Intellectual Property Rights of Electronic Information in the Age of Digital Convergence

A. Lakshmana Moorthy, M. Prahalada Rao* and C.R. Karisiddappa**

Technical Information Centre, Defence Research & Development Laboratory, Hyderabad-500 058

**Technical Information Centre, Defence Electronics Research Laboratory, Hyderabad-500 058*

***Dept of Library & Information Science, Karnatak University, Dharwad - 580 003*

ABSTRACT

The laws of intellectual property aim to protect owners of the literary, dramatic, musical, and artistic works; designs, innovations and inventions from unauthorized use or exploitation by some one else. Though every country has enacted laws to protect intellectual property of its citizens, many infringements take place and a majority of them end up in courts of law. The developments in information and communication technologies made the situation grimmer. This paper briefly explains the copyright and protection of electronic information, its security in network environment, and copyright provisions for databases, multimedia works, and computer software. The relevant provisions of the European Union, the American and the Indian legislative developments as well as the international efforts were touched. The various facets of the information Technology Act and the recently tabled Communications Convergence Bill have been discussed. Despite all the legislative efforts, a level playing field is needed for the rights owners, publishers, library professionals and users.

1. INTRODUCTION

1.1 Intellectual Property Rights

Inventions and innovations are creations or results of human mind (intellect) and are generally treated as intellectual property. The efforts preceding the invention/innovation/creation necessitate investments in material, human power, financial and other resources. Therefore the inventor/innovator/creator and/or the parent institution naturally tries to take advantage and guard such developments as an asset like any other material assets. So, such institutions/organizations feel it is their right to protect their intellectual properties legally so that they get returns on their investments and are encouraged to invest more resources in such ventures.

Developed countries realized that technology is a crucial element in foreign investment and also a key to the rapid expansion of trade and services. As a result these countries have made legal provisions to protect intellectual property rights (IPRs). Several countries moved for inclusion of IPRs in the General Agreement on Tariff and Trade (GATT). Although developing countries offered stiff resistance, the IPRs were included in the World Trade Organization (WTO) Agreement under Trade Related Intellectual Property Rights (TRIPS). Naturally, the IPRs are perceived as an imposition of technologically strong countries and there exists a considerable disagreement between the developed and developing countries (haves and have-nots) on many issues of IPRs. The World Intellectual Property Organization (WIPO), the TRIPS, the GATT, and the various other organizations are creating an environment conducive for the export of intellectual property from the technology-rich countries to the developing and technology-poor nations. The reality is, even the devel-

In NACLIN 2001: Networking of digital resources for national development: Papers of the Fourth National Annual Convention on Library and Information Networking, 6-9 November 2001, University of Hyderabad, edited by HK Kaul. New Delhi, DELNET, 2001. pp.82-106.

oped countries, when they were in the category of developing countries, have not respected the copyright interests of authors other than their own. This is true even in the case of the United States, from where Charles Dickens could not get anything out of the publication of his works, when the country was a net importer of intellectual property.

In general IPRs cover patents, registered designs, copyright and trademarks. It also covers layout designs of integrated circuits, geographical indicators and anti-competitive policies in contractual licenses. Among these copyright is relevant for library and information work. So, the scope of this paper is limited to the protection of copyright, particularly in the post-Internet era, a major issue that is relevant to all those connected with library field including library professionals, users, authors, publishers, etc. The IPR issues of digital information include copyright, ownership, pricing and rules and regulations governing multiple uses.

1.2 Copyright

Copyright is an intangible right and can be of sustainable value. Copyright shall subsist for a definite period of time in *original* literary, dramatic, musical and artistic works (including computer generated works like databases, software, multimedia), cinematograph films, and records. It is an exclusive legal right to reproduce the work in any material and vests in the author of the work. The right can be licensed or assigned to anyone of the choice of the rightful owner/author. Copyright provides rights of ownership and legal protection against unlawful reproduction of the works. Copyright Law besides recognizing their right to the benefits accrued by the usage of their creative work by others, also assures and encourages authors to pursue artistic, scientific or literary works. Copyright subsists through the total of the lifetime of the author and a term of 60 years (varies from country to country) after the death of the author. This subsistence is through out India and in countries which are the members of the Berne Convention or the Universal Copyright Convention which by virtue of their membership to these conventions extended the rights enjoyed by their citizens to the citizens of India. Similarly India has extended copyrights to the works published (and unpublished) in any of the member countries of the conventions. It is an economic system for ensuring the creation of new knowledge by rewarding their creators and their agents.

The exclusive rights of the authors of the works who can do or authorise someone to do all or a part of those activities are enumerated in Section 14 Indian Copyright Act. These, when done by unauthorised persons or without the explicit permission of the copyright holders, amount to breach or infringement of copyright (Govt. of India, 1996). However, copying of or publishing works that were once in the *public domain* and now had their copyright revived, will not be deemed as infringement of copyright.

Copyright Liability

Section 52 of the Act enumerates five categories of acts which when performed do not fall under the infringement of the copyright. Fair use (i.e., photocopying in the course of fair dealing for research, teaching, criticism, review, private use, reporting, broadcast, etc) is the category under which a number of infringements take place. The fair use principle codified by various laws is a defense against copyright liability. In deciding whether fair use is applicable in any infringement,

courts consider: (a) the purpose and character of the use including whether the use is of commercial in nature or for not-for-profit educational or training purposes, (b) the nature of the copyrighted work, (c) the amount and substantiality of the portion copied in relation to copyrighted work as a whole, and (d) the effect of use upon the potential market for or value of the copyrighted work as a whole.

2. COPYRIGHT OF ELECTRONIC INFORMATION

The developments in the field of information technology, particularly in the areas of computers, communications and mass storage, have made it possible to handle enormous volumes of electronic/digital information and data with ease. The libraries took advantage of these technologies for effectively meeting the ever-growing users' requirements and started enhancing their collections with and relying more and more on electronic information resources. Publishers of scholarly, academic and reference works from almost all fields of human knowledge started bringing them in electronic form. Many publications exist in dual (both on paper and electronic) versions and some are brought out in electronic version only. The libraries in science, technology as well as in academic fields are increasingly depending upon on electronic resources.

