Technological Approach: Digital Rights Management

Dr. Hina Basharat
Assistant Professor, Department of Law

Introduction

The ease of infringement and the difficulty of detection and enforcement has caused copyright owners to look to technology for protection of their works. Digital Rights Management **(**DRM) has been heralded as one such technology which would put an end to the copyright owner's woes. DRM is a generic term for a set of technologies for the identification and protection of intellectual property in digital form. It comprises Technical Protection Measures (TPMs) and Rights Management Information (RMI). TPMs refer to systems and technologies that allow copyright owners to control the access to their works, determine the types of permissible uses and terms of such uses and the ultimate distribution of their works in the digital world. RMI refers to mechanisms that identify digital works and are used to manage the provision of materials to customers[1].

TPMs can be added to the 'code' of (legitimately sold) digital music files, so that when sold they cannot simply be uploaded to file-sharing networks and duplicated for free thereafter, or so that more specific copyright license terms and conditions can be enforced. Many audio and video file types today support such an additional layer of DRM file protection. This additional code typically uses some form of cryptography to 'lock' the file to a greater or lesser extent. These TPMs are used to try to ensure end-user compliance with the limited digital rights purchased as per the download agreement, in other words as part of a DRM system. Given the high degree of overlap between DRM and TPMs the two terms are today often used as synonyms or at least without a clear distinction between the two being apparent. Restrictions can include preventing files from being played back except upon a specific authorized device (a computer or portable media player, for example) or can prevent files from being played more than a certain number of times in a given time period. WMA and WMV both support Microsoft's DRM system, Real Networks uses its own DRM system to protect songs downloaded from its online store, Apple Computer uses the 'Fair Play' system to manage the (M4P (encrypted MPEG-4 Part 14) file type) songs that can be 'bought' from its iTunes Music Store and Sony have their own DRM system, Open MG, which they use to protect songs encoded using the Sony ATRAC (Adaptive Transform Acoustic Coding algorithm). It is important to note that different companies implement quite different regulatory 'regimes' in their DRM systems, allowing widely varying degrees of end-user freedom and embodying widely differing regime 'values'.[2]

"The answer to the machine may lie in the ma-chine"[3] This statement is a poignant reminder of the circular nature of technology. If digital technology's havoc wrecking power on copyright law could be circumscribed by technological advances such as the DRM, then DRM itself could be emasculated by further technological advances. Thus technology brought to supplement legal

1 Government of U.K., Digital Rights Management: Report of an inquiry by the All Party Internet Group, 2006 (June 2006).

2 Richard Jones, "Entertaining code: File sharing, digital rights management regimes, and criminological theories of compliance"19(3) *International Review of Law, Computers & Technology* 292 (2005).

3 Charles Clark, "The Answer To the Machine Is In the Machine", in Bernt Hugeholtz (ed.), *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium* 139 (Kluwer Law International, The Hague, 1996).

measures, itself needs legal protection to do what it is meant to do-prevent unauthorized access.

At the international level, The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonographs Treaty (WPPT) adopted in 1996, together called the WIPO Internet Treaties, form the basis for legal protection of DRM. Articles 11, 12 of WCT and 18, 19 of WPPT provide for TPMs and RMI. Article 11 of the WCT obligates "*contracting parties to 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 the WCT 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."* Article 12 states that the "*contracting parties shall provide adequate and effective legal remedies against any person*" who knowingly performs any of the acts mentioned in this Article or has reasonable grounds to know that the performance of such *acts "will induce, enable, facilitate or conceal an infringement*" of any rights covered by the WCT or the Berne Convention. The prohibited acts consist of the removal or alteration of "*any electronic rights management information without authority*" and the distribution, importation for distribution, broadcasting or communicating to the public, "*without authority, works or copies of works"* with the knowledge that *"electronic rights management information has been removed or altered without authority.*"

Articles 18 and 19 of WPPT replicate the aforementioned provisions for Performances and Phonographs.

