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. NM Malwad, et al (Eds). New Delhi, INSDOC, 1998. pp. IV-51--IV-61. FID Publication No. 719.

FID
Jaipur & New Delhi
11-17 October 1998

Intellectual property rights and virtual libraries

A. LAKSHMANA MOORTHY and C.R. KARISIDDAPPA (India)

Abstract

This paper discusses developments which lead to the establishment of virtual libraries, and the problems posed by digital technologies and electronic information over internet. describes the nature of copyright violations in digital environment including databases and points out the disparities in legislations and deals with the influence of internet is also explains techniques like cryptography, digital watermarks and digital signatures for effective control of infringement of rights in various environment, and security of information over networks and multimedia works. The paper concludes some pertinent questions about the use of digital information.

Introduction

The path-breaking developments in information technology (IT), particularly in the field of computers, communications and mass storage, have made it possible to handle enormous volumes of digital information and data with ease. CD-ROM has become an acceptable medium for storage and dissemination. More and more academic, R&D and other institutions are turning to CD-ROM databases replacing some of the conventional publications and online databases slowly but steadily. The number of electronic databases of secondary periodicals is also growing. Retrospective and bibliographic searches and reference queries are exclusively conducted using them. Digital information would have a higher growth in the coming years. Libraries and information centres (L&Ics) are taking advantage of these technologies for effectively meeting user's requirements. There is a gradual increase in the digital information component in the holdings with a growing dependency on electronic resources, particularly in S&T and academic libraries. During the past few years, there was a quantum jump in digital information resources made available through networks, particularly over Internet and the web. The number of scholarly and peer-evaluated electronic journals (e-journals) offered over Internet is rapidly increasing; some are offered freely with printed subscription and some with a reduced subscription fee. These developments have given birth to virtual libraries.

Gapen (1994) defined virtual library as "the concept of remote access to the contents and services of libraries and other information resources combining an on-site collection of current and heavily used materials in both print and electronic form, with an electronic network which provides access to, and delivery from, external world wide library and commercial information and knowledge sources". It is "a library with little or no physical presence of books, periodicals, reading space, or support staff, but one that disseminates selective information directly to distributed library customers, usually electronically" (Powell, 1994). It is an aggregate of libraries and electronic information resources bases which are accessible electronically through personal

computers; the focus of the virtual library being the individual users or their workstations. In a true virtual library there is no corresponding physical collection, documents are available in electronic format, they are not stored in any one location, they can be accessed from any workstation and are retrieved and delivered as and when required, and effective search and browse facilities are available (Sherwell, 1997). The usage of communication networks for access, browsing, downloading or transmitting information is essential in a virtual library environment.

It is easy to create digitised copies of text, photographs, music and video. Further, digital information is highly vulnerable to manipulations and results in plagiarism. Unlike their printed counterparts, close monitoring and restriction of usage of digital documents is difficult. Many instances of plagiarism of digital information by 'unscrupulous authors' have been reported (see for example, Denning 1995). To overcome these problems, solutions like dedicated server, document digest algorithms, and exptographic signatures have been suggested (Lynch. 1994). Digital information can be distributed across the globe through e-mail, bulletin boards and networks. The proliferation of personal computers and decreasing costs of primary and secondary mass storage media made it possible to transmit, download, store, despise and print electronic information. Further, downloaded documents can be forwarded to others without the knowledge of its rightful owner. Digital documents become easy targets for tampering; unwanted, unauthorised and objectionable information could be incorporated or uploaded. Digital information poses serious concerns like acceptability, reliability, accuracy and authenticity, accountability, readability, preservation, archival maintenance, socio-cultural, ethical, pricing, and the all too important copyright issues which have been dealt by authors elsewhere (Lakshmana Moorthy and Karisiddappa, 1996). One major concern which has been recently receiving a lot of attention from authors, publishers, library professionals and users a like is the protection of intellectual property rights (IPRs) including copyright in the digital/virtual library environment. This paper addresses some of the IPRs associated with electronic/digital information resources in the digital age, particularly, in the area of internet.

Intellectual property rights

Intellectual property right is a general term which covers copyright, patterns, registered designs and trademarks. It also covers layout designs of integrated circuits, geographical indicators and anti-competitive policies in contractual licenses. As R&D or artistic work involves a lot of effort and resources, inventors, authors or creators resort to legal remedies when the IPRs of their works are infringed. Developments in modern digital technology have led to a review of the provisions of IPRs both at national level by many countries. The developing countries are also catching up with this trend as the value of IPRs is increasingly felt.

