DOCUMENT RESUME

ED 318 415 IR 014 319

AUTHOR Lyons, Patrice A.
TITLE Policy Issues in Computer Networks: Multi-Access Information Systems.
PUB DATE Oct 89
NOTE 24p.; Paper presented at the Annual Telecommunications Policy Research Conference (17th, Airlie House, Warrenton, VA, October 1-3, 1989). For other papers of this conference, see IR 014 305-322.
PUB TYPE Viewpoints (120) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Computer Networks; *Copyrights; *Databases; *Information Systems; *Intellectual Property; Online Systems; *Ownership; Privacy; Telecommunications
IDENTIFIERS Digital Libraries

ABSTRACT

As computer databases become more publicly accessible through public networks, there is a growing need to provide effective protection for proprietary information. Without adequate assurances that their works will be protected, authors and other copyright owners may be reluctant to allow the full text of their works to be accessed through computer networks. There may also be a hesitancy on the part of users, such as librarians, to avail themselves of the material that may be accessible online, where the terms and conditions of access, if any, are unclear, or where the costs are prohibitive. The development of transactional frameworks for the collection and distribution of royalties in connection with computer networks, including possible mechanisms for obtaining required permissions online, is by far the most important undertaking in this context. However, there are several related measures that also require clarification in order that computer networks may achieve their promise of wide-spread access to information in electronic form. The paper discusses five issues that require further consideration: (1) ownership of rights in pre-existing works; (2) copyrightability of databases; (3) the Electronic Communications Privacy Act; (4) identification and intellectual property; and (5) digital libraries. (GL)

POLICY ISSUES IN COMPUTER NETWORKS:

MULTI-ACCESS INFORMATION SYSTEMS

THE SEVENTEENTH ANNUAL TELECOMMUNICATIONS

POLICY RESEARCH CONFERENCE

Airlie House, Airlie, Virginia

October 3, 1989

Prepared by:

Patrice A. Lyons, Esq.
Haley, Bader & Potts
2000 M Street, N.W.
Washington, D.C. 20036

Introduction

Before addressing some issues raised in connection with Multi-Access Information Systems, I would like to reflect on the development of the intellectual property laws in the United States when faced with new developments in technology, and, in particular, the copyright law. From the early days of the republic, there has been a recognized need to extend copyright protection to creative works in order to encourage the continued production of such material for the enrichment of society at large. The usefulness of the copyright system and the real contribution it makes toward promoting the development of new products and services has long been recognized. However, determining what constitutes a work that is deserving of protection, or deciding on the degree of protection that should be afforded, has not always been easy to accomplish.

For many reasons, copyright law is often difficult for people to understand and apply. This is particularly evident in the area of computer programs where there is considerable uncertainty about the nature and scope of protection for computer screen displays as well as for the structure, sequence and organization of programs. While the complexity of the challenges posed to the copyright system by advances in computer technology has increased considerably in recent years, a flexibility has been demonstrated on the part of Congress and owners of copyright to seek ways to evolve the system to meet these new developments. Indeed, the adaptability of the legal

structure has been a hallmark of the copyright system over the two hundred years that have elapsed since the first law was enacted in 1790 (the bicentennial of the U.S. patent and copyright laws will be celebrated in May 1990).

An example from the not too distant past may help clarify how the copyright law has evolved to accommodate advances in technology. In Edison v. Lubin, [1]/ a case decided around the turn of the century when the industrial revolution was spawning many new works, the well-known inventor, Thomas Edison, brought an action for copyright infringement of his film depicting the launching of Kaiser Wilhelm's yacht Meteor. The case was decided by the Court of Appeals in 1903, shortly after the copyright law had recognized that a photograph could, in certain cases, be subject to copyright. At the time, there was no category of work called "motion pictures." The court was asked to decide whether a positive reproduction on a celluloid sheet made by light exposure that, when thrown on a screen in rapid succession "by means of an applicance similar to a magic lantern" so as to give the effect of actual motion, constituted a protected photograph.

In its decision, the court was able to make the intellectual jump from protection for a single photograph in the conventional sense to find that a series of different views when reproduced from a negative also constituted a single photograph as a whole or unit. However, in deciding this issue, the court was required to pigeonhole the new work into then existing

---

[1]/ Edison v. Lubin, 122 F. 240 (3d Cir. 1903).

classes. The status of motion pictures was finally clarified in 1912 when Congress amended the copyright law to add "motion pictures" to the specific categories of protected works. In extending this protection, however, Congress still clung to the notion of moving "pictures" rather than coining a term to reflect the particular characteristics of the new type of work.

