of resources for rapid access than more weakly encrypted versions. Some techniques require authentication from a remote site, which can be inconvenient for users.[26] In other words, there is a balance required between three primary concerns of user digital materials: security, convenience, and performance. There is also a balance that needs to be struck between security and privacy regarding how much information about a user a content provider should require. In addition, although these measures are often touted as being for the protection of publishers and artists from copyright infringement, in many cases they offer publishers much broader commercial opportunities, such as getting users to pay further for use of the material in a different format or for other "added-value" services including market research and advertising. However, it is clear that the removal of (true) RMI should be discouraged: RMI can serve as a means of furthering the provenance of the often multiple and intertwined rights that may subsist in a digital work.

D. WIPO TREATMENT AND JURISDICTIONAL IMPLEMENTATION

In December 1996 two new treaties were adopted under the management of WIPO: the *WIPO Copyright Treaty* (WCT) and the *WIPO Performances*

25 Norwegian programmer Jon Lech Johansen initiated this cycle when he first enabled iTunes songs to be played on a home computer, see: A. Orlowski, "iTunes DRM cracked wide open for GNU/Linux. Seriously," *The Register* (5 January, 2004), www.theregister.co.uk/2004/01/05/itunes_drm_cracked_wide_open. Jon has since become notorious for cracking Fairplay, see: R. Levine, "Unlocking the iPod", *Fortune* (23 October, 2006), http://money.cnn.com/magazines/fortune/fortune_archive/2006/10/30/8391726/index.htm.

26 Such as with Maxis's game "Spore" which uses Sony's SecuROM technologies. This was inconvenient for users, and led to pirating and criticism by users, and was the most pirated game in 2008. At the end of that year Maxis dropped using SecuROM.

and Phonograms Treaty (WPPT).[27] These were the first treaties to address intellectual property rights in the digital network environment. To date there are eighty-eight contracting parties to the WCT, of which nine, including Canada, have signed but not ratified. Similarly, there are currently eighty-six contracting parties to WPPT, of which ten (including Canada) have not ratified.[28] The majority of countries that first adopted these measures were developing countries or countries in transition, however, now many industrialized countries have ratified these treaties.[29] For example, the entire membership of the European Community has signed these agreements and ratified them,[30] along with USA, China, Japan, and Australia. The EU ratified the WCT and the WPPT on 14 December 2009 and both came into effect on 14 March 2010.[31]

Canada has been a signatory of the WCT and WPPT since 1997 and has, for the third time since becoming a signatory, introduced a bill to entrench WCT and WPPT obligations into Canadian legislation.[32] It can be argued that the WCT and WPPT only make small extensions to copyright as prescribed in the *Berne Convention*,[33] which Canada implemented long

---

27 *WIPO Copyright Treaty*, S. Treaty Doc. No. 105-17 (1997) [WCT]; 36 ILM 65 (1997); *WIPO Performances and Phonograms Treaty*, S. Treaty Doc. No. 105-17, 36 ILM 76 (1997) [WPPT].

28 The preceding information about the WCT and WPPT is current as of 1 July 2010. See "Contracting Parties: *WIPO Copyright Treaty*," www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16; "Contracting Parties: *WIPO Performances and Phonograms Treaty*," www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=20.

29 *Ibid*.

30 *Council Decision 2000/278/EC of 16 March 2000 on the approval, on behalf of the European Community, of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty*, [2000] O.J.L. 89/6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0278:EN:HTML.

31 *Ibid*.

32 Bill C-32, above note 1

33 According to Article 1(1) of the *WIPO Copyright Treaty*, the WCT is a "special agreement within the meaning of Article 20 of the *Berne Convention*"; Article 20 of the *Berne Convention* provides that "[t]he Governments of the countries of the Union reserve the right to enter into special agreements among themselves, in so far as such agreements grant to authors more extensive rights than those granted by the Convention." See *WIPO Copyright Treaty* (20 December 1996), http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html#P87_12240, (1997) 36 I.L.M. 65 (entry into force 6 March 2002) [WCT]; *Berne Convention for the Protection of Literary and Artistic Works* (9 September 1886; last amended 28 September 1979), www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html, 1161 U.N.T.S. 3. The *Berne Convention for the Protection of Literary and Artistic Works* (9 September 1886; last amended 28 September 1979), http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html, 1161 U.N.T.S. 3. In 1998, Canada acceded to the 1971 version of the *Berne Convention for the Protec-*