During the past few years, there was a quantum jump in the electronic/digital information resources made available through networks, particularly over the Internet and the Web. The electronic information can be distributed across the globe through electronic mail, electronic bulletin boards and networks. The proliferation of personal computers and the decreasing costs of primary and secondary mass storage media all made it possible to download, store, display and print electronic information. Further, the downloaded documents can be forwarded to others without the knowledge of its rightful owner.

Digital library environment makes the copyright protection a difficult task. It is easy to create digital or digitized copies of material including text, photographs, music and video. In comparison to printed information, electronic information is not so permanent; it is highly vulnerable to manipulations, deletions, revisions and modifications without leaving any resemblance to the original; its ownership is non-ascertainable and at times, can be questionable. Unlike the case of printed journals, close monitoring and restriction of usage of digital documents is difficult. Denning (1995) reported a few cases of plagiarism of electronic material. Lynch (1994) suggested solutions like dedicated server, document digest algorithms, and cryptographic signatures to overcome some of these problems. Although efforts have been made to prevent fraudulent acts in digital library environment, infringements are becoming quite common due to difficulties in their detection. The issues and concerns of electronic information like credibility, accessibility and acceptability by the users, readability, accountability, authenticity of the electronic information, preservation and archival maintenance have been dealt elsewhere (Lakshmana Moorthy & Karisiddappa, 1996, 1997, 1998, 2000).

Copyright applies to Internet; e-mail messages, material loaded on ftp sites, or www servers or anything else put up on Internet, are copyright protected so long as they fulfill the originality criterion. Access to e-mail by anyone other than those for whom it is meant, is infringement. However, Internet URLs, e-mail addresses, are facts so there is no copyright and can be copied. However, compilations of addresses, high-end indexes like Yahoo! and FAQ collections are protected by copyright (Oppenheim, 2000). There have been many cases of copyright infringements including

distribution of copyright material, using Internet (for example, Napster and Online Guitar Archive). One issue related to the Internet era is the applicability of copyright when more than two countries are involved. In the case of print media, if an Indian work is published in the US and is copied in the UK, then the copyright law of UK will be applicable to the violation. However, if an Indian gives instructions to the computer server in US to download software from a UK website the same is not applicable. Even in our country many cases of cyber fraud were reported. Those who are interested in knowing how to deal with cases relating to cyber law, same trademark and domain name disputes, getting copyright protection for Websites, cyber stalking, liabilities over cyberspace, cyber squatting, anonymous cyber defamation through e-mails, copyright in cyberspace, cyber hacking as well as various legal provisions of IT Act 2000, Convergence Bill, etc. may see the regular column of Duggal (2001) in the Sunday edition of the *Economic Times*.

Internet is creating new and newer avenues for rights and consumer privacy violations. Cyber frauds include cyber stalking, cyber hacking, cyber defamation, cyber harassment, cyber terrorism, cyber war, and so on. The world over, many cyber frauds are taken to courts (see, for example, Duggal, 2001; Oppenhiem and Turner, 1999; and Turnbull, 2001). This trend will increase in future. The growth of Internet is remarkable. While in developing countries the number of hosts and users is increasing at high rates, developed countries are also registering increase in these areas. The number of e-mails sent and the millions of web pages is mind-boggling. This situation led many to suggest that copyright is no longer relevant in the Internet environment. In practice it is rather difficult to impose copyright law on Internet users. Oppenhiem (1999 and 2000) discussed in detail the copyright issue over Internet. In most of the copyright violations on Internet, the owner may be unaware of it or the infringer may be difficult to identify. Further, most of the copying over Internet does not quality under exceptions (i.e., 'fair dealing' in UK, 'fair use' in US and India, 'private copying' in European countries). Some of the copyright laws do not clearly distinguish electronic information from print media (for example UK and India) and so the fair dealing laws are not applicable to the digital environment. As the nature of the print and electronic media differ so must be the laws governing them.

Copyright forbids storing of a work in electronic medium (even for private use) and electronic transmission of copyrighted material by anyone other than the copyright owner. In case a user of an online service violates copyright provisions, the service provider is held responsible unless he complies with safety measures to protect rights. Under this provision, Napster, a popular Internet music-swapping service that enables Internet users to share music files stored in their computer hard disks, was asked to comply with the law. Although the service was seen initially as a recreational one, the after effects were felt by the music industry once it became popular (25 million users in just over one year of its existence) and helping swap copyrighted material across the continents. Its impact on the Internet has been profound. Ultimately, Napster agreed to comply with the Court's injunction to prevent users swapping copyrighted material using its utility. Search engines cannot display digital pictures; they can only provide details. Digitised documents, especially the multimedia products, are prone to rights violations.

2.1 Copyright Legislations in Developed Countries

WIPO has taken steps to cope up with the creation, adoption, transmission and distribution

of digital media. Three draft treaties of WIPO were discussed by the member countries and would come into force after ratification by them. Article 10 of the WIPO Copyright Treaty (1996) states that parties may carry forward and extend into the digital environment limitations and exceptions in their national laws, and may device new exceptions and limitations that are appropriate in the digital network environment. Article 11 prohibited acts of circumvention of copyrights. Countries such as the US, Japan, Canada, Australia, and European Union have already enacted tough regulations to protect the digital media from infringements and to overcome the challenges posed by the digital technologies. In a welcome move, the Reproduction Rights Organizations of UK, namely, the Copyright Licensing Agency and the Newspaper Licensing Agency have started issuing licenses to digital copyright, copying electronic information (Oppenheim, 2000).

