CHAPTER 5

MANAGEMENT OF INTELLECTUAL PROPERTY OF DIGITAL PRODUCTS IN NETWORKED ENVIRONMENT
The issue of management of intellectual property rights take on added dimensions and urgency in a scenario when copyrighted works are increasingly being exploited on digital networks which is indeed modifying the production, distribution, and consumption patterns of copyrighted works. Not only can users easily reproduce works in countless perfect copies and communicate them to thousands of other users, but they can also manipulate works to create entirely new products.

It’s an e-business enigma. Personal computer (PC) owners are looking for more and more of their entertainment online, as Napster and its subscription-based successors have shown. And many of the companies that own today’s most popular songs, books and movies are eager to sell their content over the Internet—if only they can find a way that’s both convenient for customers and profitable for copyright owners.
The technologies pose substantial practical challenges. In order for legal protection to remain meaningful, rightsholders must be able to detect and stop the dissemination of unauthorized digital copies, accomplished at levels of speed, accuracy, volume and distance that in the past were unimaginable. And for e-commerce to develop to its full potential, workable systems of online licensing must evolve, in which consumers can have confidence.

Digital and Information technologies combined together have made the management and administration of copyright quite difficult. It has made reproduction, distribution and communication of works easier and within the competence of ordinary individual. Now copies can be made at an amazing speed with absolute fidelity to the original and transmitted over vast distances and dispersed to millions of people in a few minutes or even seconds. This has opened up the possibilities of widespread unauthorised copying and distribution of copyrighted works materially affecting the economic interest of the owners. When such activities can be done from the privacy and safety of one’s home, law becomes an impotent, mute witness. However, the solutions devised up by technologists need to be protected by law as otherwise those solutions would be modified by counter technologies, with impunity.

As more and more digital products in network environment are emerging, efficient management and controlled distribution of such products has become one of the important considerations, as never before. Digital technologies will have to be used widely for administration of copyright in the digital environment. Licensing and fee collection may have to be automated.
Issues in Management of IPRs in Digital Networked Environment

1. Rights Management Information
   - Should law protect it?

2. Technological Protection Measures
   - Should they be made compulsory for equipment manufacturers?

3. Legal Protection Against Circumvention of Technological Protection Measures
   - To be tested vis-à-vis Public Policy and Already Existing Fair Use Provisions

4. Modification of Rights Conferred Under Copyright Law by Contractual Terms
   - To be tested vis-à-vis the Information Technology Act, 2000

5. Self-Help Measures
As a result of harsh confrontation between content industries and electronic equipment industries, and users there remains much to be articulated with the management of intellectual property on the Internet. Towards this end this chapter discusses:

- What protection is required for rights management information?
- Should implementation of technological protection measures be made compulsory for the equipment manufacturers?
- Should legal protection against circumvention of technological protection measures be included in India’s copyright legislation?
- Validity of self help measures?
- How copyright law is being supplemented by contract law?
- How anti circumvention provisions impact on fair use implicit in the philosophy of copyright law?
- Are copyright limitations overridden by copy control? How do we design interface between them?

**RIGHTS MANAGEMENT INFORMATION**

The primary requirement for the automated grant of rights in a digital context is that the protected work and subject matter can be identified as such belonging to the relevant authors and rightholders and the licensing terms must also be available electronically. On the one hand, this information must be easily readable for a potential user; on the other hand it should not be easily erasable so that it remains embodied during the subsequent stages of exploitation in connection with the work. In addition, rights holders must be able to prove their authorship and ownership of rights in case of infringement; the relevant information should not be discernible to third parties and should remain
embodied within the work even after the latter has been adapted, or where parts of the work are used.\textsuperscript{1}

This is possible only if certain data which identifies the work, the author of the work, the owner of the work, or information about the terms and conditions of use of the work which are necessary for licensing and payment of licence fee, are embedded in the work. This data is classified as “rights management information” in the WIPO Copyright Treaty (WCT) and the WIPO Performers and Phonograms Treaty (WPPT).

Rights management systems operate on the basis of electronic data that is attached to the works and objects of related rights. The data may identify the author or performer, the rightsholder, and the work or object itself, and may further describe the terms and conditions for its use. ‘Rights management information’, as a technological adjunct providing legal support to network-based rights management systems will enhance the ability of rightsholders to exploit their property on the Internet, and allow consumers to rely on the accuracy of the information they receive so they can feel secure transacting online.\textsuperscript{2}

The WCT defines rights management information as: \textsuperscript{3}

\begin{flushleft}
\textsuperscript{1} Thomas Dreier, “Copyright Law and Digital Exploitation of Works - The Current Copyright Landscape in the Age of the Internet and Multimedia”, available at: http://www.intellecprop.mpg.de/Online-Publikationen/dreier-Digi-Exploitation.html#sub, at p. 31, para 6.1.


\textsuperscript{3} Art. 12(2) of WCT. Art. 19(2) of WPPT, 1996 also defines rights management information as: “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
\end{flushleft}
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 represents 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.

Contracting parties to the Internet treaties have to provide legal remedies against any kind of removal or alteration of any of the above information as well as distribution or communication to the public of copies of work with such removals or alterations.⁴

Art. 12(1) of WCT states:

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.

⁴ Art. 12(1) of WCT, 1996.
Under the treaties, Member States must provide adequate and effective legal remedies against the deliberate removal or alteration of such information, and against the dissemination of works, performances or phonograms from which such information has been removed or altered, where these acts are performed with at least reasonable grounds to know that they will induce, enable, facilitate or conceal infringement.  

The Copyright Act, 1957 provides for certain information to be displayed on cinematographic film and sound recording:

52A. Particulars to be included in records and video films --
1. No person shall publish a record in respect of any work unless the following particulars are displayed on the record and on any container thereof, namely:--
   a. the name and address of the person who has made the record;
   b. the name and address of the owner of the copyright in such work; and
   c. the year of its first publication.

2. No person shall publish a video film in respect of any work unless the following particulars are displayed in the video film, when exhibited, and on the video cassette or other container thereof, namely:--
   a. if such work is a cinematograph film required to be certified for exhibition under the provisions of the Cinematograph Act, 1952 (37 of 1952), a copy of the

6 S. 52A, Copyright Act, 1957.
certificate granted by the Board of Film Certification under Section 5A of that Act in respect of such work;
b. the name and address of the person who has made the video film and a declaration by him that he obtained the necessary licence or consent from the owner of the copyright in such work for making such video film; and
c. the name and address of the owner of the copyright in such work. (Emphasis added)

This information could be described as a part of ‘rights management information’. But this provision is not adequate for the administration of the rights in the digital environment and further it is limited to two classes of works only. The expression “No person shall publish” appearing in section 52A sets the onus on the copyright owner to put the relevant information on record or video film before its publication. In case anyone tampers with it or removes or alters this information, there is no provision in this regard. Therefore, some provision needs to be made making it an offence to remove or alter any ‘rights management information’ used in a copyrighted work.

Section 52A talks about certain information to be put on “containers” of sound records and video films. But in the digital age copyright products like video films, sound records, software, text, etc. have become container-less. They increasingly appear as part of ‘information’ in the form of bits and bytes in cyberspace. In other words they have been liberated from carriers and containers and are being transmitted over the Internet on wires and wireless. So, rights management information has to be imbedded in the work itself. In other words, it comes together with the work and it should not be possible for the anybody to remove or detach it easily from the work.
Rights management information, in this regard, becomes extremely important from the angle of moral rights as well. In this regard, section 57 of the Copyright Act reads as follows:\textsuperscript{7}

57. Author's special right.--

1. Independently of the author's copyright, and even after the assignment either wholly or partially of the said copyright, the author of a work shall have the right--

   a. to \textit{claim the authorship} of the work; and

   b. to restrain or claim damages in respect of any distortion, mutilation, modification or other act in relation to the said work which is done before the expiration of the term of copyright if such \textit{distortion, mutilation, modification} or other act would be prejudicial to his honour or reputation:

   Provided that the author shall not have any right to restrain or claim damages in respect of any adaptation of a computer programme to which clause (aa) of sub-section (1) of section 52 applies.