3.2.1 United States

In the United States, the U.S. Congress enacted complex anti-circumvention regulations as part of the Digital Millennium Copy-right Act (DMCA) of 1998.[4]

Under the DMCA[5]three major acts are prohibited namely: circumventing a technological measure that controls access to a work protected under Title 17 of the United States Code (which governs copyright);[6] manufacturing or trafficking in any technology, device or service that is primarily designed for the purpose of circumventing[7] a technological measure that (a) controls access to a work protected under Title 17 (which governs copyright)[8] or (b) protects the rights of a copyright owner.[9] The DMCA also states that other rights, remedies or defences to copyright infringement (including fair use) are not affected[10] and gives seven specific exemptions to the act of circumventing a technical protection system.[11] One of these exemptions given under Sec 1201(f)

4 See 17. U.S.C. 1201-1205 (2004).
5 DMCA Sec 1201
6 DMCA, Section 1201(a)(1).
7 Circumvention means 'avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure'. Section 1201(b)(2)(A).
8 DMCA, Section 1201(a)(2).
9 DMCA, Section 1201(b).
10 DMCA, Section 1201 (c).
11 DMCA, Section 1201(d)–(j). These specific exemptions pertain to: allowing non-profit libraries and education institutions to make a determination (in good faith) whether to acquire a copy of the work; activities of law enforcement and government; reverse engineering to achieve interoperability of a computer program; encryption research to investigate flaws of encryption technologies; preventing access of minors to Internet material; protecting personally identifying information; and testing security flaws and weaknesses.

is to enable reverse engineering[12] and consists of three 'reverse engineering' defences: (i) circumvention of an access control measure is allowed to enable a person to identify and analyse the elements of a program that are necessary to achieve interoperability of an independently created computer program with other programs; (ii) a person is allowed to develop and employ technological means that are necessary to enable interoperability; and (iii) the said technological means may be made available to others to enable interoperability of an independently created computer program with other programs. The section also states that the reverse engineering process must not involve copyright infringement or violate other laws.

The DMCA's prohibition of circumvention is in two parts: restriction of the act of circumventing, and restriction of tools that facilitate circumvention—one restriction on conduct, one on the instrument. In addition, rather than a simple ban on circumvention of any kind, the law creates a two-tiered restriction, distinguishing between circumvention for the purposes of unauthorized *access*, and circumvention for the purposes of unauthorized *copying*. Within the scope of the DMCA, the first is illegal, but the second is not. Since unauthorized copying would already violate existing copyright law, lawmakers did not want the DMCA to impose an additional penalty. However, the part of the statute restricting circumvention tools does not distinguish according to purpose. Therefore, ..., three of four circumvention behaviors envisioned by the law are rendered illegal by the DMCA. The problem is almost too obvious. Circumvention for the sake of copying is legal, but a tool that helps do so is not. Copying is illegal *except* when it is fair. So the fair user who wants to reproduce a work that is encrypted, and doesn't happen to be a skilled hacker, is out of luck; presumably, tools to help him would be unavailable.[13] The court even admitted that the law grants the tech-savvy a right it withholds from the rest of us: "The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress, unless Congress' decision contravenes the Constitution"[14] Which, the court decided, it did not.

3.2.2 E.U

In Europe, the Directive 2001/29/EC[15] obliges Member States to provide adequate legal protection against the circumvention of any effective technological measures[16] as well as against the removal or alteration of any electronic rights-management information.[17]

The EU Directive requires that Member States 'provide adequate protection against the circumvention of any effective technological measures', which prevent or restrict acts not authorized by the rights holder.[18] This includes prohibiting the manufacture, importation or possession of any technological device, product or service whose primary function is to circumvent a technological protection measure. The Directive also requires Member States to take

12 Reverse engineering is a process which involves analysing a technology to understand how it is designed and operates. *available at* http: // www chillingeffects. org/ reverse/faq.cgi (Visited on Apr. 17, 2013).

13 Tarleton Gillespie, "Copyright and Commerce: The DMCA, Trusted Systems, and the Stabilization of Distribution" 20(4) *The Information Society: An International Journal*, 242(2004).

14 F. Supp. 2d 346 [S.D.N.Y. 2000], p. 45.

15 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.

16 Article 6 Directive 2001/29/EC.

17 Article 7 Directive 2001/29/EC.

18 Directive 2001/29/EC, Article 6(1).

appropriate measures to ensure the legitimate interests of other parties especially beneficiaries of exceptions and limitations[19] provided by national laws.[20]

Current DRM systems, at least in theory, make it increasingly possible to control how individuals use intellectual property items, set forth permissible uses, establish prices according to the market valuation of a particular work and grant licences directly and automatically to individual users. Unfortunately, in the real world, technological protection measures have became a powerful tool of control reaching far beyond the said goals, as was well demonstrated by Lessig and invoke a certain alienation of the stakeholders, namely consumers, artists and the creative industries.[21]