The US Congress passed the Digital Millennium Copyright Act (DMCA) in October 1998 (effective from October 2000) included major changes to encourage advanced technologies to protect content of digital media at the same time ensuring fair use by consumers. Prohibition of circumvention of technological means employed for effectively control access of copyrighted works, devices or equipment that help in circumventing. However circumvention prohibition is exempted for libraries browsing works to determine to purchase them, law enforcing agencies, reverse engineering for achieving interoperability with other products, encryption research, privacy protection and security testing. DCMA also prohibits knowingly providing or distributing or removing or altering of false copyright management information, etc.

The European Union Directive on the aspects of Copyright and Related Rights in the Information Society was approved in May 2001. The Directive prohibits making copyrighted works available over Internet unless authorized by the copyright holder. It also specifies that member states shall protect against circumvention of and using devices to circumvent technology measures that ensure rights, except in the case of librarian, educational establishments, teaching and scientific research organizations, disabled individuals and public security. There are ambiguities and inconsistencies in the right of reproduction, on communication to the public and on exceptions to copyright. The primary purpose of the EU Directive on copyright is to harmonise the law through out the Member States.

The DMCA and the EU Directive encouraged many efforts by private R&D institutions. Some of them engaged in intellectual property rights protection include Copy Protection Technology Working Group (consumer electronics, IT products and DVDs); DVD Copy Control Association (licensor of the Contents Scramble System technology to protect copyrighted contents of DVDs), 5C (for Intel, Hitachi, Matsuhita, Sony and Toshiba companies which developed Digital Transmission Copy Protection System for Video content), the Secure Digital Music Initiative (for music), etc (Turnbull, 2001).

2.2 Security of Information in Networked Environment

There is a steady growth in the regional and the local area networks and intranets; millions of people are hooked these networks. Already users of electronic information are experiencing problems related to IPRs and as the computer networks expand, such problems would increase further. This is only because most of the content distributed over the networks is copyrighted or is under

some sort contractual licensing. Although some recognise copyrighted material, they tend to think that non-commercial distribution is fair use and that it does not amount to rights violation. This leaves the network managers/administrators in a tight spot over the liability of such infringements. Content liability (as to who will own responsibility) for the access of the seditious, and violent material accessed by users is an important issue, especially in the face of rising terrorism.

Three factors are to be taken care to provide security of information in a network environment: (a) authentication, that is, knowledge of the identity of sender to the receiver and vice versa, (b) confidentiality, that is, the message sent has not been intercepted by a third person, (c) and integrity that the message is not tampered during transmission. Security Profile Inspector for checking network security configuration, and Network Intrusion Detector, for identifying weak links in a network of clients and servers, monitoring LAN segments and producing transcripts of suspicious user connections are two systems in use for effective protection of information over computer networks (Feingold, *et al,* 1996).

Many technologies have been developed for protecting the copyright of electronic information. Several electronic copyright management systems have been designed and developed for protection of rights by government agencies, academic institutions and publishers to deliver electronic information to users in a network environment. These include Performing Arts Teaching Resources Online (Patron) at the University of Surrey, Electronic Reserve Copyright Management System (Ercoms) of De Montford University, and the Electronic Library and Information Retrieval Online Project (ELINOR) of Milton Keynes, Project Cited (Copyright in Transmitted Electronic Documents) of the European Commission, RightPages TM Service of Bell Laboratories, TULIP (The University Licensing Programme) of Elsevier Science, Security and Rights Management System of the ISI, and also of OCLC and Copyright Clearance Centre (Lakshmana Moorthy and Karisiddappa, 1997).

2.3 Databases

Database can be defined as a collection of works, data, or material arranged in a systematic and methodical way and capable of being accessed by electronic or other means. It includes materials necessary for the operation and consultation of a database such as an index. A database may contain information relating to names and addresses of clients or subscribers such as telephone directories, yellow pages, address lists, etc; a list of bibliographic references; full text of documents or periodicals such as patents or full-text databases; documents with mixed text and graphics such as multimedia directories, works); or a compilation of drawings such as engineering and architectural drawings. The creator/developer of the database is generally treated as its author.

Bibliographic databases contain abstracts of already published articles or documents that are mostly copyrighted material. If these abstracts are short and condensed, report the facts in and do not substitute the original articles, there can be no infringement of rights. If, on the other hand, the abstracts act as substitutes to original text by reproducing them, then they are likely to be treated as copyright violation. In other words, abstracts should be surrogates leading the readers to the original articles to avoid copyright infringement.

The data or material included in a database is not copyrightable. The originality and intellectual work in databases include the content selection, internal coordination between the structural elements, the arrangement of all elements of a database, and the contents itself. By running a computer programme on one or more databases, a new database can be created. The computer-generated database thus created can be treated as original only if there exists sufficient skill and judgment in the new database. Although the contents of the constituent items are not original, because a reasonable amount of judgment in the selection of items has been used in creating it, the newly created database can be considered as compilation or directory for the purposes of copyright.

Berne Convention, WIPO Copyright Treaty, TRIPS Agreement of WTO and the GATT Agreement provide protection of computer software and databases. The Indian and UK laws extend the copyright protection to computer databases, treating them as literary works. The EU Directive on Legal Protection of Databases extends protection to the structure of the database and covers non-electronic (printed) databases also. It also enables a database owner to forbid or control the extraction or re-use of material taken from a database. Under the US Copyright Law, compilations of pre-existing material or data are non-copyrightable; copyright for databases is provided under collective and derivative works. In many countries, copyright rules are applicable to computer databases and are treated as compilations. Besides international agreements and copyright laws, the databases are also protected under contracts and licensing agreements between the owner of the database and the subscriber as well as protection through technological means such as hardware and software locks or dongles, electronic copyright management systems, digital signatures and watermarks and so on (Gupta, 1999).