2. The right conferred upon an author of a work by sub-section (1), other than the right to claim authorship of the work, may be exercised by the legal representatives of the author. (\textit{Emphasis added})

Rights management information in the digital age becomes the bedrock on which author of a work could claim his moral rights. In the digital age it has become very easy and within the reach of ordinary people to detach the author's name from the work and put someone else's name in its place; manipulate with a work so as to distort or mutilate the same. In order to assert or claim authorship and to protect his work from being manipulated, distorted or mutilated, it becomes

\textsuperscript{7} S. 57, Copyright Act, 1957.
necessary for the author to employ technology which tags trademarks etc. to any work.

The pre-conditions for this are that the participating circles first agree on which information should be embodied in which form (encoding, encryption), at which point (file, work and/or part of work). The advantage of this would be that the existing systems (e.g. ISBN, ISSN, IRC, etc.) that so far have functioned side-by-side, albeit separately, could form the basis for this development. The first examples of such systems have evolved in practice. Particular reference is made to the International Standard Work Code (ISWC) developed by the Confédération Internationale des Sociétés d'Auteurs et Compositeurs (CISAC).

A considerable amount of work is being done on “copyright tagging” and developing “unique identifiers” so that the owners of digital material will be able to identify their property wherever it is and however it has been modified or distorted. This will overcome many of the problems of identification. Moreover, this technology, together with the development of “intelligent agents” or “bots” which are capable of trolling around cyberspace identifying these tags, will help track the copyright material across the Internet wherever it may be.

Figure 5.1 is an example of watermark technology which is embedded in a work, which in this case is a map. Anybody coping the map also copies it with the watermark as well, so wherever this map traverses on the information superhighway, it carries its name tag along with. In this case the map belongs to mapsofindia.com and even if anyone copies and releases it, the person receiving it will easily decipher the source of this work. As this rights management information is the result of a technology it is also possible to erase the same with the help of technology itself. Therefore, legal recognition and protection to rights management information have been provided in WCT and WPPT and have come up in a number of national legislations which penalise anybody tampering with such rights management information employed. In this direction suitable
amendments should be made in the Indian Copyright Act on lines of the WCT and WPPT specifically including a provision on rights management information. This will help rightowners exploit their intellectual property on the Internet.

![Figure 5.1](http://www.mapsofindia.com/maps/kerala/h3s1602.gif)

**Figure 5.1**

**TECHNOLOGICAL PROTECTION MEASURES**

When a digital product is made available for access on the Internet, anyone in the world becomes capable to download the product free of charge, use it without restrictions, incorporate the product into his own product and make the resulting product available in a global network, hence competing with the product of the creator himself. This is about how technology can assist a crafty person to exploit someone else’s work digitally.

In order to fight this loss of control over the product in the digital environment the legal instruments as such are not sufficient. To a large extent the solution to a
loss in technical control should be sought in technology itself. So, it becomes extremely important for the creator to incorporate an access control mechanism or any other kind of security mechanism. The problems created by technologies need to be tackled by technologies. As Charles Clark put it, "the answer to the machine is the machine."8

Increasingly, technological solutions are being found for the problems posed by the new technologies through access control or copy control mechanisms such as encryption technology or water marking incorporated into works distributed over digital networks with a view to protecting them from illegal exploitations. Technological systems of protection include: anti-copy devices, access control, electronic envelopes, proprietary viewer software, encryption9, passwords, watermarking10, electronic lamination, fingerprinting (user authentication), metering and monitoring of usage, encapsulating copyrighted works in a tamper-resistant electronic envelope, and remuneration systems. Several industry and technology initiatives to set standards in various industries have emerged over the years, although none have yet established uniform standards for technological protection measures.

The need of technology is not only for preventing the work from being stolen and misappropriated, but also for detecting infringements and misappropriations. It is

9 Encryption, or cryptography, refers to the process of using software to encode plain text information into cipher text, which can only be decoded by the intended recipients using a key or password. The two main types are public-key encryption (asymmetric) and symmetric encryption. Refer generally to Cryptography A-Z at http://www.ssh.fi/tech/crypto/.
10 A watermark is a "pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format." See, Webopedia at http://www.webopedia.com/TERM/d/digital_watermark.html.
necessary to wait and see whether in future so-called “software agents” will search the entire global network for authorized and unauthorized usage of works, communicate the relevant information to rights holders and, where necessary, block or even destroy unauthorized data packages.11

The music industry, for example, has developed copyproof compact disc (CD) technology that prevents CDs being played on computer disc drives. Copyproofing employs various technologies either by including errors in the data encoded on the CD, which allows the disc to be played on a standard CD player, but not on a CD-ROM, or by masking audio files as data files so that the CD-ROM drive cannot recognize the music.12

To guard its content and avoid further losses, the audiovisual industry has hastened to employ copy protection technology. The industry is lobbying with hardware and software producers to implement copy protection on their devices. It is said that shortly Microsoft plans to launch a new system of copy protection for its computers. The idea is to install chips into each computer that will decode audio and video information only if it comes with an unlocking key; the computer will refuse to play content if it is not digitally signed by Microsoft or an authorized party. Hard drives will no longer be able to record certain types of information.13

The goal is for the system to quietly report to authorities any unauthorized content in the computer, and the system may be instructed to delete information from the owner's hard drive. In the United States, various efforts have been made to pass copy protection legislation that will prevent the sale of any consumer ‘digital media device’ (broadly defined as any hardware or software

---

11 Supra note 1 at p. 32, para 6.2.
that reproduces, displays or retrieves or accesses any copyright work) that does not meet Federal Government copy-protection standards.\textsuperscript{14} Perhaps the most far-reaching proposal to date to force manufacturers of electronic products to include copy protection measures in hardware has emanated from the USA, where a Bill to this effect has been proposed, the Consumer Broadband and Digital Television Promotion Bill. The legislation would require that copyright-protection mechanisms be embedded in PCs, handheld computers, CD players, and anything else that can play, record, or otherwise manipulate digital information. Perhaps unsurprisingly, the Bill has encountered a good deal of opposition both from the electronics industry and from consumers. Whether it becomes law in either its current or a modified form remains to be seen.

The situation in which India finds itself today, we should not hastily move towards making it compulsory for technology makers to implement certain copy protection standards. India has low information technology product penetration and in rural areas it is all the more limited. The computer hardware industry is fledgling and should not be asked to comply with new standards of copy protection. In case we do the same, it will not only force the hardware industry to increase prices for additional implements, it will also force consumers to pay more. Moreover, there could be compatibility problems between new and old machines. So, restraint is better than rushing as far as the implementation of copy protection technology is concerned.

\textbf{LEGAL PROTECTION AGAINST CIRCUMVENTION OF TECHNOLOGICAL PROTECTION MEASURES}

Along with the invention of technical measures for protecting copyright works in the digital networked environment, counter-technologies are developed to defeat those protection technologies making it possible to circumvent each and every

\textsuperscript{14} \textit{Supra} note 5 at para. 57.
technical protection measure by using technical means. No matter how sophisticated the technological protections employed, none are invulnerable, and it is definite that the ingenuity of pirates will increasingly make it their business to hack through encryption, pick digital locks, steam open electronic envelopes, or obliterate digital watermarks so that they could make profits by stealing and misappropriating valuable intellectual property. So, the solutions devised by technologists have to be protected by law as otherwise those solutions would be modified by counter technologies, with impunity rendering the best access control mechanisms and security measures futile in want of legal sanctions. The resulting level of insecurity could prevent rightholders from being willing to disseminate valuable materials on the Internet.