ago,[34] and as well as the World Trade Organization Agreement on Trade Related Aspects of Intellectual Property Rights.[35] In other words, Canada is already complying with much of the requirements of WCT and WPPT. However, the Treaties do impose some significant new obligations and extensions to the law of copyright, most notably in connection with distribution rights, RMI, and technological protection measures (TPM) employed to control the use of copyrighted works.[36]

Following the ratifications and the entry into force of the WCT, there have been a number of jurisdictions implementing new legislation, including specific protection of RMI since the WCT defined RMI and the obligations of contracting parties in Article 12:

> **Article 12**
> **Obligations concerning Rights Management Information**
>
> (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 know-

---

tion of Literary and Artistic Works. The *Berne Convention* was first established in 1886 and has been revised and amended a number of times. The *Berne Convention* sets minimum standards of protection for authors of literary, dramatic, musical and artistic works and defines the scope and duration of protection.

34 See, e.g., Sunny Handa, "A Review of Canada's International Copyright Obligations" (1997) 42 McGill L.J. 961 at 969, where it is noted that "[a]lthough Canada did not become a signatory to the *Berne Convention* in its own right until 10 April 1928, the B*erne Convention* did apply to Canada as a colony of Britain, one of the original signatories." Canada officially ratified the *Berne Convention* with passage of the 1931 amendments to the *Copyright Act*: see *An Act to Amend the Copyright Act*, S.C. 1931, c. 8.

35 *Agreement on Trade-Related Aspects of Intellectual Property Rights* (15 April 1994) in *Agreement Establishing the World Trade Organization, Annex 1C*, www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm, 1869 U.N.T.S. 299, (1993) 33 I.L.M. 81. This was implemented by Canada through the *World Trade Organization Implementation Act*, S.C. 1994, c. 47, http://laws.justice.gc.ca/en/W-11.8/FullText.html.

36 WCT, above note 33, art. 6 (distribution rights), art. 11 (technological measures), and art. 12 (rights management information).

> 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 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. [37]

The article carries a footnote:[38]

> **Agreed statements concerning Article 12:** It is understood that the reference to "infringement of any right covered by this Treaty or the Berne Convention" includes both exclusive rights and rights of remuneration.
>
> It is further understood that Contracting Parties will not rely on this Article to devise or implement rights management systems that would have the effect of imposing formalities which are not permitted under the Berne Convention or this Treaty, prohibiting the free movement of goods or impeding the enjoyment of rights under this Treaty.[39]

Article 19 of the WPPT is essentially identical and applies to information that 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."[40] The first notable feature of these Articles in the WCT and WPPT is the knowledge requirement, or "reasonable grounds to know" for civil suits, that the removal of the RMI will be for infringement. The second point is that the treaty definitions do not restrict RMI to electronic information, though the infringement parts of the articles are aimed at electronic RMI. The implementation of RMI protection in various jurisdictions has been varied, and a brief survey is warranted in light of the Canadian proposals discussed later.

---

37 *WCT*, *above* note 33, art. 12.

38 *Ibid*.

39 *Ibid*. at n. 11.

40 *WIPO Performances and Phonograms Treaty* (20 December 1996), http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html#P143_21677, (1997) 36 I.L.M. 76 (entry into force 20 May 2002), art. 19.