Many database producers and vendors allow users download a portion of the database on to a 'temporary file' for research purposes under fair use principle. However, there are no clear-cut guidelines as to how much data can be downloaded at a time. In the case of printed documents, depending upon the size of the original, up to 5-10 per cent of the original document or a chapter can be photocopied under fair use. The same fair use principle cannot be applied in the case of databases, as even 5 per cent material would be voluminous when cumulative and large databases are used. And, when such downloading is made regularly over a period, say 2-3 years, then the resulting database would be considerably large. Such issues would become more frequent since users would like to keep the useful downloaded data in their personal library, much the same way they retain and maintain photocopies of articles in areas of their interest for re-use. Most of the CD-ROM databases are used in providing SDI services to the institution's research community. Sometimes, downloaded data against an SDI profile is sent by e-mail to save time. This is illegal as transmission of electronic information over communication networks is an infringement of copyright and is prohibited by all database owners.

2.4 Multimedia Works

Digital multimedia works, music, photographs etc. have proliferated in the last decade creating immense opportunities for the content creators, publishers, distributors and consumers. The advantages of digital media are many: Storage and manipulation, instant and inexpensive distribution, and flexibility to customize the media as per the demands/requirements of the users.

The legal status of multimedia works is not clear. Multimedia works are covered and classified under audiovisual works by the USA, UK and Indian laws. The US law also covers derivative works, which include digitized works. Multimedia works are also prone to infringement of copyright, as the increasing availability of high bandwidth networks makes it too easy to illegally duplicate and disseminate these documents without any loss of quality. When multimedia works are commissioned under contract, they are treated as works made for hire and the copyright owner will be the person or institution that commissioned the work. However, mere payment for the work does not amount to ownership unless it is clearly distinguished in writing as work made under contract. This also applies to software developed by sub-contractors as a part of a multimedia work (Wilf, 1994).

Extensive research has been carried out for security of multimedia content over the networks (see for example, Cox, *et.al.* 1997; SPIE, 1999 & 2000; and Wong and Delp, 2000). Copyright protection of multimedia works on a network is achieved using signal processing, data compression, encryption and system level security protection. Alternatively, an invisible watermark or a digital signature or visible watermarks can also be used as deterrents to multimedia piracy (Garofalakis,*et al*, 1997). Usage of watermarks can identify the legal owner of the multimedia work. Another way of protection of digital data against infringements is the Multimedia Protection Protocol (Rump, 1997).

2.5 Computer Software

A computer programme (software) is defined as a set of instructions expressed in words, codes, and schemes or in any other form including a machine-readable medium, capable of causing a computer to perform a particular task or achieve a particular result. Downloading computer software, free ware and share ware, is a common feature of cyber environment. Software can be copied any number of times. Unlike photocopies, the second and subsequent generation copies of software can be used without any loss of 'quality'. One cannot distinguish between the pirated software that is illegally sold or freely distributed and could be used as original ones.

A number of nations had interpreted their copyright laws to include computer programmes for protection. The European Union took a leading role to protect computer programmes, and derivative and digital works. Prior to the adoption in 1991 of the European Directive on the protection of computer programmes, there was a general acceptance in Europe of copyright as a form legal protection of computer software. The Council Directive (91/250/EEC) of 1991 aimed at harmonising the legal protection throughout the European Community. The EU 1992 Copyright Directive on Rental and Lending Rights (92/100/EEC) extends exclusive right to all copyrighted work; public library lending of computer software and CD-ROMs is an offence unless there is a permission or license for doing so. France protects computer software and categorises it under industrial art. German law requires demonstration of the software to satisfy the originality standard of copyright law. Japan is the first nation to consider adoption of a *sui generis* approach to the protection of computer programmes. The Indian law extends protection to computer software and computer-generated works and treats storing of a work in any medium by electronic means as infringement. While some countries amended existing laws to extend copyright protection, a few countries provide patent protection computer software.

A number of methods have been in use for making computer software difficult to copy. These

include hardware and software locks or dongles. A computer program is run only if the lock (or dongle) is in place. However, no sooner a protection mechanism appears in the market, than the devices designed to overcome these appear. Even the dongles have been defeated. But the law recognizes such acts as cognizable offences and deliberate acts of designing devices to circumvent the copyright protection mechanisms. The Copyright, Designs and Patents Act 1988 of UK (section 296) provides protection from making, incorporation, sale or hire etc of devices or means specifically designed or adapted to circumvent copy protection of works in electronic form by treating such acts as infringement of copyright. The US Law forbids supply of equipment, software, or services capable of circumventing protection of IPRs. Due to limitations in protection and also as it protects expressions and not ideas, algorithms will not be effectively protected by copyright law. So, some corporates involved in software development are moving towards patenting computer software rather than applying copyright.

2.6 Copyleft

One of the developments of cyberspace is the culture of making software/advice/ support/ troubleshooting as a right free of charge. The plethora of FAQ websites in various subject fields are examples of such culture. Netizens are willing to share what they have and expect the same from fellow Netizens. Coupled with stringent copyright laws, some felt to free the software from the clutches of IPRs. One such movement is the Free Software Foundation (FSF) established by Richard Stallman, an employee of MIT Artificial Intelligence Lab. The FSF and other like mended initiatives over the Net became proponents of 'Open Source' and advocate development of free software (as against licensed software). The free software entails the developer distribute it with source code, allow to share it with anybody, with freedom to modify/rewrite and redistribute to others freely or for a price. The GNU/Linux is free Operating System software of FSF that was made available on these lines. Many a software packages are available for word processing (for example; Abiword, Text shield, etc).

To avoid any unscrupulous people modify the free software and distribute/sell without source code, FSF brought the concept of Copyleft. As per the description of the FSF website (www.gnu.org), to copyleft a program, first FSF copyrights it and then distribution terms are added which are legal instruments that give everyone the rights to use, modify and redistribute the program's code or any program derived from *it with a condition that distribution terms are unchanged*. Thus the code and freedom become legally inseparable. While proprietary software developers use copyright to take away the user's freedom, the FSF uses copyright to guarantee the freedom of users. That is why FSF reversed the name by changing copyright to copyleft. There are other similar initiatives including Open Source Initiative (www.opensource.org) and FreeBsd (www.freebsd.com). The importance of the free software is that it is highly relevant for poor countries.