Since every kind of technical protection provokes circumvention, technical identification and control mechanisms require accompanying legal protection. In order to protect against the circumvention of technological protections applied to copyrighted products in the digital environment, provisions have been incorporated in the WCT making it obligatory for member states to provide legal protection against the circumvention of technological measures that are used by authors in connection with the exercise of their rights which are as follows:¹⁵

¹⁵ Art. 11 of WCT, 1996. (Emphasis added). Art. 19(1) of WPPT, 1996 also talks about circumvention of technological measures as:

“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 knowing that electronic rights management information has been removed or altered without authority.”
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.

At the Diplomatic Conference of 1996 where the treaties were finalised, participating countries did not agree upon the exact definition of “effective” technological measures, “adequate” legal protection or “effective” legal remedies, for copy/access control technology was still premature in 1996\(^\text{16}\) and most of the participants had no concrete idea about it. Interestingly, many countries concluded and acceded to the treaty well before the actual introduction of the digital lock to the market. Now, only after 6 years from the accession, consumers are encountering "copy-control compact disc". They complain much about inconvenience with the new product. Also, some of the copy-protection technologies temporally adopted are not free from mechanical defects, for instance, played on certain type of PCs, they may cause some hardware malfunction.

Article 11 of the WCT and 18 of the WPPT only oblige the member countries to protect technological measures that restricts acts “not permitted by law.” In other words, countries need not prohibit users from circumventing technological measures for the purpose of “permitted” use of the copyrighted work. According to the majority opinion, article 11 of the WCT requires that protection of Technological Protection Measures be granted only with respect to technologies used by rights owners in connection with the exercise of a right protected by copyright law. This means that the application of technological protection measures to public domain material does not fall within the ambit of article 11 and that it is not enough that Technological Protection Measures be "used in

connection with the exercise’ of a copyright. In other words, the circumvention of a technological protection measures in order to use a work while benefiting from one of the exceptions to copyright is, in principle, not prohibited by article 11 of the WCT.

Technological protection measures are designed to prevent, in the digital networked environment, the unauthorised access to or use of works protected by copyright. Their legal protection comes as a third, cumulative, layer of protection for rights owners, in addition to copyright protection itself and to the technical protection of works.

One of the questions that the WIPO Internet Treaties left open is what types of acts must be prohibited: the acts of circumvention themselves, the business or trafficking in circumventing technologies or both? Whereas Contracting Parties were free to implement the principle set out in articles 11 of the WCT and 18 of the WPPT according to their national legal traditions, there are significant differences in the manner in which countries have implemented this obligation. A brief overview of the implementation legislation of the United States, Japan, and Europe is provided below to understand the issue.

United States

In the United States, the Digital Millennium Copyright Act, 1998 (DMCA) added a new Chapter 12 to title 17 United States Code, which among other things prohibits circumvention of access control technologies employed by copyright owners to protect their works. Specifically, section 1201 provides in extensive detail that ‘no person shall circumvent a technological measure that effectively controls access to a work protected under this title.’ Section 1201(a)¹⁷ of the U.S.

¹⁷ S. 1201 (a), DMCA, 1998 reads:

VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOCAL MREASURES. — (1)(A) No person shall circumvent a technological measure that effectively controls access to a
work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine —

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.
Copyright Act prohibits the circumvention of a technological measure protecting the access to a work by making two different conducts unlawful:

- The act of circumvention itself and
- The business of trafficking in circumventing technology

This provision has been much criticised because it essentially creates a new 'right of access' to the works in favour of rights owners. Under the regime of the DMCA, unless the user can benefit from a specific exemption that would allow him to circumvent the technological access control to get access to a digital work, each access to the work is submitted to the conditions imposed by the copyright owner.

In addition, section 1201(b)\(^\text{18}\) of the Act prohibits the preparatory activities to the circumvention of a technological measure protecting the use of a work. The

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection —

(A) 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; and

(B) 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.

\(^{18}\) S. 1201 (b), DMCA, 1998 reads:
decision of Congress not to prohibit the act of circumventing a technological measure protecting a copyright was made because it would otherwise penalise potential non-infringing uses such as fair use. United States courts have enforced the provisions of the DMCA concerning the prohibition on the circumvention of technological protection measures already on numerous occasions with various outcomes.¹⁹

Japan

Japan has amended two statutes to address the circumvention of Technological protection measures for the purpose of complying with the WIPO Treaties. The

**ADDITIONAL VIOLATIONS.** — (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection —

(A) to “circumvent protection afforded by a technological measure” means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological 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 under this title.

two statutes are the Japanese Copyright Law and the Japanese Unfair-Competition Law. The amendments to the Copyright Law focus on the circumvention of Technological protection measures protecting works subject to copyright, whereas the amendments to the Unfair-Competition Law focus primarily on the circumvention of access control technologies. With effect from October 1, 1999, article 120bis of the Japanese Copyright Act provides as follows:

The following shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding one million Yen:
(i) any person who transfers to the public the ownership of, or lends to the public, manufactures, imports or possesses for transfer of ownership or lending to the public, or offers for the use by the public, a device having a principal function for the circumvention of technological protection measures (such a device includes such a set of parts of a device as can be easily assembled) or copies of a program having a principal function for circumvention of technological protection measures, or transmits publicly or makes transmittable such program;
(ii) any person who, as a business, circumvents technological protection measures in response to a request from the public.

The anti-circumvention provisions do not apply, for example, to devices that restrict the viewing or listening of a work, such as by encryption, because simple viewing or listening is not an act covered by copyright. Technological measures to prevent the individual use of pirated editions used for game software are not classified as technological measures too, because the act of individually using a pirated edition is not an act that is covered by copyright. Having due regard to the possible chilling effect of regulations banning every circumvention, the

20 Non-official Japanese to English translation available on the website of Copyright Research and Information Center: <http://www.cric.or.jp/cric_e/clj/clj.html>.
Japanese Copyright Law does not penalize the manufacture of the hacking device or end user's circumvention.

Article 2(1)(11) of the Japanese Unfair-Competition Law provides protection against the act of trafficking in devices and programs solely designed for circumventing an effective technological measure that restricts the recording or viewing of the content to specified parties. This provision is explained to address the problem of unauthorized descrambling of subscription satellite, subscription cable broadcasts, and pay per view services. The Japanese Unfair-Competition Law only prohibits the trafficking in devices or programs and not the manufacturing of such devices or programs or the act of circumvention itself.

**European Union**

In Europe, the legal protection of technological measures is dealt with through the Directive 98/84/EC on the legal protection of conditional access services and by article 6 of the Directive on Copyright in the Information Society. Concentrating exclusively on the provisions of the Directive on Copyright in the Information Society, it is worth pointing out that, contrary to the United States, the European Union chose not to prohibit acts relating to the access to a work, but rather chose to prohibit the actual acts of circumvention of a technological measure protecting a work, as well as the business of importing, selling or otherwise dealing with products or providing services which:

---

21 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, O.J.C.E. L 320, 28 November 1998, p. 54 – 57, art. 4 which reads as follows: ‘Member States shall prohibit on their territory all of the following activities: (a) the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices; (b) the installation, maintenance or replacement for commercial purposes of an illicit device; (c) the use of commercial communications to promote illicit devices’.
(a) are promoted, advertised or marketed for the purpose of circumvention of, or
(b) have only a limited commercially significant purpose or use other than to circumvent, or
(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

In addition, the expression ‘technological measures’ as defined under article 6(3) of the Directive means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the right holder of any copyright or any right related to copyright. This formulation differs from article 11 of the WCT, which protects technological protection measures only to the extent that they restrict acts that are not authorised by the authors or permitted by law. One could infer from this that the European legislator did not intend to allow the circumvention of a technological protection measure solely for the purpose of exercising a limitation on copyright? At this time, most Member States are still in the process of transposing the provisions Directive on Copyright in the Information Society into their national law, process which appears to be particularly challenging for the individual legislators.