Copyright regulations and legislations

Copyright is generally understood as a right or license free copying. However, in reality it is a legal right to prevent others from illegal copying. Copyright is an economic system for ensuring the creation of new knowledge by rewarding their creators and their agents; (it provides) an assurance that the creator can determine, if, how, where and which form his or her creation can be used (Garrett, 1991). Copyright provides the creators of literary or artistic works rights of ownership and legal protection against unlawful reproduction of their works. Many developed countries such as the US, Japan, European Commission, Canada, Australia, etc have tough regulations to

overcome the challenges posed by the digital technologies. Many countries have amended copyright regulations to deal with IT developments and also issued new laws to control infringements. For example, the Anti-electronic Racketeering Act of 1995 of US makes it unlawful to use any computer or computer network to transfer unlicensed computer software, to transmit a communication intended to conceal or hide the origin of money or assets derived from racketeering activity, and to operate for racketeering activity. It is unlawful to distribute computer software that encodes or encrypts electronic or digital communications over computer networks even unknowingly regardless of whether such software is designated as non-exportable. It is also unlawful to damage or threaten to damage electronically or digitally stored data.

The electronic transmission of copyrighted material, without the permission of its rightful owner, is an infringement. The online service providers will be held strictly liable for all user infringements irrespective of whether they knew it or taken any preventive steps against it. It is illegal to supply equipment, software, or services which are capable of circumventing the technological protection of intellectual property rights. This puts manufacturers at risk even if they have no ulterior motive in developing a system or device which can be used by some 'ingenious' user for decryption or circumventing the copyright mechanism.

Although there is difference of opinion with respect to originality and treating a database as intellectual property, the contents and their selection, internal coordination between the structural elements, and the arrangement of elements in a database are generally treated as original intellectual work. Under Berne Convention, WIPRO Copyright Treaty, and TRIPS agreement of World Trade Organisation, copyright rules are applicable to computer databases and are treated as compilations for this purpose. In many countries including USA and UK, copyright laws extend the copyright protection to computer databases, treating them as literary works, and treat storing of a work in any medium by electronic means as infringement. The European Union Directive on Legal Protection of Databases (introduced from January 1998) protects the structure of the database and covers non-electronic (printed) databases also. It enables the owner to forbid or control the extraction or re-use of material taken from the database..

Most of the database vendors allow users, through license agreements, to download a portion of the database on to a 'temporary file' for research purposes. However, there is no clear-cut guideline as to how much data can be downloaded at a time. Most of the CD-ROM databases are used in providing SDI services to the institution's research user community. When SDI profiles are large in number, data downloaded for printing will be substantial, although there will be considerable repetition of downloaded data due to the overlapping subject interests of users working on similar projects. Though this is being done strictly for research purposes and under fair use, is it permissible? Also, retransmission of downloaded information over communication networks is prohibited by all database owners. But it is not clear if a user downloads information of his research interest from more than one database over a period of time and compiles a subject-specific personal database in a modified format. Has the user infringed the rights of the database owners? Can the user be permitted to transmits this personal database to colleagues? All these questions need to be addressed.

There are disparities in the IPR laws of different countries and need harmonisation to facilitate transborder flow of information and trading. For example, storing a work in electronic form by anyone other than the rights owner is treated as infringement. It is not permitted under the

copyright laws of UK, USA or India even for research purposes or private use. Some national copyright laws do not prevent and allow electronic storage and copying. For example, the French Copyright Law does not prevent the electronic copying and storing of information although it prevents electronic delivery to third parties (Norman, 1995). Policies of some countries (for example, the USA) deny export of secure encryption products to other countries; some do not allow usage of encryption techniques. Unless the encryption key and algorithm are provided to the authorities, encryption of civilian communications in France is prohibited. Taiwan and South Korea request companies to remove encryption from voice, *data, and facsimile telephone connections (Schneiner, 1997, p. 277). The US Copyright Law covers derivative works which include digitised works (Wilf, 1994). The European Union 1992 Copyright Directive on Rental and Lending Rights (92/100/Eec) extends exclusive right to all copyrighted work; public library lending of computer programmes (software) and CD-ROMs is an infringement of copyright unless there is a permission or license for doing so (Copyright Queries, 1995).