DRM systems present a danger of enforcing technology monopolies and creating an oligopoly of major distributors, the volume of business of which can sustain the costs of converting to and operating a cross-border DRM system. Current DRM systems are also not tolerant of the fair uses of information, thus compromising the accessibility of works and freedoms of education and research. Furthermore, they raise privacy concerns. The feasibility of DRM largely depends on the interoperability of different systems, as well as user friendliness, which currently are future objectives rather than reality. As already noted, research into consumers' behaviour with the current online creative content confirms that users prefer not only the least expensive, but at the same time least restrictive content.[22]

DRM systems frequently introduce total control over managed intellectual property, excluding any uncompensated uses thereof, including uses that otherwise are available to the lawful licensees or society at large, so-called fair uses of intellectual property. Thus, DRM somewhat compromises the societal benefits of intellectual property, in particular reuse thereof for derivative creations or even educational uses. The latest research also suggests that DRM technologies may contribute to the pricing of intellectual property products and drive consumers away from more restrictive services.[23]

Using DRM technology, consumers are granted various usage rights that enforce the provisions of licenses granted when a song/track is purchased. Typical usage rights focus on the amount of computers the songs can be played on; the amount of burns allowed to a CD, and the number of times the songs can be transferred to digital music players. These digital music players typically are designed to playback MP3 files and more recently files encoded in selected DRM system. For example the Creative Zen Micro players (from Creative Technology Ltd) are capable of playing file formats such as MP3, WAV and protected Microsoft Windows Media Audio (WMA) files (which are encoded in its Windows Media DRM system). Unprotected WMA songs can also be played. Another concern is the interoperability of DRM. Currently no agreed framework exists to create a global DRM standard or to make current systems compatible with each other. Indeed this may be a deliberate economic strategy for companies to maintain market share in digital music sales and compatible hardware players. While this may benefit businesses, consumers may not be

---

19 This would imply exceptions and limitations (Article 5) to the reproduction right (Article 2) and the right of communication to the public (Article 3) (e.g. private use, public libraries, broadcast organizations) should be allowed. Right holders, however can limit the number of reproductions for private use given under Article 5(2)(b).

20 Directive 2001/29/EC, Article 6(4).

21 Mindaugas Kiskis & Rimantas Petrauskas, "Lessig's implications for intellectual property law and beyond them" 19(3) *International Review of Law, Computers & Technology* 309 (2005).

22 Id. at 311.

23 Id. at 310.

well served by such practices.[24]

In a DRM system, content providers are not protected by technology and anti-circumvention regulations alone. Rather, they may use contracts to oblige consumers to use the protected content only under certain conditions. In such a contractually-protected DRM system, consumers are required to enter into a contractual agreement, either at the time they acquire some DRM-enabled hardware or software, or at the time they want to access some content within the DRM system.

Most DRM usage contracts are such click-wrap licenses.[25] U.S. courts have held click-wrap licenses as enforceable contracts as well.[26] The Uniform Computer Information Transactions Act (UCITA) also accepted such licenses as enforceable contracts.[27]

Very often, before consumers acquire DRM-protected content, they are not fully aware of the specific uses which the DRM system allows and prevents. Usually DRM provider do not reveal such information and the consumers in their ignorance do not to ask for it.DRM contracts are simply a type of standard form of contract. Therefore all the procedural safeguards available in the standard form of contracts should be extended to DRM contracts. Better still, a statutory duty should be imposed on the content providers to fully disclose the scope and char-acteristics of the DRM protection they use for their content. This could ensure that the consumers make an informed decision about whether they want to buy the protected content or not. Also the statute should itself provide that in order to be valid the terms and conditions of the DRM contract should be reasonable.

3.2.3 INDIA

The Copyright Amendment Act (2012) has introduced two new sections viz. Section 65 A and 65B which aim at prohibiting circumvention of technological measures and protection of rights management information. Section 65 A declares that any person who circumvents an effective technological measure applied for the purpose of protecting any of the rights conferred by Copyright Act, with the intention of infringing such rights, shall be punishable with imprisonment and fine.[28]

---

[24] Carlisle George & Navin Chandak, "Issues and challenges in securing interoperability of DRM systems in the digital music market" 20(3) *International Review of Law, Computers & Technology*, 273 (2006).

[25] A "click-wrap license" appears on the users' computer screen and requires him to agree to the license terms before being able to use the software or service.

[26] See I.Lan Systems, Inc. v. Netscout Service Level Corp., 183 F.Supp.2d 328, 338-339 (D. Mass. 2002); Steven J. Caspi, et al. v. The Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999).