India

As per the Copyright Act, 1957 knowingly making or possessing any plate for the purpose of making infringing copies of a copyrighted work is a punishable offence. The definition of ‘plate’ under the Copyright Act is very wide indeed. It includes:

22 S. 65 of the Copyright Act, 1957:
Possession of plates for purpose of making infringing copies.— Any person who knowingly makes, or has in his possession, any plate for the purpose of making infringing
any stereotype or other plate, store, block, mould, matrix transfer, negative duplicating equipment or other device used for or intended to be used for printing or reproducing copies of any work, and any matrix or other appliance by which sound recording for the acoustic presentations of the work are or are intended to be made.

This definition to a great extent provides protection for the technological measures adopted by a copyright owner. Taking a lead from Article 11 of the WCT some countries of the world have already enacted anti circumvention provisions like in Digital Millennium copyright Act, 1998 in USA, in Australia in 2000, European Directive 2002 and in Canada and Japan. The debating point for India is whether to put such provisions in the Copyright Act, 1957? Since anti circumvention provisions have bearing on the fair use provisions, the suitability of these provisions for India is discussed in the subsequent part on "co-existence between technological protection measures and limitations on copyright".

LIMITATIONS ON COPYRIGHT - FAIR USE PROVISIONS

The basic principle of copyright like other Intellectual Property Rights is the balance of the interests of the individual creator and that of the society at large.24 The limitations placed on copyright serve to balance the interests of authors against the legitimate interest of the copyright industry, users and the general public especially in freedom of information and freedom of intellectual creation. Therefore, the laws while granting exclusive rights to authors or producers of copies of any work in which copyright subsists shall be punishable with imprisonment which may extend to two years and shall also be liable to fine.

23 S. 2(t) of Copyright Act, 1957.
24 This is reflected in Art. 27 of Universal Declaration of Human Rights for understanding the philosophy behind such balancing.
creative works limit those rights in time. Even during the period of copyright certain special uses are allowed without any specific permission from the copyright owners such as for private, academic, educational, judicial or legislative purposes. The copyright limitations are inserted to ensure that the deadweight loss caused by the exclusion of non-rival uses does not outweigh the gain in social welfare which follows from the incentive to create. Clearly, in this view too much exclusion, either on the basis of the law or of technology, is intrinsically undesirable.

Copyright has never been a full property right or monopoly. Neither has copyright ever been about perfect control over copies of creative works. Rather, there have always been a number of limitations and exceptions which evolved, not only to give the author sufficient incentive to produce new works to satisfy the public interest, but also to ensure that parts of existing creative works are available to build upon in the creation of new works. Unfortunately, copy control technology doesn’t affect only pirated distribution on the Internet networks—it can prevent users from making any copies at all, even ones that formerly would have qualified as fair use. With the possibilities of digital technology, the copyright industry is trying to extend their control over the products in a manner which is in fact tighter than what was possible before.

Technically, limitations reflect each legislator’s assessment of the need and desirability for society to use a work against the impact of such a measure on the economic interests of the rights holders. The outcome of this evaluation will most often determine which limitations are laid down in national legislation and the form that each particular limitation takes. This weighing process often leads to varying results from one country to the next. Indeed, some countries have adopted a very restrictive set of limitations on copyright, like France, Luxembourg, and India, while other countries, like the United

25 L Lessig, “Intellectual Property and Code”, (1996) 11 St John’s J Legal Comment 635, 638. “While we protect real property to protect the owner from harm, we protect intellectual property to provide the owner sufficient incentive to produce such property. ‘Sufficient incentive,’ however, is something less than perfect control.”

205
Kingdom, Australia and Canada, have included extensive provisions in their legislation allowing acts to take place without the prior authorisation of the rights owner.

The limitations on copyright and related rights have never been harmonised at the international level. The limitations listed in the Berne Convention of 1971 are the result of serious compromise on the part of national delegations – between those that wished to extend user privileges and those that wished to keep them to a strict minimum – reached over a number of diplomatic conferences and revision exercises. Consequently, all but one limitation set out in the text of the Berne Convention are optional: countries of the Union are free to decide whether or not to implement them into their national legislation. These provisions are meant to set the minimum boundaries within which such regulation may be carried out.26

Limitations on copyrights are an integral part of the copyright system, for they are the recognition in positive law of the users’ legitimate interests in making certain uses of copyrighted material without obtaining permissions. In accordance with their nature as exceptions to exclusive rights, as a matter of principle the existing provisions limiting copyrights are subject to a narrow interpretation. The digital media have definite implications for limitations on copyright as they have for other substantive provisions relating to copyright. But the copyright balance has never been under as much strain as it is today. Moreover, the customary lines between creators and users of copyrighted material and between private and public acts of use are gradually fading away. Also, when new interpretations are made on existing provisions and new provisions are added to existing laws of copyright, it is but necessary to consider the effect of such extensions on the interest of the society, and to clarify the extent and scope of permitted acts.

26 Lucie Guibault, “The nature and scope of limitations and exceptions to copyright and neighbouring rights with regard to general interest missions for the transmission of knowledge: prospects for their adaptation to the digital environment” report presented to the United Nations Educational, Scientific and Cultural Organisation (Institute for Information Law, Universiteit van Amsterdam, June 2003).
The WCT contracting parties are free to provide for such provisions, provided that they do not conflict with a normal exploitation of the work and do not unreasonably prejudice the author's legitimate interests. The WCT provides for such limitations and exceptions subject to the three-step test, namely, only in certain special cases, that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interest of the author. New exceptions and limitations that are appropriate in the digital network environment can also be devised. Art. 10 of the WCT states:

(1) Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.

(2) Contracting Parties shall, when applying the Berne Convention, confine any limitations of or exceptions to rights provided for therein to certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.

The provisions of the Indian Copyright Act permit a fair dealing with a literary, dramatic, musical or artistic work for the purpose of private or academic use. But

27 Art. 10 of the WCT, 1996. Art. 16 of the WPPT, 1996 enumerates the fair use provisions as:

(1) Contracting Parties may, in their national legislation, provide for the same kinds of limitations or exceptions with regard to the protection of performers and producers of phonograms as they provide for, in their national legislation, in connection with the protection of copyright in literary and artistic works.

(2) Contracting Parties shall confine any limitations of or exceptions to rights provided for in this Treaty to certain special cases which do not conflict with a normal exploitation of the performance or phonogram and do not unreasonably prejudice the legitimate interests of the performer or of the producer of the phonogram.
because of the onset of digital technologies, the issue is fraught with serious, almost insurmountable, difficulties. Most of the fair use provisions are dependent on the distinction between private use and public use. Law permits fair dealing for private non-commercial use whereas the public, commercial use can ordinarily be done only with the permission of the right holder. This distinction gets blurred and obliterated in the digital environment where an individual is able to transmit over the Internet a work to millions of users scattered over the entire globe and who may download the same in the privacy of their homes. For example, when limitation for private copying was introduced in 1970’s, home copying was exceptional and damage for copyright owners was negligible. Now, with enormous damage made by digital copying and at the same time possibility for right holders to enforce his right to every use by the end users, rationale for preservation for private copying is only dim. In this way, we now illegalise private copy, but only through hacking copy protection. Another example could be of Access control, which in theory, conflicts with the long established “freedom to access” under traditional copyright regime. Copyright owners may not prohibit legal purchaser of his book to read it. Reading is not among his copyrights. On the other hand, with an effective access control, now he will be the gatekeeper to any “use” of the work, which might erode the careful balancing designed within copyright system. More exactly, with works equipped with access control, consumers are pressed to pay extra amount for use of “ideas” or “public domain works".28 From users’ perspective, protection of copy/access control, if introduced, must preserve the public domain.