This early case serves to illustrate the difficulty with which the law addresses new technological developments, and to demonstrate that, when protection is finally recognized, it is often by a process of accretion. In this respect, it may be said that the copyright law has one foot in the past and one in the future. While this may be a bit frustrating for scientists who would like the law to be more decisive and change more rapidly, it does insulate the public from turbulence in the copyright system. Gradual evolution of the system allows for a degree of predictability in legal relationships, and affords interested parties a period within which to adjust their business practices to the new realities.

The Edison case may also help place the current debate over copyright protection for computer programs and databases in perspective. From an historical vantage point, it appears evident that motion pictures were a new creative work. In the early part of the century, however, it was not so clear. A lesson to be learned is that the law requires time to evolve to meet new situations and that persons of foresight and courage, such as Thomas Edison, can make a difference.

Computer Networks and Copyright

Let me now turn to the issues raised by multiple access to information systems in light of recent and anticipated future advances in the computational speed, capacity and pervasiveness of computer networks. In approaching this subject, I will not specifically discuss situations where a computer information system (comprised generally of computer databases and any related programs and hardware) is developed within the confines of a private entity, and access is restricted to persons directly related to that entity, whether at the same or a remote location. Access in that context would likely be restricted by contractual arrangements, and the data protected as a trade secret.

As you move away from the private realm to computer databases that are publicly accessible through public networks, there is a growing need to provide effective protection for proprietary information. Without adequate assurances that their works will be protected, authors and other copyright owners may be reluctant to allow the full text of their works to be accessed through computer networks. There may also be a hesitancy on the part of users, such as librarians, to avail themselves of the material that may be accessible on-line, where the terms and conditions of access, if any, are unclear, or where the costs are prohibitive. The price lists and restrictions on access that often accompany exisiting commercial databases, and the diversity and complexity of access mechanisms, are frequently off-putting to the user.

The development of transactional frameworks for the collection and distribution of royalties in connection with computer networks, including possible mechanisms for obtaining required permissions on-line, is by far the most important undertaking in this context. However, there are several related measures that also require clarification in order that computer networks may achieve their promise of wide-spread access to information in electronic form. The following are a few of the issues that merit further consideration.

1. Ownership of Rights in Preexisting Works

The status of rights in works covered by previously negotiated contracts may require some adjustment. At a recent gathering to discuss possible arrangements for the clearance of rights, a periodical publisher expressed an interest in making works available on computer networks, but noted that their existing contracts with contributors do not provide for access in this form. To go back at this stage and renegotiate these contracts would pose a substantial burden. On the other hand, since the new use was not anticipated in the original arrangements, some additional remuneration should be provided, where appropriate, in the event an author may be located.

Some guidance on this issue may be found in the wording of the copyright statute as it applies to contributions to collective works such as periodicals. Section 201(c) of the copyright law provides that: "In the absence of an express transfer of the copyright or of any rights under it, the owner

of copyright in the collective work is presumed to have acquired only the privilege of reproducing and distributing the contribution as part of that particular collective work, any revision of that collective work, and any later collective work in the same series." [2]/ Consideration could be given to extending this presumption to cover access through a computer network solely for works created before an agreed date. However, this would only cover collective works. Other measures may be required for photographs, maps, and other material.

A related question was raised by an organization having possession of thousands of photographs in its archives. In the case of recently created works, the copyright owner's address may be known, even though it may be administratively difficult to contact him or her to obtain the authorization to make the works available on-line. However, for older works, there may be no trace of the original author. This is a difficult and sensitive issue that will require careful and imaginative treatment in order to establish an equitable balance between the need to respect the rights of authors and the access requirements of researchers and other users.

2. **Copyrightability of Databases**

There has been considerable legal uncertainty with respect to the status of databases under the U.S. copyright law. Databases are usually considered "compilations" under a copyright analysis; and, a compilation is defined under the copyright law

---

[2]/ 17 U.S.C. § 201(c) (1982).

as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship." [3]/ Where a compilation is formed through the selection and arrangement of works which are in themselves protected by copyright, the work is called a "collective work." Problems usually arise where a given database contains primarily fact-based material that is not separately copyrightable. An example of such fact-based material would be a compilation of names, addresses and telephone numbers in an electronic directory.

A conflict has emerged between the U.S. Circuit Courts of Appeal on whether protection for databases may be premised on "sweat of the brow" or "industrious collection" alone, or whether "originality" in the selection and arrangement of the contents is also required. Particular doubt was cast on the adequacy of the copyright law as a vehicle for securing protection for databases by the decision of the Second Circuit in Financial Information v. Moody's Investors Service. [4]/ In that case, the court took a restrictive view of copyright protection in the case of fact-based works. The case involved a service consisting of financial information printed on index cards regarding municipal or other government bonds which the issuer had called for redemption.

---

[3]/ 17 U.S.C. § 101 (1982).

[4]/ Financial Information v. Moody's Investors Service, 808 F.2d 204 (2d Cir. 1986), cert. denied, 108 S.Ct. 79 (1987).