[27] See UCITA 112 (d) (2002) with Official Comment No. 5; see also UCITA 209, 211 (2002).

[28] Section 65 A: Any person who circumvents an effective technological measure applied for the purpose of protecting any of the rights conferred by this Act, with the intention of infringing such rights, shall be punishable with imprisonment which may extend to two years and shall also be liable to fine.
(2) Nothing in sub-section (1) shall prevent any person from,-
(a) doing anything referred to therein for ·a purpose not expressly prohibited by this Act:
Provided that any person facilitating circumvention by another person of a technological measure for such a purpose shall maintain a complete record of such other person including his name, address and all relevant particulars necessary to identify him and the purpose for which he has been facilitated; or
(b) doing anything necessary to conduct encryption research using a lawfully obtained encrypted copy; or
(c) conducting any lawful investigation; or
(d) doing anything necessary for the purpose of testing the security of a computer system or a computer network with the authorisation of its owner; or
(e) operator; or

That the Indian Legislation contains a rather tepid version of anti-circumvention provisions. This is something that is evident from even a cursory glance. Further analysis reveals a number of interesting things. First, the requirements for applicability of Section 65 A are:

i) There must be intention of infringing any of the rights conferred by the Copyright Act. By bringing in an element of mens rea, the legislature has raised the threshold quite high, which is a rather welcome step. Predictably, the word "intention" has not been defined. This is to provide for the myriad of situations that can crop in a continually changing digital environment. It could mean '*knowingly*', *'recklessly'* (i.e. completely disregard for consequences) *or 'wilfully'*. In defining the contours of what it means to '*intentionally'* infringe copyright for purposes of criminal liability, the courts should remember the intention of the legislature in enacting copyright law. Copyright is not about granting monopoly to copyright holders over their works but promotion of knowledge and learning. ... intellectual creation is a cumulative process – each creator of 'new' intellectual property building on his predecessors ...[29]

One very positive element in the terminology employed by the section is that it requires' intention to infringe' rather than an 'intention to copy'. This would give a lot of leeway to anyone who only wishes to make fair-use of the copyrighted work but ends up infringing the copyright. For the lay person, knowing whether a particular use constitutes infringement can be extremely difficult.[30]

ii) The technological measure must have been put in place for the purpose of safeguarding the rights conferred by the Copyright Act. The American experience with the working of DRM has perhaps prompted the Indian Legislature to predicate the protection of DRM on a finding of copyright infringement. In the U.S companies have attempted to use anti-circumvention regulations in circumstances for which they were clearly not intended: throttling competition and choking innovation. To illustrate: on October 2004, the U.S. Court of Appeals for the Sixth Circuit vacated an earlier DMCA-related injunction which a manufacturer of laser printers had sought against a manufacturer of toner cartridges that competed with the printer manufacturer's own cartridges.[31] In August 2004, the U.S. Court of Appeals for the Federal Circuit up-held a summary judgment preventing a manufacturer of garage door opener systems from using the DMCA to hinder competitors in the downstream market of hand-held portable transmitters from offering transmitters that interoperate with the manufacturer's garage door opener system.[32]

DRM systems have been also used to restrict the access and use of copyright expired works present in the public domain thereby hampering innovation as the common pool of knowledge is a repository for material that is needed for research and development and is responsible for creation

---

(f) doing anything necessary to circumvent technological measures intended for identification or surveillance of a user; or
(g) taking measures necessary in the interest of national security.
Section 65B: Any person, who knowingly,-
(i) removes or alters any rights management information without authority, or
(ii) distributes, imports for distribution, broadcasts or communicates to the public, without authority, copies of any work, or performance knowing that electronic rights management information has been removed or altered without authority's hall be punishable with imprisonment which may extend to two years and shall also be liable to fine:
Provided that if the rigbts management information has been tampered with in any work, the owner of copyright in such work may also avail of civil remedies provided under Chapter XII against the persons indulging in such acts.".

29 William M Landes and Richard A Posner, "*The Economic Structure of Intellectual Property Law*" 4, (The Belknap Press of Harvard University Press, Harvard, 2003).