While drafting provisions for fair use care must also be taken to ensure that the expansion of rights of copyright owners to the new digital media does not result in an unreasonable curtailment of the public’s right to access and use cultural resources of humanity as otherwise that may adversely affect cultural and technological progress.

In the context of limitations on copyright, evolutive amendments to the existing limitations are advisable. The amendments are to be guided by the principle that the exclusive rights should be limited to the smallest possible extent and to the extent necessary in order to arrive at a reasonable balance between the interests of all participants in the digital environment. Consequently, the current wording of the existing provisions should be examined from the following perspectives:

- it should be broadened where it is too narrow to fulfil the previous purpose of the relevant limitation, in a digital context;
- it should be narrowed where it embraces digital exploitation but where the interests of rights holders would thus be impaired unreasonably;
- in view of the specific nature of digital exploitation of works, the extent to which additional exceptions should be laid down to the benefit of users should be examined.\(^{29}\)

It should be clarified that digital reproduction, i.e. making of a single digital copy of a work for private use and for personal scientific use, as well as inclusion of a work in digital archives for private and personal scientific purposes is permissible without the author's consent, provided that a personal copy of the work is used as the model for the reproduction. Only personal making of copies, not making by another person should be permissible. If the above measures are adopted, it is hoped that the law will be able to take cognisance of changes brought by technology.

\(^{29}\) Supra note 1 at p. 18, para 4.5.
MODIFICATION OF RIGHTS CONFERRED UNDER COPYRIGHT LAW BY CONTRACTUAL TERMS

Digital networked technologies offer scope for the rightholders to individually enter into contractual arrangements with consumers, thanks to its structure and its interactive nature. This was quite unknown before the onset of the digital age. Contracts are thus seen, in addition to or in place of copyright law, as a ready solution for the determination of the conditions of use of protected material in the digital networked environment. Copyright regime is not the only way to protect digital contents. If you assert every use permitted by copyright law shall be absolutely kept free and not to be subject to any contractual restraint, you may be labelled as a “copyright imperialist.” In fact, we have long protected proprietary information by contract, whether the content is copyrightable or not. Trade secret law has existed as “analog lock-up.”

But, a more realistic – or perhaps pessimistic – view of contractual arrangements in the digital networked environment might be that most contracts will be in the form of ‘take-it-or-leave-it’ licences, where users will only have the choice of accepting or refusing the terms of the licence presented to them on the Internet. In other words, the digital networked environment offers no guarantee that the parties will be able to ‘individualise’ their contract in a manner that takes due account of ‘the specific features of the acts covered by the exceptions and limitations’ so that everyone is better off.

In the digital medium, the doctrine of fair use is also being watered down by a combination of legislative provisions and contractual terms. The Uniform Computer Information Transactions Act of the U.S which has recommended the insertion of section 2B in the Uniform Commercial Code provides legality to click wrap, shrink-wrap and web wrap licences and contracts. This enables the hi-tech companies to curtail the freedom of users to deal with the digital products by

30 Supra note 28.
means of imposing legally binding contractual terms which extend to the gagging of fair use in digital products thus extending the reach of copyright protection far beyond the scope envisaged under the legislative provisions. In case a contractual term curtails fair use – what should prevail, statutory fair use or contract? In our opinion, since fair use provisions are designed keeping in mind the public interest and in order to foster future creativity, modifications in fair use provisions by contracts should not be permissible. In other words, the provisions of Copyright Act should prevail on individual contracts in case of fair use.

**CO-EXISTENCE BETWEEN TECHNOLOGICAL PROTECTION MEASURES AND LIMITATIONS ON COPYRIGHT**

The intersection between technological protection measures and limitations on copyright is undeniably the thorniest issue confronting lawmakers around the world in the field today. As much as the protection regimes differ from one another regarding the protection against acts of circumvention of technological measures, so do the solutions put in place to allow legitimate users to be able to exercise limitations on copyright with respect to works protected by such technological protection measures.

The measures put in place by the legislatures are far from being fully satisfactory and there is reason to fear that the exercise of legitimate limitations on copyright may be seriously compromised in the digital networked environment through the application of technological protection measures. In fact, the generality of the international obligations regarding the adoption of adequate legal protection and effective legal remedies against the circumvention of effective technological measures has left the nations with the difficult task of devising new rules, which do not fit well in the overall copyright framework. Let us examine the provisions incorporated in a few countries in this regard.
United States

In the United States, the Digital Millennium Copyright Act, 1998 contains a number of exceptions to the prohibitions laid down in section 1201 of the Copyright Act. The main exception relates to section 1201(a), the provision dealing with the category of technological measures that control access to works. Section 1201(a)(1)(B)-(E) establishes an ongoing administrative rule-making proceeding to evaluate the impact of the prohibition against the act of circumventing such access-control measures. The Librarian of Congress may, on the recommendation of the Register of Copyrights, exempt certain classes of works from the prohibition against circumvention of technological measures that control access to copyrighted works. The purpose of this proceeding is to determine whether there are particular classes of works as to which users are, or are likely to be, adversely affected in their ability to make non-infringing uses due to the prohibition on circumvention of access controls. In conducting such rulemaking, the Librarian must take account of the following aspects:

(i) the availability for use of copyrighted works;
(ii) the availability for use of works for non-profit archival, preservation, and educational purposes;
(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and
(v) such other factors as the Librarian considers appropriate.

Following a first rulemaking proceeding conducted in 2000, the Librarian of Congress announced that two classes of works were subject to the exemption from the prohibition on circumvention of technological measures that control

31 Supra note 17.
access to copyrighted works: compilations consisting of lists of websites blocked by filtering software applications; and literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence. A new round of rulemaking started in October 2002, requesting interested parties to make comments before 18 December 2002 on whether there are particular classes of works as to which users are, or are likely to be, adversely affected in their ability to make non-infringing uses due to the prohibition on circumvention.32

Section 1201(e)33 of the U.S. Copyright Act lays down an exception to the operation of the entire section, for law enforcement, intelligence, and other governmental activities. Six additional exceptions to the prohibition on the circumvention of technological measures protecting the access of works included in the DMCA deal with reverse engineering, encryption research, protection of minors, personal privacy, security testing and non-profit library, archive and educational institutions. The prohibition on the act of circumvention of access control measures is subject to an exception that permits non-profit libraries, archives and educational institutions to circumvent solely for the purpose of making a good faith determination as to whether they wish to obtain authorized access to the work. This exception is of a rather limited practical significance since its application is restricted to acts accomplished for the purpose of deciding whether a library will obtain authorised access to a work.

32 Supra note 26.
33 S. 1201(e), DMCA, 1998 reads:

*LAW ENFORCEMENT, INTELLIGENCE, AND OTHER GOVERNMENT ACTIVITIES. —* This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term “information security” means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.
Finally, while section 1201(c)(1)\textsuperscript{34} specifies that ‘nothing in this section shall affect rights, remedies, limitations, or defences to copyright infringement, including fair use, under this title’, it does not apply to the circumvention of a technological measure protecting the access to a work since access is not a right protected under the Copyright Act. Indeed, emerging case law from the United States courts shows that fair use constitutes no defence to acts of circumvention of technological measures.\textsuperscript{35}

Scholars are concerned that Sections 1201 to 1204 of the DMCA will have a chilling effect on analysis, research, and publication, as the result of litigation itself or of the threat of or concern about potential litigation. The anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA) are having ‘substantial negative impacts on the conduct of basic research in the U.S.’ Among other issues, the computing community as a whole considers that the law prevents scientists and technologists from pursuing legitimate research related to cryptography and other computer security areas.