E. EARLIER CHANGES IN JURISDICTIONS COMPARABLE TO CANADA

Even amongst those countries that have ratified the WCT or intend to shortly, there are significant variations in the approaches to RMI protection provided by "traditional" copyright regimes. A brief examination of the legislation in New Zealand, Japan, the European Union, and the United States highlights some of the diversity, although further discussion is outside of the scope of this overview.[41]

In 2008, New Zealand introduced an Amendment to their *Copyright Act* that received Royal Assent later that same year. This Amendment includes provisions stating that it is an offence to circumvent a TPM and it is not an offence to shift format of a copyrighted work under certain circumstances. The Amendment also provides protection for copyright management information (CMI), the equivalent of RMI.[42] Specifically, at section 226F CMI is defined as:

> . . . copyright management information means information attached to, or embodied in, a copy of a work that—
> (a) identifies the work, and its author or copyright owner; or
> (b) identifies or indicates some or all of the terms and conditions for using the work, or indicates that the use of the work is subject to terms and conditions.[43]

Further to that, at section 226H(1) the amendment specifies that:

> A person (A) must not, in the course of business, make, import, sell, let for hire, offer or expose for sale or hire, or advertise for sale or hire, a copy of a work if any copyright management information attached to, or embodied in, the copy has been removed or modified without the authority of the copyright owner or the exclusive licensee. [44]

And the act of removal of a "CMI" is criminalized in section 226J:

---

41 For a WIPO review of the legal framework in the US, EU, Australia, and Japan see World Intellectual Property Organization Standing Committee on Copyright and Related Rights, *Current Developments in the Field of Digital Rights Management* (4 May 2004), SCCR/10/2, www.wipo.int/edocs/mdocs/copyright/en/sccr_10/sccr_10_2_rev.pdf.

42 *Copyright (New Technologies) Amendment Act 2008* (N.Z.), 2008/27, www.legislation.govt.nz/act/public/2008/0027/latest/whole.html#DLM1122767.

43 *Copyright Act 1994* (N.Z.), 1994/143, http://legislation.govt.nz/act/public/1994/0143/latest/whole.html?search=ts_act_copyright+act_resel&p=1#dlm345634 , s. 226F.

44 *Ibid*., s. 226H(1).

> (1) A person (A) who contravenes section 226H commits an offence if —
> (a) A knows that the copyright management information has been removed or modified without the authority of the copyright owner or exclusive licensee; and
> (b) A knows that dealing in the work will induce, enable, facilitate, or conceal an infringement of the copyright in the work.
>
> (2) A person who commits an offence under subsection (1) is liable on conviction on indictment to a fine not exceeding $150,000 or a term of imprisonment not exceeding 5 years or both. [45]

For the New Zealand approach, it is notable that there is no distinction between digital and analogue content.

Japan was an early adopter of the attempt to address digital issues and ratified the WCT before the treaty came into force; thus it became bound by the treaties on 6 March 2002, along with the other nations that had ratified by that time. The Japanese definition of RMI generally follows the WIPO Treaties, however, there exists some specificity that is not found in other international agreements. For example, Article 2 of the Japanese Copyright Law provides:[46]

> (xxi) "rights management information" means information concerning moral rights or copyright mentioned in Article 17, paragraph (1) or rights mentioned in Article 89, paragraphs (1) to (4) (hereinafter in this item referred to as "copyright, etc.") which falls within any of the following (a), (b) and (c) and which is recorded in a memory or transmitted by electromagnetic means together with works, performances, phonograms, or sounds or images of broadcasts or wire diffusions, excluding such information as not used for knowing how works, etc. are exploited, for conducting business relating to the authorization to exploit works, etc. and for other management of copyright, etc. by computer:
> (a) information which specifies works, etc., owners of copyright, etc. and other matters specified by Cabinet Order;
> (b) information relating to manners and conditions of the exploitation in case where the exploitation of works, etc. is authorized;

---

45 *Ibid*., s. 226J.

46 Copyright Law of Japan, as Amended (19 June 2009) at Article 2, From the Copyright Research and Information Center (CRIC) website, June 2010. Translated by Yukifusa Oyama *et al*., www.cric.or.jp/cric_e/clj/clj.html.

(c) information which enables to specify matters mentioned in (a) or (b) above in comparison with other information. [47]

The Japanese definition of RMI restricts it to electronic versions. The intentional alteration or removal of RMI, or distribution of copies of works knowing there has been unlawful addition or removal of RMI, is deemed by Article 113[48] to be an infringement of "moral rights of authors, copyright, moral rights of performers or neighboring rights relating to rights management information." Excepting private use, Article 119[49] makes such actions punishable by imprisonment for up to ten years or fines up to ten million yen.[50] Notable in the Japanese legislation is the reference to moral rights and copyright, specifically linking them to RMI.