3. TEHNOLOGIES FOR PROTECTION OF COPYRIGHT

3.1 Cryptography

Cryptography is one of the oldest ways to ensure security and privacy of information. Cryptography has been in use for protection of intellectual property rights. It is a common practice to

scramble the cable and satellite television signals to prevent unauthorized viewing. However cryptography protects the work during transmission or distribution only. After the work is decrypted, it does not provided any protection. Encryption makes the file unreadable or un-understandable by anyone others than the legitimate user who only can decrypt. This protects confidential information from eavesdropping, and illegal copying of software etc. Cryptography can be used as an envelop for information sent via e-mail and file transfer. Another method is employment of encryption protocols wherein the document server encodes, encrypts, compresses and sends to a registered user, where the software supplied by the network service provider decrypts and displays on the user's terminal. The document server authenticates the user requests before sending a document (Choudhary, *et. al*, 1995).

3.2 Digital Watermark Technology

Digital watermarking technology complements cryptography in that it embeds imperceptible signals in a document or message and the content can vary accordingly. Digital watermarks are signals, logos or patterns inserted into digital documents. A unique identifier can be used to identify the work or the message might contain information regarding ownership, sender, recipient, etc. or information about copyright permission and a system consists of watermark generator and embedder, and a watermark detector decoder. This technique enables protection of ownership rights of digital information. Unlike encryption which warrants file transformation and not understandable unless encrypted, digital watermarking leaves the original document intact and viewable. These watermarks persist during viewing, printing or re-transmitting, thereby establishing ownership. When an illegal copy bears watermark, the source of the piracy can be established. The legal user can remove these watermarks with a predetermined algorithm. This technology is different from digital finger printing technology. A detailed discussion of watermark embedding can be seen elsewhere (Barni, 2001; Decker, 2001; Martin and Kutter, 2001).

Apart from authentication, detection of unauthorised source of legal copies, the visible and invisible or hidden watermarks help in discouraging illegal copying. Two types of invisible watermarks, viz. those that are destroyed when subjected to manipulations and those that cannot be destroyed are in use. Two techniques of invisible watermarking of multimedia images, which can detect all but the minutest changes in the image, are discussed by Wolfgang and Delf (1996). The visible watermark uses a barcode on the first page of each article. The watermarking technology is extensively used in protecting multimedia works. Digital watermarking technology ensures only lawful image and audio files are used, thus protecting against copyright infringement and so is helpful for the Webmasters. Argent, Cognicity, Copysight, EIKONAmark, Giovanni, JK_PGS, Musicode, Digimarc, PixelTag, StirMark, SureSign, SysCoP, unZign, etc are some of the watermarking tools available in the market place for the purpose (Roy, 1999). A detailed account of watermarking technology including counterfeiting schemes is discussed elsewhere (Berghel, 1997).

3.3 Digital Signature Technology

Digital signature includes the identity of sender (and receiver), date, time, any unique code etc. and can be added to digital products. This digitally marks and binds a software product for transferring to a specified customer. The Security and Rights Management System of ISI Electronic

Library Project employs digitally signed fingerprint to guarantee document authenticity (Anderson & Lotspiech, 1995).

3.4 Electronic Marking

The electronic marking and identification technique can be employed to distribute electronic information over networks at the same time discouraging illegal copying. In this technique, a unique and indiscernible mark is automatically generated by the system and put on each of the document copies. The system also registers the recipient of an illegally copied document. It is difficult for an illegal user to find the unique marking pattern in the user‘s document. This technique can be used to protect copyright, IPRs and in electronic publishing where a documents are printed, copied or faxed (Low, et al, 1995).

4. INDIAN SCENARIO

In the light of recent developments like granting patents for neem and turmeric products as well as a clone of Basmati rice (Taxmati), there is an urgent need to contest such issues (which the Department of Scientific and Industrial research is doing) and safeguard the interests of our society. Protection of intellectual property rights was one of the foremost and important areas towards discharging the commitments under the TRIPS agreement. In this context the government introduced some Bills in 1999 that included Information Technology Bill (got President’s assent in May 2000), Patents (Amendment) Bill, Trademarks Bill and Designs Bill, and Geographical Indication of Goods (Registration and Protection) Bill. Further, there were many old and archaic laws that need to be repealed or amended in tune with the changing scenario.

Although, the Indian law extends protection to computer software and computer-generated artistic or literary works and compilations including computer databases, it has no provisions for electronic and online books, journals and electronic information. Further, the law needs exhaustive changes in the light of fast changing technological developments, especially in the information technology, communications and related fields. There was a necessity for a law to take care of the role of networks, electronic information, Internet and their impact on the society. Although, an organisation/ institution purchases a legal copy of software, the law prohibits its duplication or making multiple copies for use by different constituent divisions or units in the same organisation/institution. The law provided for severe penalties for copyright violations. If an infringement is established in a civil or criminal court of law, the defaulter is liable for punishment with imprisonment up to three years or a fine of an amount up to Rs 2 lakh or both. The law also makes provisions for claiming actual and statutory damages by the copyright holders. However, still a number of problems persist in enforcing the law (Kumar, 1997).