Japan

The amendment brought in 1999 to the Japanese Copyright Law deals only very partially with the question of the intersection between the application of technological protection measures and the exercise of limitations on copyright. Article 30(1)(ii) carves out from the private copy exception the case: \textsuperscript{36}

\begin{itemize}
\item \textsuperscript{34} S. 1201(c)(1) reads:

\begin{quote}
Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.
\end{quote}


\item \textsuperscript{36} Non-official English translation available on the website of Copyright Research and Information Center: <http://www.cric.or.jp/cric_e/clj/clj.html>.
\end{itemize}
[w]here such reproduction is made by a person who knows that such reproduction becomes possible by the circumvention of technological protection measures or it ceases to cause obstruction, by such circumvention, to the results of acts deterred by such measures ("circumvention" means to enable to do acts prevented by technological protection measures or to stop causing obstruction to the results of acts deterred by such measures, by removal or alteration of signals used for such measures; the same shall apply in Article 120bis, items (i) and (ii) ("removal" or "alteration" does not include such removal or alteration as is conditional upon technology involved in the conversion of recording or transmission systems).

In other words, this provision excludes from the application of Article 30 only those copies that are made in bad faith after circumvention of technological protection measures. The status of the remaining limitations enumerated in the Japanese Act in relation to the circumvention of technological protection measures is highly uncertain, since the amendment of 1999 made no explicit reference to any one of these limitations. Opinions of scholars are divided on this issue: some argue that technological protection measures can be circumvented in order to benefit from a limitation, while others maintain that limitations are only default rules of law, which may be set aside by contract or technology. This matter will eventually have to be resolved by the courts, presumably on the basis of public policy considerations.

The only express exemption mentioned in the Japanese Unfair-Competition Law is provided in article 11(1)(7) of the Act. This provision makes it lawful to distribute devices used for testing or researching on technological protection measures in order to foster the development of technological improvements. Proposals for the inclusion of an exemption to allow the distribution of devices used for purposes of reverse engineering were abandoned in response to the
lobby of the content industry. The new Japanese rules may in theory allow the act of circumvention, particularly when this act is aimed at benefiting from a limitation on copyright, but in practice may prevent its exercise.\textsuperscript{37}

**European Union**

In Europe, the issue of the intersection between technological protection measures and limitations on copyright and related rights is dealt under article 6(4) of the Directive on Copyright in the Information Society. It provides that, in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned, Member States must take appropriate measures to ensure that right holders make available the means of benefiting from a certain number of limitations, to the extent necessary to benefit from these limitations and where that beneficiary has legal access to the protected work or subject-matter concerned. The limitations aimed by this provision are:

- Acts of reproduction by means of reprographic equipment;
- Acts of reproduction by publicly accessible libraries, educational establishments or museums, or by archives;
- Ephemeral recordings of works made by broadcasting organisations;
- Reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons;
- Use for the sole purpose of illustration for teaching or scientific research;
- Uses for the benefit of people with a disability;
- Use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

\textsuperscript{37} Supra note 26.
This provision probably raises more questions than it pretends to answer. Among the several questions left unanswered by the Directive are the following:

- What type of voluntary measures must be put in place by rights owners?
- What are the criteria for considering the appropriateness of the measures taken by the rights owners?
- How long must Member States wait before taking action and what type of action be instituted? More fundamentally, why have some limitations been included in the list and not others, such as the right to make reproductions for purposes of criticism, research, news reporting, and parody?

The whole effect of this provision may be further undermined by the fourth indent of article 6(4) which provides that:

> The provisions of the first and second subparagraphs shall not apply to 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.

The key purpose of this provision is to promote the conclusion of contractual agreements between copyright owners and users. If the parties are left alone for a while, they will certainly be able to work out appropriate arrangements with due attention to the specific features of the acts covered by the exceptions and limitations listed in the first paragraph. This is a rather optimistic view of how contractual arrangements will take form in the digital networked environment. A more realistic – or perhaps pessimistic – view of contractual arrangements in the digital networked environment might be that most contracts will be in the form of ‘take-it-or-leave-it’ licences, where users will only have the choice of accepting or refusing the terms of the licence presented to them on the Internet. In other words, the digital networked environment offers no guarantee that the parties will
be able to ‘individualise’ their contract in a manner that takes due account of ‘the specific features of the acts covered by the exceptions and limitations’ so that everyone is better off.38

It is still too early to tell how the different Member States will implement this complex provision. The safest way to follow for the Member States would unquestionably be to keep their implementing legislation close to the wording of the Directive. As a consequence, the intersection between the application of technological protection measures and the exercise of limitations on copyright may remain vague for quite some time before the practicable solution can crystallise in the law. In practice, it is difficult to conceive how these rules may work out for institutions and individuals. For instance, what would be the point for a rights owner to provide the means to circumvent a technological protection measures for the making of a reprographic reproduction on paper or other similar support? Under the regime of article 6, libraries can only hope to obtain the means to circumvent a technological measure for certain acts of reproduction of works for purposes of preservation or restoration, not for communication to the public. While Recital 48 of the Directive on Copyright in the Information Society declares that the legal protection afforded technological protection measures must not create an obstacle to cryptography research, it remains to be seen how legislators and courts will interpret the exception listed in article 6(4) of the Directive allowing circumvention for the sole purpose of illustration for teaching or scientific research.

Challenge for India to legislate

The digital networked environment has this paradoxical effect that, on the one hand, users can easily reproduce works in countless perfect copies and communicate them to thousands of other users, but that, on the other hand, rights owners are in a better position than in the analogue world to dictate the

38 ibid.
terms of use of their works. Encryption methods and other similar techniques allow rightholders to control the use made of their works more effectively. Some of these techniques can have the effect of blocking access to the work altogether, while other techniques permit rights owners to monitor the actual use that a person makes of a copyrighted work with relative ease. Moreover, the digital environment fosters the conclusion of contracts, thanks to its structure and its interactive nature. Contracts are thus seen, in addition to or in place of copyright law, as a ready solution for the determination of the conditions of use of protected material in the digital networked environment.

Technological protection measures allow the exclusion of uses. However, while copyright is limited in many ways (by its term, its object, the scope of the restricted acts and the explicit statutory exemptions), exclusivity based on technology is potentially unlimited. It may, for example, be possible by way of technology to exclude others from using information which is not copyrightable, or to exclude acts which are not restricted acts under copyright, either because they do not fall under the definitions of the exclusive rights or because they are explicitly exempted by way of fair use.39

How should the legislator then deal with this phenomenon of expanding exclusion? Should he maintain the information policy which is expressed in copyright law - of which the limitations on the right are an integral part - or should he endorse the broader exclusivity based on technology? Do the changing circumstances in the on-line environment require more or less exclusivity? In analyzing what the proper approach might be, a distinction must be made between the scope of protection of technologies which control access to information and copy-controlling technologies.

It appears to be difficult to reconcile an effective protection of technological measures with (all) the limitations on copyright. Technology - at this stage - is simply not developed enough to accommodate all the subtleties of the law. The applicability of many exemptions depends upon the circumstances. To quote the same part of the same work, for instance, may be permissible in one situation and an infringement in another. Technology cannot recognize whether a particular quotation is allowed or not. A technological measure which blocks copying will therefore block both the infringing and the non-infringing use. A legislator could decide that the copyright limitations are of such importance that it is appropriate to forbid the technological blocking of uses which cannot be prohibited on the basis of copyright. However, such a provision would likely amount to a complete prohibition on applying copy-protection technologies, since any copy-protection technique will, under certain circumstances, hinder acts of reproduction that do not constitute an infringement.