The EU adopted a Directive on "the harmonization of certain aspects of copyright and related rights in the information society."[51] In addition to EU wide harmonization, the Directive was aimed at gaining compliance with the terms of the WCT and WPPT.[52] The Directive addresses RMI in Article 7:

Obligations concerning rights-management information

1. Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:

(a) the removal or alteration of any electronic rights-management information;

(b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or

47 Copyright Law of Japan 19 June, 2009, Law No. 48 (1970), art. 2. This translation is from the CRIC website, translated by Yukifusa Oyama *et al*., www.cric.or.jp/cric_e/clj/clj.html.

48 *Ibid*., art. 113.

49 *Ibid*., art. 119.

50 Around CAN$121,000 as of 3 July 2010.

51 *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society* (EU), O.J.L. 167/10, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32001L0029&model=guichett.

52 *Ibid*. preamble para. 15.

> concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC.
>
> 2. For the purposes of this Directive, the expression "rights-management information" means any information provided by right holders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other right holder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.[53]

The adoption of this Directive meant that Member States agreed to implement it before 22nd December 2002, but only Greece and Denmark met that deadline.[54] It is interesting in that it shows the need, in the mind of the drafters of the Directive, for knowledge by the person who removes RMI and is by this act inducing, enabling, facilitating or concealing copyright infringement. Secondly it is limited to "electronic" RMI. By December 2009 the EU and its member States ratified the treaties, with the usual fanfare, but reaffirming the political preconceptions of the continuing benefits of the WIPO Treaties:

> Internal Market Commissioner Charlie McCreevy commented on the WIPO ratifications: "Today is an important day for the European Union and its Member States and WIPO. We, as a group have shown our attachment to the international system of protection of copyright and related rights. These two treaties brought protection up to speed with modern technologies. As the technological evolution ac-

---

53 *Ibid*. art. 7.

54 In a European Commission press release it is noted, "By adopting the Directive in the Council, Member States agreed to implement it before 22 December 2002. The European Court has already ruled against Belgium, Finland, Sweden and the UK — for the territory of Gibraltar — for their failure to implement the Directive. The Commission has now decided to start infringement proceedings against Belgium, Finland Sweden for non-compliance with the Court's rulings. In the case of the United Kingdom, the Commission has postponed its decision to start infringement proceedings as the UK authorities have informed the Commission that implementation in the territory of Gibraltar is imminent." See European Commission, News Release, IP/05/347 (21 March 2005), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/347&format=HTML&aged=1&language=EN&guiLanguage=en.

> celerates, protecting creators and creative industries is more urgent than ever."[55]

A common measuring stick for the implementation of WCT and WPPT provisions can be found in the United States where the early adoption of the *Digital Millennium Copyright Act* (DMCA) and case law shows both the potential and the pitfalls of such legislation. The DMCA contains provisions regulating RMI that it refers to as copyright management information.[56] The definition of CMI combines the definitions of RMI in the WCT and WPPT:

> DEFINITION — As used in this section, the term "copyright management information" means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work. . .[57]

The DMCA has two levels of knowledge requirements in this regard. Section 1202 makes it illegal (as in criminally actionable) to knowingly remove or distribute works that are known to have had their CMI removed, "knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title."[58] Thus, only those who have knowledge of the tampering with the CMI and also that the alteration is for infringing purposes, are liable. However, the alteration of a CMI to facilitate a prohibited circumvention would clearly satisfy this requirement. There is also a prohibition on the provision of false CMI for infringement purposes. There are a few particularly interesting facets of section 1202. This section specifically excludes user information in the definition; thus, the alteration of the user information that is included in the Advanced Audio Encoding information in iTunes downloaded files would not be protected by this section. Superficially this may seem surprising and even a weakness in the DMCA as RMI may require user information as noted

---

55 European Commission, News Release, IP/09/1916 (14 December 2009), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1916&format=HTML&aged=0&language=EN&guiLanguage=en.