30 See Mark Lemely, "Dealing with Overlapping Copyrights on the Internet" 22 *Univ. Dayton L. Rev*. 577 (1997).

31 Lexmark Intern., Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

32 Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir., Aug. 31, 2004)

of several iconic cultural images. Adobe's e-book DRM applied to novels like Alice in Wonderland and CSS technology on DVDs of public domain movies, are an attempt to shrink this common pool of free information.[33]

iii) The act which is sought to be prohibited must not fall in any of the exceptions carved out by section 52 i.e. it must not constitute fair-use. The Doctrine of fair use remains one of the most troublesome and unsettled areas of the law.[34] The doctrine has been said to be "so flexible as virtually to defy definition."[35]

iv) It must also not fall in any of the exceptions contained in Section 65A itself which include encryption research, lawful investigation, security testing, personal privacy and national security. These exceptions have been more or less borrowed from the DMCA.[36]

More importantly, Section 65A does not, unlike its western counterparts, outlaw manufacture, distribution or selling of technology that aims at circumvention of technological devices. It therefore follows that, anti-circumvention technology is not per se prohibited but use of such technology with the intention to infringe is prohibited.

One very positive point in Section 65A is that it grants copyright owners protection only against copying of their digital works[37], unlike the DMCA (Digital Millennium Copyright Act), where the anti circumvention provisions grant the owners protection of both access control and copy control over digital works. The former can provide more protection than the latter. ... The notion of an ''access right'' has been at the heart of current DRM arguments as in the absence of access no possibility of fair-use arises. Access control therefore subverts any legally permitted use of the copyrighted work under the fair-use doctrine thus compromising the societal benefits of intellectual property.

The proviso to Section 65A(2)

In order to ensure that the fair use privilege is available to everyone irrespective of the degree of their technologically knowledge the Indian Legislature enacted the proviso to Section 65A(2).It provides that any person facilitating circumvention by another person of a technological measure for such a purpose shall maintain a complete record of such other person.

The rationale for incorporation of the proviso to Section 65A(2) can be better understood after analyzing the analogous provisions of the DMCA.

Under the DMCA, circumventing technological measures for the purpose of fair use of a copyrighted work is permissible. However, the DMCA prohibits circumventing of technological measures for the purpose of unauthorized access in toto. This in effect would mean that a person wishing to make fair use of a copyrighted work that is technologically protected is entitled to do so, but his means to do so are severely curtailed. Why? the technology that would help him to decrypt the work is outlawed meaning thereby that a person should himself possess the

---

33 Nilanjana Sensarkar, "The Potential impact of Digital Rights Management on the Indian Entertainment Industry*"* 6(1) *Journal of Intellectual Property Law and Practice* 47(2007).

34 See Princeton Univ. Press v. Michigan Document Servs., 99 F.3d 1381 (6th Cir. 1996) (en banc).

35 Time Inc. v. Bernard Geis Assoc., 293 F. Supp. 130, 144 (S.D.N.Y. 1968).

36 See DMCA Section 1201(e),1201(g),1201(i), 1201(j).

37 For a contrary view see Aarthi Ashok, "Technology Protection Measures and Indian Copyright (Amendment) Act: A Comment" 17 *Journal of Intellectual Property Rights* 526 (2012).

technological know-how to decrypt a work. If he is technologically naive, he cannot look for outside help to decrypt because availability of such technology is barred. The court recognized this anomaly when it observed "The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress, unless Congress' decision contravenes the Constitution". The court however held that the impugned provision was constitutionally valid.[38]

Under Section 65 A(2), one person can be aided by another to facilitate circumvention for fair-use purposes. While this is laudable, yet one is constrained to say that the proviso has been ill-conceived. A duty is cast on the person facilitating circumvention to maintain a complete record of the person so facilitated. Sadly, the Act is silent on the consequences of non compliance with the requirements of the proviso (i.e. maintaining records) rendering it in fructuous. Further, there is nothing in the language of the Section which bars dissemination of information pertaining to circumvention of technological measures by the person who has been himself facilitated. This would mean that such person (whose records are maintained) has to maintain records in respect of any person who has been facilitated by him. Clearly, such a record keeping, akin to an endless chain is unserving of any logical legal purpose. Thus it seems that the proviso is an ill thought piece of legislation.

It is quite evident that the Indian Legislature has framed the DRM provisions while being cognizant of its working in the West. Drawing on the American experience, a number of pitfalls have been avoided. However, in a developing country like India, the necessity of having DRM provisions is debatable. It is submitted, that in order to restore the balance between the rights of the copyright owners and the rights of the public, all the procedural safeguards which are available in a standard form of contract should be extended to DRM contracts. Also, the proviso to Section 65(A) should be deleted as it is an ill conceived piece of legislation.

[38] 111 F. Supp. 2d 346 [S.D.N.Y. 2000], p. 45.