An alternative approach would be to allow the technological exclusion of any use, but to permit at the same time the circumvention of the measure, if such circumvention is necessary to perform a non-infringing act. But, again due to the inherent crudeness of technology, this approach cannot reconcile the protection of technological measures with the copyright limitations either. Most people lack the technical abilities to circumvent. They are dependent on circumvention devices supplied by third parties. If these devices are not available, most people will, therefore, not be able to crack a technological measure for the purpose of performing a non-infringing act and, consequently, activities not covered by copyright may effectively be blocked by way of technology. Only with the rightholder’s permission can the blocked act in fact be performed. Clearly, if circumvention devices are not available, the copyright limitations will lose their meaning. However, as with technological measures, circumvention devices cannot distinguish between infringing and non-infringing uses. Therefore, if circumvention devices are freely available, anybody can obtain them to engage
in infringing activities and the protection of technological measures will supposedly not have a large impact in practice. Perhaps one might then just as well decide not to protect technological measures at all.40

It appears that the legislator must decide either to maintain the (copyright) limitations on the control that an information producer can exercise over the use of information, or to in effect protect technological measures. In ascertaining which is the right approach, it seems appropriate to look at the different justifications given for the copyright limitations and to assess whether they remain valid in the digital environment.

Two main rationales can be distinguished for the limitations of copyright. One view is that the copyright limitations are the result of balancing the copyright holders' interests with the countervailing interests of information users. Imagine, for example, that ideas were copyrightable. Rightholders could then control the use of ideas which obviously would be to the detriment of public discourse. This could serve as an explanation for the limitation of the object of the right. A similar argument may lay at the root of limitations which allow quotations or copying in news media. Copyright, according to this view, is limited to the extent that the interest in a free flow of information outweighs the rightholders' interests.

Applying the different ways of reasoning to the question of what the appropriate scope of protection of technological measures would be, leads to ambiguous results. Arguments can be made for a statutory backing of technological exclusion as well as against it. One reason put forward to sanction the broader exclusivity based on technology is the presumed vulnerability of the copyright holder in the digital environment. To make perfect copies and to distribute a work world-wide becomes much easier. Anybody can be a pirate at almost no cost.

Mass infringement is feared. In the balancing process - whether it is a balancing of rights or interests, or instead a balancing of incentive versus non-rivalry in the economic approach - the copyright holder loses out. To even the scales again, some weight should be added to the rightholders' side. More exclusivity is needed. Thus, it is argued that protection of the extra control which technological measures provide for is justified by the loss of control over the use of information in the digital environment. Another often-mentioned argument to expand the scope of control over information uses is that transaction costs will go down in the on-line environment. Contracts will be concluded and enforced automatically - and therefore cheaply - through the application of technological measures. These measures facilitate the internalisation of external effects to a further extent than is possible in the off-line world. Therefore, according to this view, uses which currently do not fall within the scope of copyright because they are of low value should, in a world where technological measures exist, be controlled by the rightholder.

It is uncertain how the information market will develop. The 'digital revolution' may have more advantages than disadvantages for rightholders. Clearly, the emerging possibility to directly market information products on-line and to establish lasting customer relations may be conducive to the generation of more revenue. Also, as the costs of printing and of distribution become much lower not only for pirates, but also for rightholders, they will be able to sell their products at a lower price, even if the profit per unit sold remains the same. Since demand will go up, when the price goes down, more units may be sold and total profit may rise. Additionally, it may be that the enforcement of copyright will be much cheaper and easier in the on-line environment than it is in the off-line hard-copy world. By using search-engines infringing material can be traced automatically. Streamlined notice and take-down procedures may facilitate the cheap and rapid cessation of infringing activities.\textsuperscript{41} If the limitations are regarded as the result of a

balancing process and if copyright owners will indeed be better off in the on-line
environment, there is no need to protect by way of statute the enhanced
exclusivity based on technological measures. It can even be argued that less
exclusivity is needed.

A final reason not to protect technological measures could be that such
protection may not solve the problem it intends to address. Mass infringement
may still occur, but not of copyright but of the protection of technological
measures. The same problems that allegedly arise in enforcing copyright may
arise in enforcing an anti-circumvention prohibition. If the prohibition will be
violated en masse, enforcement will be just as unfeasible as it is to enforce
copyright itself. A more realistic strategy may be for rightholders to target
circumvention devices rather than persons who actually circumvent. As stated
above, if circumvention devices are not available, most people will be unable to
circumvent anyway. However, recent examples show that circumvention devices
(e.g. DeCSS) may proliferate over the internet as do infringing copies. 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.42

The above analysis shows that no definite conclusions can be drawn as yet.
There are no easy answers. Assuming that copyright law reflects some sort of
balancing process, it is too early to know whether - to even the scales again
more weight should be attached to the copyright holders' interests or rather to the
interests of information users. Moreover, the technologies which will be used for
circumvention of technological protection measures will also have many other
uses different from inducing copyright infringement. In this situation, including an

42 Supra note 40.

42 Supra note 40.
anti circumvention provision in the Copyright Act will only be an exercise in futility. So, for now no such provision is needed in the Indian statute on Copyright.

**SELF-HELP IN MANAGING INTELLECTUAL PROPERTY**

Apart from managing intellectual property through technological measures and accompanying legal provisions the copyright industry is also employing considerable self-help measures. The industry is relying on such self-help countermeasures since other efforts to thwart piracy on the Internet are not working to give desired results. The duel between industry and their opponents who want to obtain more and more products free of cost is turning into a high-tech arms race, as each side boosts the stakes with digital weaponry.

**File spoofing**

The copyright industry is targeting P2P networks via spoofing. It means posting corrupt or misleading files to discredit P2P network files. File spoofing calls for flooding P2P networks with decoy downloads created with the approval of the copyright owner. It appears to be one of the most effective methods of preventing P2P sharing. Spoofing makes it hard to find real media in a P2P search because the decoys, which may be ads or low-quality media, can vastly outnumber the pirated versions. For the most part, file spoofing is being kept low profile.43 Musicians typically don't admit they're hiring techies to spoof, so it's hard to tell how widespread the practice is. Rap singer Eminem and the band 'The Bare Naked Ladies' are among those known to spoof.44

---

44 Ibid.
For more than a year, the technical consulting firm Overpeer has distributed hundreds of millions of files every month on the leading P2P networks, says Mark Morgenstern, chief executive officer. He says the company is very successful at intervening for their clients to protect copyrighted music, games, video, and software. He measures their success by how often users access Overpeer files when apparently seeking pirated content. Overpeer also keeps a low profile; the company’s Web site offers no information but a street address in New York City and an e-mail address. Morgenstern emphasizes that Overpeer’s clients are the copyright holders, and its work is protecting copyrighted material.

Swamping the Search

A second tactic of P2P foes, interdiction, targets the search process. It repeatedly requests media on a P2P network, starving out other searches by occupying the request line so others cannot access it. The method resembles a denial of service attack, which involves bombarding a specific Web server with so many requests for information that it can’t keep up and crashes.

46 Supra note 43.
47 On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money. See, http://searchsecurity.techtarget.com/sDefinition/0,.sid14_gci213591,00.html.
Because P2P connections are created temporarily by whatever computers are logged in at any given time, experts fear that innocent bystanders could also be hurt through a denial-of-service attack.

**Validity of self-help measures**

There is a move to adopt new laws that would validate self-help measures. But there are great dangers in that. On July 25, 2002, a bill was introduced in the House of Representatives of the USA that allows copyright owners to "be able to use reasonable, limited self-help measures" to stop the unauthorized sharing of their copyrighted materials on P2P networks. The bill is designed to enable copyright owners to fight individuals trading copyrighted files through the P2P networks. This bill will allow hacking into computers to look for copyrighted information, blocking of file transfers, and adding fake files into the information stream to fool downloaders. Copyright owners would be provided a safe harbour in which they could disable, interfere with, block, divert or otherwise impair trading through a peer-to-peer network without criminal or civil liability.