Influence of internet

Virtual libraries have been made possible mainly because of internet; the vast electronic information resources held by it became handy in the development and management of virtual libraries. However, this has also resulted in an increased number of rights violations, and data and network security problems. Internet has given an opportunity to be one's own publisher. The influence of internet, challenges, issues and concerns of librarians and users in the virtual library environment have been discussed elsewhere (Lakshmana Moorthy and Karisiddappa, 1998). In the developed countries, there is hardly any R & D or academic institution, or professional society or commercial publisher which has not established a home page on internet for disseminating information about itself, its activities and services, products, etc. This is slowly catching up with developing countries like India, Internet facilitates easy mass distribution of digital material. It is increasingly being used for a variety of crimes ranging from simple to complicated ones. Uploading fraudulent matter_encrypted or hidden_on to remote hosts, spreading computer viruses, importing unwanted and obscene material, and software bootlegging and hacking activities, etc are a few such activities and for protecting the rights of owners.

Problems and concerns in cyberspace

The most important problem in the virtual library environment is copyright in cyberspace. Existing copyright laws have not caught up with the technological developments in cyberspace. Many a times there is no clarity whether the content of electronic resources are free or priced. Although the copyright statements appear in many cases, they are elusive to locate in some cases. It can be argued that publishers of promotional, advertising and marketing material on the web implicity encourage downloading, printing and copying the material for redistribution to more than one in the same organisation (Ardito and Eiblum, 1998). However, one can see copyright notices on advertising and marketing material confusing the situation.

One of the most popular ways to protect rights and provide secure access to e-journals over networks is through the usage of passwords. Many e-journal publishers and vendors use this time-tested mechanism. The Security and Rights Management System of ISI electronic library project (Anderson & Lotspiech, 1995) employs password for providing secure viewing at the client level Blackwell offers Electronic Journal.

Navigator service which also acts as a subscription mechanism and allows subscribers/end-users log on and browse journals with a single password regardless of the storage format or location. The access is through user name and password. The Science Direct of Elsevier Science, a full-text electronic information resource service of nearly 1600 scholarly journals, also uses password.

Many electronic papers on internet allow personal and fair use; many more lack explicit statements if they are free or priced. It is not clear whether one can forward free electronic resources available on internet to colleagues and friends or through listservs. It is a copyright violation to e-mail a web page by an intermediary to a colleague or a user strictly for information sake and even no financial gain is involved. In these circumstances, the user can only provide information about the URL where the piece of information appears; this restricts the availability of information to those having access to Internet which is against the principles of fair use. Even downloading e-mail is an offence under the new copyright regimes (Rosenoer, 1997).

Cyber commerce offers new ways of buying and selling for vendors as well as customers (users). The inexpensive and world-wide access to internet available to business, public and private institutions and the general public coupled with the inherent weaknesses of the traditional paper-based transactions and payment made e-commerce an exciting opportunity. It offers cost and time savings through electronic data interchange, electronic fund transfers, online ordering and just-in-time delivery of goods/services. The growing value of Internet commerce is a testimony to its popularity. But lack of integrity and security leads to a loss of dollars due to skilful counterfeiting, fraudulent replication of cheques and compromising credit card numbers.

In the process of e-economic, information sent by users/customers can easily be scanned by clever hackers, eaves-droppers, system administrators or regular users while the mail passes through intermediaries before reaching destination. It would be easy to operate an automatic computer programme to collect credit card information which could be used for ulterior purposes including impersonating others (Schneiner, 1997, p.275). While sporadic usage of encryption of messages by users may arouse suspicion, its widespread use would ensure security. A Consumer Protection Act for Digital Products has been proposed in USA to support e-commerce and to control the increasing abuse and lack of security over information highways (Hampel, 1996).

Usage of digital watermark/signatures

Digital signatures of information like buyer/seller identity numbers, date, time, unique transaction number, etc. can be added to digital products. This technique makes it possible to digitally mark and bind a software product for transferring to a specified customer. The Security and Rights Management System employs digitally signed finger prints to guarantee document authenticity (Anderson & Lotspiech, 1995). A digital watermark is a digital signal or pattern inserted into a digital document, similar to the on-screen logos used by TV channels. In this technique, a signal or a pattern or a logo, digitally included in a document, 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. However, these watermarks persist during viewing, printing or re-transmitting, thereby establishing ownership. These watermarks can be removed by the legal user with a predetermined algorithm.