56 The New Zealand legislation uses the same taxonomy — see above note 43 at s. 226F.

57 *Digital Millennium Copyright Act*, Pub. L. No. 105-304, § 1202 (c), 112 Stat. 2860 at 2873 (1998), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.

58 *Ibid*. at §1202(b)(3).

above, but given the way that the technology now typically binds the RMI (CMI in US parlance) with other Digital Rights Management (DRM) encoding, it could be argued that the user information so bound with DRM is covered under the other anti-circumvention provisions of the DMCA. For example, software that is tied to use on a particular computer or set of computers would probably include user information in its security paradigm (or at least machine information). The types of RMI in the definition of CMI includes the usual suspects: title of work, name of author, copyright owner, other identifying information, conditions for use, identifying symbols, and, with the exception of public performance by radio and television stations, the identification of performer, writer, director, and performer's performance. Section 1202 also includes a number of exceptions for broadcast and cable transmissions and for adoption of standards in the broadcast and cable realm. The civil remedies provided within the DMCA are found in section 1203 while the criminal offenses and penalties are found in section 1204. Both of these sections apply to circumventions outlined in the provisions of sections 1201 and 1202.[59] The DMCA definition of RMI is not restricted to electronic versions.

An early illustration of problems with the DMCA arose in 2000. It was suggested by a group of computer scientists that one of the watermarking technologies being considered in the Secure Digital Music Initiative (SDMI) had some weaknesses. In September 2000, the SDMI called on members of the public to attempt to crack several security technologies that SDMI was contemplating for use with the digital distribution of music. Contestants needed to click through a series of screens and "I Agree" buttons in order to take part in the contest in which SDMI offered a reward of up to $10,000 for each successful attack. However, in order to collect the money the contestants needed to enter into a separate agreement assigning all intellectual property rights in the effort to SDMI and promising not to disclose any details of the attack. A group of researchers was successful in attacking one of the technologies, but subsequently refused to accept the $10,000 as they wished to present their efforts in a scientific paper. After being warned by the SDMI, they decided not to present the paper and instead commenced an action against the constitutionality of the DMCA.[60] This case illustrates one of the problems common to all

59 17 U.S.C. §§1201–1204

60 "Computer Scientists Challenge Constitutionality of DMCA", Case Comment on *Felten et al. v. Recording Industry Association of America Inc. et al.,* (2001) 7:24 Andrews Intell. Prop. Litig. Rep. 5. Although this challenge failed, Felten and other researchers in this project were not pursued under the DMCA.

areas of anti-circumvention legislation, namely the dampening effect on research into the area. Although the work described here was directed at developing a means of circumventing an RMI technology, other less targeted research could also fall foul of this "catch-all" legislation.[61]

F. THE CANADIAN APPROACH

In the Copyright Reform Statement there is the suggestion that a simple following of the WCT and WPPT articles is sufficient to achieve the desired effect of modernizing copyright to meet the needs of the digital age:

> In conformity with the WCT and WPPT, the alteration or removal of rights management information (RMI) embedded in copyright material, when done to further or conceal infringement, would itself constitute an infringement of copyright. Copyright would also be infringed by persons who, for infringing purposes, enable or facilitate alteration or removal or who, without authorization, distribute copyright material from which RMI has been altered or removed. [62]

Given the evolution and growing maturity of the digital content market, a simple codification of the minimal requirements of the Treaties is unsatisfactory to meet the needs of today, let alone the future. Unfortunately, this is the approach that the Canadian federal government took when it introduced Bill C-32, its latest attempt to "modernize" the *Copyright Act*.[63] This Bill has been brought in with the explicit purpose of amending the *Copyright Act* to make it compliant with the WCT and WPPT, including prohibitions on the circumvention of technological protection measures and prohibiting tampering of RMI. This is the third such government attempt to reform the *Copyright Act* for these purposes since 2005.[64] There has been very little variation in the sections dealing with RMI over the five year period.