4.1 Information Technology Act, 2000

With the enactment of Information Technology Act, 2000, India became the twelfth country to have a comprehensive cyber law. Besides facilitating electronic communications and e-commerce, the Law aims to curb computer crimes. The Act proposes amendments to the Indian Evidence Act and the RBI Act 1934. The main objective of the Act is to provide legal recognition for

transactions carried out by means of electronic data interchange and other means of electronic communication, commonly known as E-commerce, which involve the use of alternatives to paper-based methods of communication and storage of electronic information to facilitate electronic filing of documents with government agencies (Govt of India, 2000). The Act enables:

- Electronic communication (e-mail) will now be a valid and legal form of communication which can be produced as evidence in a court of law.
- Companies can now carry out e-commerce with renewed vigor using the legal framework of the Act. Business transactions can be carried out using digital signatures, which are legally valid.
- Electronic contract has been made legal and binding (contracts can be accepted by electronic means of communication, unless otherwise agreed).
- Private corporations with necessary infrastructure can effectively participate as Certifying Authority for issuing Digital Signature Certificates (DSCs).
- Electronic forms can be filed with government or its agencies.
- The Act enables companies legally to retain the valuable corporate information in electronic form.
- The Act also addresses the security issues.
- Promoting the legal and business infrastructure development necessary to implement e-commerce,
- Some cyber crimes have been defined and declared as penal offences punishable with imprisonment and fine.

(a) Salient Features of IT Act

- *Electronic Records:* Section 3 provides for authentication of electronic records with digital signature and verification of these records with public key of the subscriber.
- *Digital Signature:* Sections 4-6 provide legal recognition of electronic records, digital signatures and use of these in government and its agencies. Any subscriber can authenticate electronic record by affixing digital signature.
- *Electronic Gazette:* Section 8 provides for publication of rules, regulations, etc. in electronic form (Electronic Gazette).
- *Electronic Governance:* The Act allows submission of information, forms, etc to the government or its agencies in electronic form instead of written or printed forms. Digital signatures can be affixed to the documents.
- *Secure Electronic Records and Digital Signature:* Sections 14-16 provide for secure electronic records, secure digital signature and security procedure.
- *Certifying Authorities:* Section 17-34 deal with Regulation of Certifying Authorities including license to issue DSCs, and appointment of Certifying Authorities.
- *Digital Signature Certificates:* Sections 35-39 provide for DSCs. The Act provides for public and private key for operating DSCs. Section 42 emphasises the subscriber should exercise reasonable care to retain control of the private key corresponding to the public key listed in his DSC, take care not to disclose and report any compromises (violations) to the Certifying Authority.
- *Penalties and Adjudication:* The Act makes any person liable to pay damages not exceeding Rs. 1 crore to the affected person(s) for illegally accessing, downloading, copying or extracting data from computer databases; designing computer instructions or computer viruses to modify or

destroy, record or transmit data; disrupting or damaging computer/network/database; denying access to computer/network to authorized persons, providing assistance to others for accessing computer/network in contravention of the provisions of the Act and charging for services by manipulating/tampering (Section 43). In addition penalty is also imposed for failure to furnish information, return report to the Controller or the Certifying Authority (Section 44). Further a residual penalty not exceeding Rs. 25,000 is imposed on those who contravene any rules and regulations made under the IT Act for which no separate penalty is provided for, including to any person who is affected by such contravention (Section 45).

- *Cyber Appellate Tribunal:* Sections 48-64 provide for Establishment of Cyber Appellate Tribunal, the presiding officer of which will be from Indian Legal Service or a Judge of High Court with a term of five years.
- *Offences:* Tampering with computer source documents, and hacking a computer system will be liable for imprisonment up to three years or with fine up to Rs. 2 lakh or both. Publishing obscene information in electronic form attracts imprisonment up to 10 years and also fine up to Rs. 2 lakh. Section 71 provides for penalty of imprisonment up to two years or fine up to Rs. one lakh or both for misrepresentation or suppression of facts to the Controller or Certifying Authority. For unauthorized access to electronic information, breach of confidentiality and privacy (Section 72), publishing false DSCs (Section 73), publishing DSCs for fraudulent purposes (Section 74) invites a penalty of imprisonment up to two years or fine up to Rs. one lakh or both. The computer and related equipment used in contravention to the IT Act, 2000 will be liable for confiscation (Section 76).
- *Others:* Section 79 exempts Network Service Providers (NSP) from liability for any third party information or data made available over the network if the NSP proves that the offence or contravention was committed without his knowledge or that he has exercised due diligence to prevent such offence or contravention. Section 88 provides for the constitution of Cyber Regulation Advisory Committee to advise the government, and Controller of Certifying Authorities.

(b) Gray Areas

It is not clear as to how and in what particular manner the Act shall apply to any offence or contravention committed outside India by any person (Section 75). It is also not clear how Adjudicating Officers will exercise their authority outside India. The law does not touch upon issues with respect to Domain Names and this is beyond logic that these are linked to e-commerce and Internet. The Act does not deal with IPRs like copyrights, Trademarks or Patents. While advocating use of electronic records and digital signatures in government and its agencies, Section 9 does not confer any right upon any person to insist that the document showed be accepted in electronic form. Crimes like cyber theft, cyber stalking, cyber harassment, and cyber defamation are not covered in the Act. Draconian powers are vested (Section 80) on police officers of the rank of DSP for investigation and prevention of cyber crime (Duggal, 2001).

Although the much-awaited Cyber Law was passed in parliament in May 2001, Government took 5 months to implement it. Very little has been done during the past one year, except registering a few cyber crimes. A cyber crime police station was launched in Bangalore recently. A Controller and Deputy Controller of Certifying authorities have been appointed. The Cyber Regulations Advisory Committee has been constituted which held a couple of meetings. Beyond this little has pro-

gressed. Important aspects to be given attention include the manner/ standard governing authentication of electronic records, prescribed forms/for electronic filing in government and related departments, the nature and format of filing, issue of electronic records and mode of payment. Digital signature regime and the selection/appointment of Certifying Authorities are yet to take off as per a recent report (*The Hindu*, 14 September 2001, p. 5), the Certifying Authority for security-related issues and digital signatures will be established in the next two months). Despite these hiccups, it is a positive forward step towards regulating IPRs in cyberspace.