Finding that the selectivity involved in compiling the factual information on municipal bonds was in the nature of "a simple clerical task" and that there was "no room for selection or choices or judgment" in compiling the data, the court held that the compilation of financial facts included in the Daily Bond Cards in question were not copyrightable.

The U.S. Copyright Office recently looked to the decision in Financial Information in deciding that claims to copyright in digitized representations of typeface designs were not registrable under the Copyright Act of 1976. Citing the Financial Information case, the Office noted that: "To be an original work of authorship, a compilation must include subjective elements of human selection and arrangement.. . . Because the typefont data is determined by the ultimate shape of the typeface character, and requires de minimas, if any, selection and arrangement, it does not qualify as a compilation or any other original work of authorship." [5]/ There is a growing concern that, in order to further the continued development of the database industry, an understanding should be reached either in the courts or in Congress on the proper construction of the copyright law in connection with computer databases.

Whether "originality" should be the standard for databases was also deliberated at a recent meeting convened under the auspices of the United Nations Educational, Scientific and

---

[5]/ Policy Decision on Copyrightability of Digitized Typefaces, Notice of Policy Decision, 53 Fed. Reg. 38110, 38112 (1988).

Cultural Organization (Unesco) and the World Intellectual Property Organization (WIPO). Several participants noted that:

> [T]here were countries where mere skill and labor were not enough for collections to qualify as works protected by copyright on the basis of the notion of originality prevailing in such countries, but where the significant investments made by data base producers did, on the other hand, need and deserve some kind of protection. [6/]

At the Unesco/WIPO meeting, it was urged that consideration be given to the adoption of a limited related-rights type protection for electronic databases that are not eligible for copyright protection because of their lack of originality. Some participants cautioned, however, that a sui generis protection for databases would not be covered under existing international copyright conventions and could result in the dilution of copyright protection. While it was suggested that "states should extend copyright protection to electronically compiled collections of data on the basis of a reasonable standard of originality and should never insist on a higher standard than for traditional compilations," the Unesco/WIPO group did not make a specific recommendation on what would constitute a reasonable standard of "originality."

While copyright law plays a lead role in connection with the entry of protected material into a digital information

---

6/ Memorandum Prepared by the Secretariats, Pt.III, para. 232, Committee of Governmental Experts on the Evaluation and Synthesis of Principles on Various Categories of Works (Geneva, June 27 to July 1, 1988), reprinted in Copyright (WIPO) (Nov. 1988); see also Green Paper on Copyright and the Challenge of Technology, COM(88) 172 final, Commission of the European Communities, para. 6.6.2, at 215 (June 1988).

system (i.e., entry being deemed a reproduction), it may not provide adequate protection for the system itself when the information is accessed electronically. Since it will be necessary to assure information suppliers that their works will be protected against unauthorized access, reliance on other bodies of law is advisable. Of particular interest in this context is the recently enacted Electronic Communications Privacy Act of 1986, and, to some extent, the Communications Act of 1934, as amended.

3. Electronic Communications Privacy Act

In a prescient draft prepared for a 1983 conference, the late Professor Ithiel de Sola Pool reflected on the inadequacies of copyright in an electronic environment. He stressed that, unlike the age of the printing press, where there was a "strategic bottleneck for control," "[i]n electronic publishing, copying does not require printing. One need simply provide computer access." Reflecting on the need to "stop speaking about 'copyright' and start speaking about 'service-right,'" Prof. Pool observed that:

> [W]hat must be prevented above all else, most would agree, is for vendors who pay nothing to the owner of privileged software to use this software in services for sale. Legal restraints should be applied primarily to such organized vending, not to copying. The industry should encourage the formation of directory, maintenance and other value-added service organizations, and seek to have government enact legal structures through which such institutions become collectors and distributors of royalties. 7/

7/ I. de Sola Pool, "Whither Electronic Copyright," Electronic Publishing Plus, at 228 (1983).

Some progress in this direction was made by Congress with the enactment of the Electronic Communications Privacy Act of 1986 ("ECPA"). Under the ECPA, the focus of protection is not on specific rights in specific works, but rather on the integrity of the electronic transfer and storage process. This protection for the electronic communications service may provide the necessary "strategic bottleneck of control." It also reflects the trend in recent years toward relying on a concept of controlled access, buttressed by technical controls, rather than traditional copyright theory for protection.

With certain exceptions, the ECPA generally prohibits any person from "intentionally" intercepting, [8]/ using, or disclosing any electronic communication, where the interception or access to the communication is not made through an electronic communication system that is configured so that the communication is "readily accessible to the general public," that is, where the communication is scrambled or encrypted, transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of the communication, and specific other situations set forth in the law. [9]/ The law also protects against access without authorization to "a facility through which an electronic

---

[8]/ 18 U.S.C.A. § 2510(4) (West Supp. 1989).