---

61 For example, downloading and testing software that removes user identities from RMI, or even using simple tools to uncover the content of RMI information as used for this paper, could fall foul of a broadly drafted section.

62 "Government Statement on Proposals for Copyright Reform", Government of Canada, http://strategis.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01142.html. The Bill to amend the *Copyright Act*, Bill C-32 was introduced 2 June 2010.

63 Bill C-32, above note 1.

64 Bill C-60, *An Act to amend the Copyright Act*, 1st Sess., 37th Parl., 2005, 1st session, 37th Parliament, First Reading 20 June 2005; Bill C-61, *An Act to amend the Copyright Act*, 2nd Sess., 39th Parl., 2008 First Reading 12 June 2008.

The Bill modifies the *Copyright Act* with a Canadian version of the RMI definition:

> **Definition of "rights management information"**
>
> 41.22 (4) In this section, "rights management information" means information that
>
> (a) is attached to or embodied in a copy of a work, a performer's performance fixed in a sound recording or a sound recording, or appears in connection with its communication to the public by telecommunication; and
>
> (b) identifies or permits the identification of the work or its author, the performance or its performer, the sound recording or its maker or the holder of any rights in the work, the performance or the sound recording, or concerns the terms or conditions of the work's performance's or sound recording's use.[65]

This definition is broad and not limited to electronic or digital RMI, nor to electronic or digital content — the two could be combined. For example a book could have a radio frequency identity device inserted into the cover that included RMI. Many products have such devices, primarily for asset management and market tracking.[66]

Bill C-32 aims to amend the *Copyright Act* in relation to RMI by adding the following prohibitions:

> **Prohibition — rights management information**
>
> 41.22 (1) No person shall knowingly remove or alter any rights management information in electronic form without the consent of the owner of the copyright in the work, the performer's performance or the sound recording, if the person knows or should have known that the removal or alteration will facilitate or conceal any infringement of the owner's copyright or adversely affect the owner's right to remuneration under section 19.
>
> **Removal or alteration of rights management information**
>
> (2) The owner of the copyright in a work, a performer's performance fixed in a sound recording or a sound recording is, subject to

65 *Ibid*., s. 41.22(4).

66 Indeed, RFID devices are even being used in hospitals to track patients. Jill Fisher and Torin Monahan "Tracking the social dimensions of RFID systems in hospitals" International Journal of Medical Informatics (March 2008) 77/3: "Radio frequency identification (RFID) is an emerging technology that is rapidly becoming the standard for hospitals to track inventory, identify patients, and manage personnel . . . ."

this Act, entitled to all remedies — by way of injunction, damages, accounts, delivery up and otherwise — that are or may be conferred by law for the infringement of copyright against a person who contravenes subsection (1).

Subsequent acts

(3) The copyright owner referred to in subsection (2) has the same remedies against a person who, without the owner's consent, knowingly does any of the following acts with respect to any material form of the work, the performer's performance fixed in a sound recording or the sound recording and knows or should have known that the rights management information has been removed or altered in a way that would give rise to a remedy under that subsection:

(a) sells it or rents it out;
(b) distributes it to an extent that the copyright owner is prejudicially affected;
(c) by way of trade, distributes it, exposes or offers it for sale or rental or exhibits it in public;
(d) imports it into Canada for the purpose of doing anything referred to in any of paragraphs (a) to (c); or
(e) communicates it to the public by telecommunication.[67]

The Canadian approach, thus far, is closely tied to the terms in the treaties and does not limit the definition of RMI to the digital environment, unlike its Japanese counterpart,[68] but it does restrict RMI in the infringement section, unlike the New Zealand Act[69]. The other point is that the removal or alteration of the RMI should be with knowledge that the change would be to further or conceal copyright infringement, as is common in the DMCA as well as in the New Zealand and Japanese legislation as well as the European Directive. However, the interpretation of the intent required varies between nations. Most legislation to date, with the possible exception of the proposed changes in India that are not reviewed here,[70] has taken the WCT and WPPT templates and implemented with little change.