4.2 Communications Convergence Bill, 2001

In the current scenario of convergence of technologies, like telecommunications, multimedia, and broadcasting, the Communications Convergence Bill was tabled in the Parliament in August 2001. The major objectives of the Bill are to facilitate and enable access to a national communications infrastructure for providing wide range of services to consumers; set up a common regulatory framework to tackle telecom, IT and broadcasting sectors; and spelling out the powers and role of a single licensing and regulatory authority for the three sectors. An autonomous body Communications Commission of India is proposed with headquarters at New Delhi and branches at Chennai, Mumbai and Kolkata. It is proposed to create five categories for licenses, viz. providing or owning infrastructure facilities; providing services in networking, network applications, content application, and value added network application. The IT-enabled services like call centers, e-commerce, tele banking, tele-education; tele-trading, videotext and video conferencing will be exempted from licensing and registration.

The Bill proposes to repeal the age old Indian Telegraphic Act 1885; Cable TV Networks Act 1995; Indian Wireless Telegraphy Act 1933, The Telegraph Wires (unlawful possession) Act, 1950; and the Telecom Regulatory Authority of India Act, 1997. The Bill provides for various offences with penalties and imprisonment. While the Bill covers cyber stalking, it does not cover cyber crimes like cyber defamation, cyber harassment, cyber terrorism, etc.

Even the proposed Convergence law is riddled with a number of controversial and contentious elements. The law to regulate convergence does define the word “convergence”, resulting in the lack of a legal definition of the subject matter. In the era of liberalization and globalization the law provides for immense control to the government through the proposed super regulator Communications Commission of India and some of the provisions may rob autonomy from the Commission. As it has to follow the policy directives of the government, the Commission may not have independent existence. Certain aspects like censoring data, etc have been left to subjectivity and discretion under ‘fairness and impartiality’ which will de difficult to achieve (Duggal, 2001).

5. CONCLUSION

The technological advancements are outpacing the legislative measures for the protection of intellectual rights. The present copyright laws are failing in effectively preventing piracy or infringement. These laws are to be heavily modified to suit to the digital and networked environment. A digital document can potentially replace all printed copies in a networked environment and still can be accessed by multiple users simultaneously. Remote access and downloading can virtually make

one single document enough for all the libraries and users of the network. This can lead to many issues. In near future, electronic file transfer would be replacing inter-library loan and photocopying. Browsing through the digital document without accessing is impossible. And accessing is always fee based. Potential users of a digital document must be in a position to determine, in advance, the usefulness of the document and the price tag if they are expected to pay a fee. This is one issue that concerns the librarians and readers in the same manner. The various deterrent/regulatory steps like cryptographic techniques; authentication of users and limits to their access; security across multiple platforms and protection at network, system, application and user workstation levels; password regulations, etc will no doubt protect the IPRs but also deter many a potential user. The copyright laws should enhance the use of material, encourage readers but not hamper through the various regimes. It is very difficult to draw a boundary line, on many occasions, between what is permissible and to what extent, and what is infringement of rights.

Though laws are stringent, there is little consensus on the extent of copyright protection in the digital world. Many groups (for example, Association of American Universities) are demanding Copyright exemption of digital versions of scholarly journals; maps, newsletter archives and some databases. Their argument is that these materials are valuable mostly for their facts and so are not copyrightable. Librarians from Library of Congress, National Archives and Records Administration and the National Library of Congress also are supporting a looser interpretation of copyright in digital domain (Sherman, 2000). Similar initiatives should come from the professional community in developing countries including India, as it is clear that the public good is being served by such efforts.

A number of distinguished commentators have suggested that copyright has no future in the networked environment (see Oppenhiem, 2000 and references 1, 27-30 referred there). It will become harder in future to enforce nights. However, copyright cannot be ignored as it provides the legal foundation upon which many licenses are based. Three types of rights have been suggested by copyright supporters: (a) pseudo-copyright, to protect databases by means of database rights or other non-copyright regimes; (b) para-copyright, to protect electronic copyright management systems and copyright management information; and (c) meta-copyright for extending protection by use of click-on licenses (Jaszi, 1998). In any environment, user's rights are to be promoted along with taking care of the interests of rights owners. New systems are to be developed for document supply in the electronic environment where both the copyright owners as well as users should get benefit. This type of owner-user cooperation, combined with some genuinely innovative thinking by legislators, owners and creators, is needed if copyright is to survive the network age.

ACKNOWLEDGEMENTS

The authors are thankful to Shri Prahalada, Director, DRDL for providing facilities and for permission to present this paper in the Convention. Thanks are also due to Smt K Shailaja Reddy for her secretarial assistance in preparing the paper.

REFERENCES

Anderson, Laura Challman & Lotspiech, Jeffrey B. Rights management and security in the elec-

tronic library. *Bulletin of the American Society for Information Science*, 1995, **22**(1), 21-23.

Barni, Macro. Watermark embedding:Hiding a symbol within a cover image. *IEEE Communications Magazine,* August 2001, **39**(8), 102-108.

Berghel, Hal. Digital village: watermarking cyberspace. *Communications of the ACM,* November 1997, **40**(11), 19-24.

Choudhary, Abhijit K.; Maxemchuk, Nicholas F.; Paul, Sanjay and Schulzrinne, Henning G. Copyright protection for electronic publishing over computer networks. *IEEE Network*, May-June 1995, **9**(3), 12-20.

Cox, I.etal. Secure spread spectrum watermaking for multimedia. *IEEE Transactions on Image Processing*, 1997, **6**(12), 1673-87.

Decker, Steve. Engineering considerations in commercial watermarking. *IEEE Communications Magazine*, August 2001, **39**(8), 128-134.

Denning, Peter J. Plagiarism on the Web (editorial). *Communications of the ACM*, December 1995, **38**(12), 29.

Duggal, Pavan. 2001. See the column Brief Cases published in *Economics Times* on every Sunday on p. 9.

Duggal, Pavan. Cyberlaw: Satyam, shivam and sundaram. *In* The Internet economy of India: Inomy knowledge book 2001a, edited by Osama Manzar, *et.al.*(Eds). Inomy Media, New Delhi, 2001. pp. 84-92.