Opposition to the Peer-to-Peer Prevention Act has been fierce. Fred von Lohmann of the Electronic Fronteir Foundation states, "the bill allows copyright owners to violate the law and this is a power that has never been granted to law enforcement and never to a single industry."\(^48\) He describes the law as "Government Sanctioned Vigilantism" where copyright owners are allowed to ignore the law in pursuit of those they deem guilty and can do so without a warrant, no trial, no due process, and little recourse to the innocent bystander who may be affected.\(^49\) Fred von Lohmann is not defending those who do trade copyrighted material without permission. He is concerned for the innocent bystanders who will be hurt by this bill. He gives an example if a person is using a cable modem (most cable modems are part of a shared network) and the RIAA


\(^{49}\) Ibid.
launches an attack against your neighbour, it may also impair your ability to access the Internet. Many people argue the bill does not specify the particular kind of attack that may be used and does not have a sufficient fix if a computer is wrongfully targeted. This bill applies only to P2P file trading while ignoring all the other ways of piracy over the Internet.

But as of today many of the self-help measures would strictly speaking be termed illegal when tested on the touchstone of laws like the Information Technology Act, 2000 of India. Section 43 of the IT Act states:

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,—

(a) accesses or secures access to such computer, computer system or computer network;
(b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;

---

50 Ibid.
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) “computer contaminant” means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) “computer data base” means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data
or instruction is executed or some other event takes place in that computer resource;
(iv) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means. (Emphasis added)

As stated above, many of the self-help measures would lead to either denial of service\textsuperscript{52}, damage\textsuperscript{53} or disruption\textsuperscript{54} of computer networks. So, they may be termed as unlawful under the IT Act, 2000. Introducing viruses to discredit P2P networks also would lead to introducing computer contaminant\textsuperscript{55} in a computer network. Further section 66 talks about hacking states\textsuperscript{56}:

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both. (Emphasis added)

Spoofing, swampimg or any other measures adopted on the Internet may also lead to unwanted damage to computers, networks or servers belonging to persons who may have played no role in alleged copyright infringement. In the light of this it is not wise to adopt self-help measures in managing intellectual

\textsuperscript{52} Covered by s. 43(f), Information Technology Act, 2000.
\textsuperscript{53} Covered by s. 43(d), Information Technology Act, 2000.
\textsuperscript{54} Covered by s. 43(e), Information Technology Act, 2000.
\textsuperscript{55} Covered by s. 43(c), Information Technology Act, 2000.
\textsuperscript{56} S. 66, Information Technology Act, 2000.
property on the Internet. Moreover, any move to validate any of the self-help measures should not be encouraged in India as is being done in the USA.

CONCLUSION

The primary requirement for the automated grant of rights in a digital context is that the protected work and subject matter can be identified as such belonging to the relevant authors and rightholders and the licensing terms must also be available electronically. Rights management information which identifies the work, the author of the work, the owner of the work, or provides information about the terms and conditions of use of the work which are necessary for licensing and payment of licence fee, are essential in the digital networked environment and must be protected by law.

Rights management information in the digital age has become the bedrock on which author of a work could claim his economic and moral rights because in the digital age it has become very easy and within the reach of ordinary people to detach the author’s name from the work and put someone else’s name in its place; manipulate with a work so as to distort or mutilate the same. Therefore, legal recognition and protection to rights management information have been provided in WCT and WPPT and have come up in a number of national legislations which penalise anybody tampering with such rights management information employed. In this direction suitable amendments should be made in the Indian Copyright Act on lines of the WCT and WPPT which will help rightowners exploit their intellectual property on the Internet.

When a digital product is made available for access on the Internet, anyone in the world becomes capable to download the product free of charge, use it without restrictions, incorporate the product into his own product and make the resulting product available in a global network, hence competing with the product of the
creator himself. In order to fight this loss of control over the product in the digital environment the legal instruments as such are not sufficient. To a large extent the solution to a loss in technical control should be sought in technology itself. Increasingly, technological solutions are being found for the problems posed by the new technologies through access control or copy control mechanisms such as encryption technology or water marking incorporated into works distributed over digital networks with a view to protecting them from illegal exploitations. The debating point here is that should we make it compulsory for hardware manufacturers to employ copy control mechanisms?

The situation in which India finds itself today, we should not hastily move towards making it compulsory for technology makers to implement certain copy protection standards. India has low information technology product penetration and in rural areas it is all the more limited. The computer hardware industry is fledgling and should not be asked to comply with new standards of copy protection. In case we do the same, it will not only force the hardware industry to increase prices for additional implements, it will also force consumers to pay more. Moreover, there could be compatibility problems between new and old machines. So, restraint is better than rushing as far as the implementation of copy protection technology is concerned.

Apart from managing intellectual property through technological measures and accompanying legal provisions the copyright industry is also employing considerable self-help countermeasures since other efforts to thwart piracy on the Internet are not working to give desired results. There is a move to adopt new laws that would validate self-help measures. But there are great dangers in that and any move to validate any of the self-help measures should not be encouraged in India.

The copyright limitations are inserted to ensure that the deadweight loss caused by the exclusion of non-rival uses does not outweigh the gain in social welfare.
which follows from the incentive to create. There have always been a number of limitations and exceptions which evolved, not only to give the author sufficient incentive to produce new works to satisfy the public interest, but also to ensure that parts of existing creative works are available to build upon in the creation of new works. Unfortunately, copy control technology doesn't affect only pirated distribution on the Internet networks--it can prevent users from making any copies at all, even ones that formerly would have qualified as fair use. In the context of limitations on copyright, evolutive amendments to the existing limitations are advisable. The amendments are to be guided by the principle that the exclusive rights should be limited to the smallest possible extent and to the extent necessary in order to arrive at a reasonable balance between the interests of all participants in the digital environment. It should be clarified that digital reproduction, i.e. making of a single digital copy of a work for private use and for personal scientific use, as well as inclusion of a work in digital archives for private and personal scientific purposes is permissible without the author's consent, provided that a personal copy of the work is used as the model for the reproduction. Only personal making of copies, not making by another person should be permissible.

In the digital medium, the doctrine of fair use is also being watered down by a combination of legislative provisions and contractual terms. This enables the hi-tech companies to curtail the freedom of users to deal with the digital products by means of imposing legally binding contractual terms which extend to the gagging of fair use in digital products thus extending the reach of copyright protection far beyond the scope envisaged under the legislative provisions. Since fair use provisions are designed keeping in mind the public interest and in order to foster future creativity, modifications in fair use provisions by contracts should not be permissible.

Employing copy protection may become necessary for copyright holders in the digital age; otherwise everybody would be free to use the digital product without
paying for the same. But this copy protection can also lead to further restrict the fair use of a copyrighted work, thereby affecting the public interest implicit in the concept of copyright. The intersection between technological protection measures and limitations on copyright is undeniably the thorniest issue confronting lawmakers around the world in the field today and there is reason to fear that the exercise of legitimate limitations on copyright may be seriously compromised in the digital networked environment through the application of technological protection measures.

Along with the invention of technical measures for protecting copyright works in the digital networked environment, counter-technologies are developed to defeat those protection technologies making it possible to circumvent each and every technical protection measure by using technical means.

Circumventing an effective copy control might be regulated as a preparatory act for copyright infringement or a kind of “indirect, contributory” wrongdoing. Should the law then penalize manufacture of the hacking device or end user’s circumvention? Legislating in this area is fraught with danger as potential chilling effect resulting from a regulation banning every circumvention need be considered too. Assuming that copyright law reflects some sort of balancing process, it is too early to know whether - to even the scales again more weight should be attached to the copyright holders' interests or rather to the interests of information users. Moreover, the technologies which will be used for circumvention of technological protection measures will also have many other uses different from inducing copyright infringement. In this situation, including an anti circumvention provision in the Copyright Act will only be an exercise in futility. So, for now no such provision is needed in the Indian statute on Copyright.