---

67 *Ibid.*, ss.41.22(1)–(3).
68 Discussed above note 47.
69 Discussed above note 43.
70 This is discussed in Mark Perry, "Towards Legal Protection for Digital Rights Management in India: Necessity or Burden?" (draft of 23 July 2010), http://ssrn.com/abstract=1647582.

G. IS THERE A BETTER WAY?

By combining access, copying, and RMI technologies into a complete DRM environment, a content provider is able to exercise much greater control over the ways in which content can be used by consumers. Such control measures range from limiting access to particular start and end dates, the number of times a product can be used, whether it can be copied and/or the type of device on which a file can be played or transferred. RMI in itself is fairly innocuous as in its naïve form it merely states what every consumer may like to know (i.e., the provenance of the work, what can be done with the work, and when the work may be freely reproduced). Problems for the user of a work can arise when RMI is melded with user information, creating an individualized RMI for the individual user that contains information that is not available to the user. This then becomes a tool that can be used as a quasi-secret tracking device of user behaviour that may be inseparable from the total DRM system applied to the work in question. RMI in digital works offers users a possible benefit that is often overlooked: namely, that the content of the work can be discriminated at a level of granularity unseen in physical works or analogue recordings. There are potential benefits to users in that they can choose to 'buy' just one track of an album, or view a film once, without the need for the larger purchase of the whole album or cinematograph.

The WCT and WPPT, although determined to address new technologies, are arguably already technologically outdated.[71] Rather than continue to pursue piecemeal and fragmented regulatory solutions, a new, more comprehensive approach to the control of distribution of digital works could be formulated. There is an opportunity for Canada to be ahead of the curve in legislation concerning RMI, providing a unique opportunity to benefit all parties from end to end in the digital content stream. The following features introduced in legislation would provide benefits to all:

1. *Transparent*: All RMI attached or embedded in a work should be fully readable by all users;
2. *Complete* and *balanced*: RMI should identify limits on the rights claimed, e.g., parts of works that are not protected by copyright should be clear (e.g., parts in the public domain);

---

71 For example, there was not a commercial product that would allow a content creator to "trace" works over the internet at the time the treaties were developed. Digimarc advises that users of "Mywatermarc" technology are able to "Track your covertly watermarked photos on millions of pages across the public Internet." http://digimarc.com

3. *Private*: User information collected by suppliers of content should be identified, limited, disclosed (to the user) and protected;
4. *Fresh*: The information should be current.

There are technological solutions for these stated objectives, which at first sight may seem burdensome for the provider of content, or even challenging to the purposes for which RMI are employed. For example, *transparency* does not mean that the RMI should not be embedded in the work and encrypted (and thus hard to remove), rather that access to the authorized user could be provided, or the embedded content replicated as stand alone. To provide *complete* and *balanced* RMI would create a burden in the sense that content not protected by copyright would need to be identified and disclosed by the provider, but given that the provider is charging for (access to) such content, this seems a reasonable request. Aspects of securing *privacy* of user-related RMI will also create work and cost for content providers, but even without legislative changes in copyright law, this is likely to be necessary under privacy legislation. Perhaps the idea of keeping RMI *fresh* may seem daunting to some. Indeed, this may seem like a heavy transaction burden to place on the suppliers of content, as noted in an earlier Canadian study:

> Some commentators have noted that certain information currently included as "rights management information" in accordance with the definitions provided in the WCT and WPPT may change often during the lifetime of the copyright. In particular, the rights owner may often change, though the author will not, or in the case of a particular sound recording, the performer will not. Similarly, terms and conditions may not only change, but have uncertain legal validity in Canada. This may cause confusion among users and detract from a rights management regime rather than promote it. [72]

However, as we become increasingly networked, with data flowing back and forth between suppliers on a regular basis, even this doesn't seem too much to ask of a new content-provider industry. It is clear that the old relationships between distributor–publisher–rights-holders–author–consumer as determined under the "traditional" content dissemination

72 Industry Canada Intellectual Property Directorate & Canadian Heritage Copyright Policy Branch, *Consultation Paper on Digital Copyright Issues* (22 June 2001), http://strategis.ic.gc.ca/eic/site/crp-prda.nsf/vwapj/digital.pdf/$FILE/digital.pdf at 28.