Feingold, Richard; Bruestle, Harry R.; Bartoletti; Tony; Saroyan, Allyn and Fischer, John. Verifying the secure setup of Unix client/server and detection of network intrusion. *In* Proceedings of the Conference on Information Protection and Network Security, 24-26 October 1995, Philadelphia, edited by Viktor E Hampel and Clifford Barlow Neumann. SPIE proceedings, V 2616. SPIE, Washington, DC. 1996. pp. 55-64.

Garofalakis, John; Kappos, Panagiotis; Sirmakessis, Spiros and Tzimas, Giannis. Digital data processing for intellectual property rights protection over World Wide Web. *In* Proceedings of Thirteenth International Conference on Digital Signal Processing (DSP 97), 2-4 July 1997. IEEE, New York, 1997. V2, pp. 833-836.

Govt of India. The Copyright Act, 1957 as amended by the Copyright (Amendment) Act, 1994. Delhi, Universal Law Publishing, 1996. 83 p.

Govt of India. The Information Technology Act, 2000. Alt Publications, Hyderabad, 2001. 212p.

Gupta, V.K. IPR issues in databases : An update. Paper presented in the ITT'99: Towards Informa-

tion Content for Global Competitiveness, 16-19 November 1999, Hyderabad. NISSAT, New Delhi, 1999.

Jaszi, P. Is this the end of copyright as we know? *In* 40 Nordisk Forum for hensingfors. Nordinfo, 1998. pp. 58-65 (quoted in Oppenhiem, 2000).

Kumar, Arvind. Problems of copyright enforcement in India. *Information Today and Tomorrow*, April-June 1997, **16**(2), 8-16 (reproduced from *Journal of Intellectual Property Rights,* January 1997, **2**(1)).

Lakshmana Moorthy, A. and Karisiddappa, C.R. Copyright in networked environment. *In* CALIBER-2000:Seventh National Convention on Information Services in a Networked Environment, R. Vengan, H.R. Mohan and K.S. Raghavan (Eds). INFLIBNET Centre, Ahmedabad, 2000. pp. 4.18—4.30.

Lakshmana Moorthy, & Karisiddappa, CR. Electronic Publishing : Impact and Implications on Library and Information Centres. *In* Digital libraries: Dynamic storehouse of digitized information. Papers presented at the SIS 96: Fifteenth Annual Convention and Conference, 18-20 January 1996, Bangalore, edited by NM Malwad, TB Rajashekar, IK Ravichandra Rao and NV Satyanarayana. New Delhi, New Age International Publishers, 1996. pp 15-35.

Lakshmana Moorthy, A. and Karisiddappa, C.R. Intellectual property rights and virtual libraries. *In* Towards the new information society of tomorrow : Innovations, challenges and impact. Papers presented at the 49th FID Conference and Congress, New Delhi, 11-17 October 1998. N.M. Malwad, *et al* (Eds). New Delhi, INSDOC, 1998a. pp. IV.51—IV.61. FID Publication No. 719.

Lakshmana Moorthy, A and Karisiddappa, CR. Copyright and electronic information. *In* Access to Electronic Information: Papers presented at Sixteenth Annual Convention and Conference on Access to Electronic Information, 25-29 January 1997, Bhubaneswar, edited by M Mahaptra, DB Ramesh, KN Kittur, P Padhi and JR Sahu. SIS, New Delhi, 1997. pp. 403-416.

Lynch, Clifford A. The integrity of digital information, mechanics and definitional issues. *Journal of the American Society of Information Science,* 1994, **45**(10), 737-744.

Martin, Juan R. Hernandez and Kutter, Martin. Information retrieval in digital watermarking. *IEEE Communications Magazine*, August 2001, **39**(8), 110-116.

Norman, Sandy. Electronic copyright - a time to act. *Library Association Record*, 1995, **97**(4), 209.

Opperhiem, Charles and Turner, Margaret. Copyright and Internet fanzies. *Aslib Proceedings*, 1999, **51**(9), 290-301.

Opperhiem, Charles. Does Copyright have any future on the Internet? *Journal of Documentation*, 2000, **56**(3), 279-298.

Roy, Atanu. Techtrends : The copyright crawlers : Digital watermarking. *Computers Today*, 16-30 April 1999, **15**(177), 90-92.

Rump, Neils. Copyright protection of multimedia data : The Multimedia Protection Protocol (MMP) (http://www.its.fhg.de/departs/ amm/layer3/mmp/).

Ryder, Rodney D. Information Technology Act: Regulating Indian Cyberspace. *Computers Today,* 16-30 June 2001, 46-49.

Sherman, Chris. Napster: Copiright killer or distribution hero? *Online,* 2000, **24**(6),16-28.

SPIE. Eleventh Annual Symposium on Electronic Imaging '99: Security and watermarking of multimedia content. SPIE proceedings, 3657 San Jose 1999. SPIE, Washington, DC. 1999.

Turnbull, Bruce H. Important legal developments regarding protection of copyrighted content against unauthorized copying. *IEEE Communications Magazine,* August 2001, **39**(8), 92-1000.

Wall, Raymond A.; Norman, Sandy; Pedley, Paul and Harris, Frank. Copyright made easier, Ed. 3. Aslib-Imi, London, 2000. 548 p.

Wilf, Frederic M. Legal aspects of multimedia productions. *In* The McGraw-Hill multimedia handbook, edited by Jessica Keyes. McGraw-Hill, New York, 1994. Chapter 17.

Wolfgang, Raymond B and Delp, Edward J. A watermark for digital images. *In* Proceedings of the third IEEE International Conference on Image Processing, 16-19 September 1996, held at Lausanne, V.3. IEEE, New York, 1996. pp. 219-222.

Wong, P.W. and Delp, Edward J.(Eds). Proceedings of Twelfth Annual Symposium on Electronic Imaging 2000: Security and watermarking of Multimedia Content II. SPIE proceedings 3971, San Jose 2000. SPIE, Washington, DC., 2000.