Apart from authentication, detection of unauthorised source of legal copies, the visible watermark also helps in discouraging illegal copying. Invisible watermarks can also perform these tasks. A detailed account of watermarking technology including counterfeiting schemes is discussed elsewhere (Berghel, 1997). The Security and Rights Management System (Anderson & Lotspiech, 1995) employs encryption and watermarks for secure printing guarantee to document authenticity by means of a digitally signed finger print. Two types of watermarks are added to discourage unauthorised copying: one hidden in the image file of each page of the electronic article, and the other, a visible water mark encoding one Kbyte information in a two-dimensional bar code placed on the first page of each article. The illegal copies will not have the bar code which means that coyright infringement has taken place.

Like their digital counterparts, multimedia works are also prone to infringement of copyright, as increasing availability of high bandwidth networks makes it too easy to illegally duplicate and disseminate these documents without any loss of quality. Legislations by various nations do not clearly address the legal status of multimedia works. These works, though not explicit, are covered and classified under audio-visual works by the USA, UK and Indian laws. When multimedia works are commissioned under contract, they are treated as works made for hire where the copyright owner will be the person/institution who 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 another sub-contractor as a part of a multimedia work. As it provides a cost-effective medium for dissemination many creators use the web for publishing animation, images, video and music. With increasing popularity of hypertext-based web, the possibility of illegally obtaining the multimedia data is growing. This prevents the owners of multimedia works fearful of releasing their proprietary information without proper security and rights management benefits.

The growth of networked multimedia calls for mage copyright protection. This can be achieved using signal processing, data compression, encryption and system-level security protection. Another way is the incorporation of an invisible watermark (or a digital signature). However, it is easily identified by a computer programme which decodes the key used to affix the wate mark in a particular location on a page or part of the document and retrieves it. These invisible watermarks are of two types; those which are destroyed when subjected to manipulations and those which cannot be destroyed (Garofalakis, et. al., 1997). Usage of watermarks can identify (a) the legal owner (for example, the creator) of the multimedia work, (b) the recipient of an authorised single user copy, and (c) when the multimedia work is modified or tampered (Civanlar and Reibman, 1997). The multimedia protection protocol is another convenient way of ensuring IPR for all types of digital data (Rump. 1997). Wolfgang and Delf (1996) described two techniques of invisible watermarking of multimedia images which can detect all but the most minute changes in the image.

Protection from piracy of mass-produced, look-alike digital products on floppies or CDs containing software, applications, graphics and images, music, etc. is all the more difficult. Some companies take various steps to reduce losses. These include holographic emblems affixed on each copy (for example, by Microsoft). However, such steps only help in establishing authenticity of the product and may not prevent their illegal copying.

Security of information over networks

Several electronic copyright management systems have been evolved by many academic institutions and publishers to deliver electronic information to users in a network environment. These include Patron, Ercoms, and ELINOR Projects (UK), Project Cited (European Commission), Right Pages TM Service, TULIP Security and Rights Management System, etc. a brief account of which can be found elsewhere (Lakshmana Moorthy and Karisiddappa, 1997). Security of information in a network environment involves three aspects, viz. authentication, that is, knowledge of the identity of sender to the receiver (and vice versa); confidentiality, that is, the message sent has not been intercepted by a third person; and integrity that the message is not tampered during transmission. One way to discourage illegal and illicit copying and still distribute over the networks is the use of electronic marking and identification technique. In this, the system automatically generates and puts a unique and indiscernible mark on each of the document copies and registers its recipient. If any one receives an illicit copy (by illegal copying), the system detects the unique mark from the copy and identifies the illegal recipient. The marking is such that it is difficult for an illegal user to discover the unique marking pattern in the user's document. This technique can be used to protect copyright and IPRs, even in electronic publishing where a document is printed, copied or faxed (Low, et al. 1995).