framework is crumbling, and likely to need reformation within the next decade anyway.[73]

The use of RMI could move the provision of digital content into the twenty-first century; it can provide information to users *in addition to* the freedoms that they enjoy under the law. This aspect of providing the limitations on the rights of copyright holders and content suppliers is typically ignored, although it would go a long way towards balancing the legislation. This should be mandated in any reform of the Canadian copyright legislation. There is always the potential danger of confusing consumers by giving them information, but this is hardly an argument for keeping them in the dark. A framework can be developed, with the appropriate resources and timeframe, that will support informed digital work use in a fair market environment. The benefits to content publishers of RMI usage, particularly in a digital environment that uses sophisticated DRM, is clear and the evolving business models depend on them. However, this cannot be a one-sided advancement into a digital era with all the benefits accruing to business; instead, balance must be brought to all sides of the digital market. All stakeholders in creative works — creators, copyright holders and users — should be given the protection of transparency, completeness, privacy and freshness that must underpin all RMI related policy initiatives.

The Canadian initiative, Bill C-32, fails to address these issues. It has merely adopted a minimal compliance with the WCT and WPPT, an inadequate solution to the problems facing creators and users in the digital arena. This Bill is clearly an attempt to comply with the WIPO Treaties and respond to the demands of the USA to reform Canadian copyright legislation. Unfortunately, in its current form, legislators have missed an opportunity to amend the legislation to achieve a *new balance* that can address the issues of publishers with unauthorized replication of materials and the issues of consumers and users with avoiding undue impact on their (constantly eroded) privacy, ensuring the maintenance of their rights to materials in the public domain.[74]

Obviously there are many perspectives on the reform of copyright. Those that benefit in the short term from increased profit margins are likely to agree with the perspective of CRIA President Graham Henderson: "Nielsen's figures [falling album sales for 2006–2007] validate an unfortu-

---

73 This overview of Bill C-32 is not the place to discuss such developments in depth, but it would be wise for government instigated reform to at least consider the longer term evolution of the digital content environment.

74 As recognised by Séverine Dusollier in Scoping Study above note 5.

nate truth — that unabated illegal Internet music file-sharing continues to harm artists and the organizations and people behind them. They also underscore the need for updated copyright laws, mirroring those of our major trading partners, to help bring unauthorized downloading under control in Canada."[75] However, the Nielsen Company and Billboard's 2009 Canadian Industry Report shows a small decline in total album sales (2.2 percent) and a large increase in digital album sales (over 40 percent).[76] It is unwise to base long-term copyright policy on fluctuations in the market over such short terms, and clearly futile to attempt to second guess the effect of RMI policy on Canadian society as a whole by looking at a sector's market figures in isolation. If this current Bill C-32 is to meaningfully amend the *Copyright Act*, and thus affect future developments in all facets of creative endeavors aided or restrained by copyright policies, a deep and thorough review also needs to be built into the legislation. Intellectual property reform is not usually very high on the priority list of governments, despite active lobbying by self-interested parties, and it is only through embedding review into reform that the matter is likely to be considered again in the near future.

Rights Management Information is the key to giving creators, users, conducers and all other players in the content driven world, the opportunity to *know* about the works that they are involved with over and above the obvious. This is where the proposed legislation fails.[77]

---

75 Canadian Recording Industry Association, News Release, "Neilsen SoundScan Figures Confirm Canada's Weak Digital Music Market and the Sharp, Ongoing Decline in Overall Recorded Music Sales" (4 January 2008), www.cria.ca/news/08-01-08_n.php.

76 Scoop Marketing, "The Nielsen Company and Billboard's 2009 Canadian Industry Report" (4 February 2009), www.billboard.biz/billboardbiz/photos/covers/2009/Nielsen_Canada_2009.pdf at p. 1.

77 This paper is a criticism of the Bill, but the author refutes any suggestion that criticism of draft legislation implies extremism, but rather a hope for a better Canadian legislative structure on copyright.