Cryptography is the oldest mechanism employed to ensure security and privacy of information over networks. This involves encryption of the information to render it unreadable or not understandable language which only the legitimate user can decrypt. This is a common technique to protect confidential information from eavesdropping, preventing computer viruses and illegal copying of software, etc. Employment of encryption protocols (public, private and split-key) wherein every bit of information is encrypted at the server end and decrypted at the recipient's end is another technique. The mechanism is such that the cost of reverse engineering is too high and uneconomical, thereby discouraging people from attempting it. Under these protocols the document server encodes, encrypts and compresses the electronic document before sending to a bonafide user. The copyright server authenticates the requests from the user for obtaining documents. A software provided by the publisher at the user's terminal decrypts, displays and prints the document received from document server. The privacy of the user is ensured by encrypting the requests made by the user, and the document serve authenticates the request with a variety of passwords, public encryption keys, etc (Choudhary, et al., 1995). Effective protection of information requires ongoing analysis of computer and network resources. Networks operating in Unix environment pose a host of problems. Unix host-and network-based security products have to meet the increasing complexities and challenges in information security. Further, host-based information techniques and tools must be supported by network-based capabilities. Security Profile Inspector, a technique to perform real-time static analyses of Unix-based clients and servers to check on their security configuration and Network Intrusion Detector, a dynamic tool to identify weak links in a network of clients and servers, monitor and analyse activity on LAN segments and produce transcripts of suspicious user connection have been in use in the US (Feingold, et al., 1996).

Conclusion

The major problem in a virtual library environment is the difficulty of proving rights

violations when they occur. For legal experts, gathering evidence of digital crimes and to maintain its usefulness in a court of law are the greatest problems. The multiplicity of computing standards and data formats makes this still complicated. A 'protocol' for this purpose has been developed in UK which has yet to get acceptance from all parts of the globe. Such systems cannot be 'fool proof'; as soon as it comes into vogue; hackers, who generally have greater resources, better skills and greater desire over those who try to prevent such illegal acts will make efforts to overcome (Barrett, 1997). One way of proving copyright infringement of electronic databases in a court of law is deliberately placing seeds into or salting a database, i.e. planting of errors and omissions. If a pirated database contains the same 'seeds' and errors, it is easy to prove the infringement. Sometimes a particular pattern which is not easily observed can also prove whether the database is a pirated copy. A clever pirate can detect and correct or eliminate some errors or omissions, but removing all, particularly in a large database is rather too unlikely (Losey, et al., 1995).

The various deterrants or regulatory steps like security across multiple platforms, cryptographic techniques, authentication of users and limits to their access, multilevel protection (i.e. at network, system, application and user workstation levels), metering of access time, password regulations, etc. will no doubt protect the IPRs but also work, some times, against fair use. The IPR laws were conceived to enhance, and not to prevent, the information access and usage. The attempts for ensuring and enforcing copyright may be seen by the end-users as non-user-friendly. The mechanisms developed for rights protection may restrict the access and use of digital information only to the privileged few who can afford to pay thus defeating the main purpose of copyright law. Further, it is difficult to draw a boundary line between what is permissible, to what extent, and what is infringement. Small-scale violations which do not conflict with owners rights may have to be accepted as a part of fair use for at least some more time.

Even browsing is a violation of fair use (the existing fair use is applicable only to printed works) and amounts to infringement. It is impossible to ascertain the usefulness of a digital document without browsing and without accessing one cannot browse. This forces the user to pay some sort of fee which is unjustified. If potential users of a digital document are expected to pay a fee, then they must be in a position to determine, in advance, the usefulness of the document and the fee. This is one of the most important issues which concerns the users and librarians alike. In case of printed publications no additional charges are involved even if they are consulted by multiple number of users on a multiple number of occasions. But subscription to online or e-journals involves additional 'fee' in the form of platform fee, multi-user fee, password fee, etc. which is not justified. For the benefit of rights owners and bonafide users, it is suggested to have site licenses at a reasonable cost allowing institutions to provide services and do research without involving complex fee structures.

In virtual library environment, the librarians (or cybrarians) should have the same kind of fair dealing arrangement as in the case of printed books. They should be able to read or browse electronic information without having to pay for it; preserve in digital format copyright material held in their collections; and fulfil inter-library document requests electronically (Norman, 1995). The cybrarians should sharpen their skills in meeting these challenges and should negotiate the same type of privileges as in the case of printed documents for accessing digital information also. They have to develop experitse

in copyright, licensing and electronic redistribution regimes and train staff and end-users in these areas. As we move to the twenty-first century, we may see more and more authors and publishers turning to legal redressal. This is one reason that the copyrighted books and other material are not expected to be readily available sooner in cyberspace are currently available in traditional libraries.

Acknowledgements

The authors thank Dr. SS Murthy, Director, DESIDOC for providing facilities and for the kind permission to present this paper. They also thank Smt. K Shailaja Reddy for secretarial assistance and help in preparing the paper.

References

1. Anderson, Laura Challman & Lotspiech, Jeffrey B (1995). Rights management and security in the electronic library. *Bulletin of the American Society for Information Science* **22**(1), 21-23.

2. Ardito, Stephanie C and Eiblum, Paula (1998). Conflicted copyrights-inevitability : Death, taxes and copyright, *Online*, **22**(1), 81-85.

3. Barett, Neil (1997), *Digital crime: Policing the cybernation*, Kogan Page, London

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

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

6. Civanlar, Reha and Reibman, Amy (1997). Signal processing for networked multimedia. *IEEE Signal Processing Magazine*. **14**(4), 39-44.

7. Copyright queries (1995) ; *Library Association Record*, **97**(9), 469.

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

9. Feingold, Richard: Bruestle, Harry R; Bartoletti; tony; Saroyan, Allyn and Fischer, John (1996). 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. Pp. 55-64.

10. Gapen, D Kayne (1994). *Virtual library: An information kit*, Washington, DC, SLA. p.54.

11. Garofalakis, John, Kappos, Panagiotis; Sirmakessis, Spiros and Tzimas, Giannis 91997). 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, V2, pp. 833-836.

12. Garret, John R (1991). Text to screen revisited : Copyright in the electronic age, *Online*, **15**(2), 22-26.

13. Hampel, Viktor E (1995). A Consumer Protection Act for Digital Products. In *Proceedings of the Conference on Information Protection and Network Security*, 24-26 October 1995, Philadelphia, edited by Viktor E Hampel and Clifford Barlow Neumana, *SPIE Proceedings*, V. 2616, SPIE, Washington, DC. Pp. 145-158.

14. Lakshmana Moorthy, A and Karisiddappa, CR (1997). 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, D.B. Ramesh, K.N. Kittur, P. Padhi and J.R. Sahu, SIS, New Delhi. Pp. 403-416.

15. Lakshmana Moorthy, A and Karisiddappa, CR (1996). Electronic publishing : Impact and implications on library and information centres. In *Digital Libraries: Dynamic store house of digitised information*. Papers presented at the *SIS 96*; Fifteenth Annual Convention and conference, 18-20 January 1996, Bangalore, N.M. Malwad, T.B. Rajashekar, I.K.Ravichandra Rao and N.V. Satyanarayana (eds). New Age International Publishers, New Delhi, pp. 15-35.

16. Lakshmana Moorthy, A and Karisiddappa, CR (1998). Transformation to virtual libraries: Real or virtual? In Working papers presented at the *SIS 98: Seventeenth Annual Convention and Conference on Virtual Libraries : Internet-based Library and Information Services*, 12-14 march 1996, University of Hyderabad, SIS, Hyderabad, pp. 109-122.

17. Losey, Ralph C.; Subin, Shams and Rosenbluth, Moran. *Practical and legal protection of computer databases*, Wisdom@digital.net.

18. Low, Steven H.; Lapore, Aleta M. And Maxemchuk, Nicholas F (1995). Document identification to discourage illicit copying. In *Procedings of GLOBECOM* 95, 13-17 November 1995, Singapore, IEEE, New York. V.2, pp. 1203-1208.

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

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

21. Powell, Alan (1994). Management models and measurement in the virtual library, *Special Libraries*, **85**(4), 260-263.

22. Rosenoer, Jonathan (1997) CyberLaw: the law of the Internet. New York, Springer p.362.

23. Rump, Neils, *Copyright protection of multimedia data: The multimedia protection protocol.* (http://www.its.fhg.de/departs/amm/layer3/mmp/).

24. Schneiner, Bruce (1997). E-mail security. In The *electronic privacy papers ; Documents on the battle for privacy in the age of surveillance*, edited by Bruce Schneiner and David Banisar. John Wiley. Net York. pp. 275-284.

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

26. Wolfgang, Raymond B and Delp, Edward J (1996). 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, pp.219-222.

A. Lakshmana Moorthy obtained his M.Sc (Physics) and ADIS from DRTC. He has been in the field of Information science for nearly two decades and is currently working as Joint Director at DESIDOC, at New Delhi. He is a member of several professional bodies in India.

Address : Jt. Director, DESIDOC, Metcalfe House, Delhi 110 054.
E-mail : general@desidoc.ren.nic.in
almoorthy@hotmail.com

C.R. Karisiddappa received PhD in Library and Information Science from Gulbarga University in 1983. He served as an expert member of IGNOU, New Delhi, B.R. Ambedkar Open University, A.P. and Annamalai University Distance Education Programme.

Address: Professor, Dept of Library & Information Science, Karnatak University, Dharwad-580 003