[9]/ See 18 U.S.C.A. § 2511(1)(a)-(d) (West Supp.1989). For definition of "readily accessible to the general public," see 18 U.S.C.A. § 2510(16).

communication service is provided." [10]/ However, if an electronic communication system does not place the required technical restrictions on access, protection for the electronic communications transmitted or stored in that system would not be available under the ECPA.

The ECPA also provides for the situation where an electronic service provider offers a mixture of services: some readily accessible to the public, and other intended to be private or confidential. In its report on an early draft of the law, the House Judiciary Committee observed that:

> Such a system typically has two or more distinct levels of security. A user may be able to access electronic bulletin boards and the like merely with a password he assigns to himself, while access to such features as electronic mail ordinarily entails a higher level of security (i.e., the mail must be addressed to the user to be accessible specifically).. . . Those wire or electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public. [11]/

Thus, where a system is configured with several access layers requiring "keys" or some other mechanism to move from one access layer to another, it would appear to be covered by the ECPA. Such systems are usually developed as a control on access to sensitive restricted data; however, this capability may also be relevant for purposes of securing protection for copyrighted

---

[10]/ See 18 U.S.C.A. §§ 2701 and 2707 (West Supp. 1989).

[11]/ Electronic Communications Privacy Act of 1986, H.R. Rep. No. 99-647, 99th Cong., 2d Sess. 63 (1986) (hereinafter cited as House Report).

works in a high-speed computer network environment.

The advantage in relying on the ECPA for protection of electronic communications in connection with digital information systems is that liability under the statute is not based on a determination of the legal status of the specific contents of an electronic communication. Where steps are taken to ensure that an electronic communication is not readily accessible to the public, the ECPA would generally provide protection against the intentional and unauthorized interception, use or disclosure of the communication, apart from the myriad possible rights in the contents, or lack thereof. Since the provisions restricting access by third parties generally relate to the electronic communication, not the contents embodied therein, arguments based on "fair use" of the contents under a copyright analysis may not be appropriate in this context. However, since the ECPA is new and virtually untested in the courts, the parameters of this important legislation remain unclear at this time.

The Communications Act of 1934, as amended, may also have some relevance in this context. For purposes of the ECPA, an electronic communication includes generally "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." [12/] Since the definition covers transmissions by radio, there is an area of overlap

---

[12/] 18 U.S.C.A. § 2510(12) (West Supp. 1989).

between the ECPA and the Communications Act. With respect to this overlap, the Senate Committee on the Judiciary has observed:

> As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice. Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences. Although radio communications are within the scope of the Act, the provisions of the Electronic Communications Privacy Act directed specifically to radio do not affect the applicability of section 705 of the Communications Act of 1934, as amended, to actions by members of the public. [13]/

The House Committee on the Judiciary further clarified the interplay between section 705 of the Communications Act and the new law. In its report, the Committee pointed out that, "where this bill provides that 'it shall be unlawful' for the public to engage in specific conduct with respect to radio transmissions, the Committee intends that such a provision does not 'authorize' the conduct for purposes of the first sentence of Section 705(a) of the Communications Act." [14]/ With respect to activities that were "implicitly authorized" for purposes of section 705 by judicial interpretations, the House Committee stated its intention that these interpretations were to remain in effect

---

[13]/ Electronic Communications Privacy Act of 1986, S. Rep. No. 99-541, 99th Cong., 2d Sess. 14 (1986); see also House Report, at 22 (Communications Act might have some limited application to electronic communications).

[14]/ House Report, at 41.

after enactment of the new law. [15]/

The relationship between the ECPA and the Communications Act is also clarified to some extent in the language of the ECPA. Section 2511(2(g)(iii) of the ECPA provides that it is not unlawful for a person to engage in any conduct which: "(I) is prohibited by section 633 of the Communications Act of 1934 [relating to unauthorized reception of cable service]; or (II) is excepted from the application of section 705(a) of that Act [dealing with the interception or receipt by an individual of satellite cable programming for home viewing]. [16]/ The interaction between these statutes may have some relevance where an electronic communications service is furnished to the public over cable systems or using satellite carriers. Future judicial decisions construing these provisions may resolve certain of the ambiguities that arise with respect to the application of the communications law to unauthorized access to computer networks.

4. Identification of Intellectual Property

An important new area of concern is how to identify and display information pertaining to intellectual property rights in new storage technologies such as compact read only optical disks (CD-ROM). The National Information Standards Organization has charged NISO Standards Committee TT with the drafting of

---

[15]/ Id. For text of section 705 [47 U.S.C. § 605], see Compilation of the Communications Act of 1934 and Related Provisions of the Law, at 181 (Comm.Print 1988).

[16]/ 18 U.S.C.A. § 2511(2)(g)(iii) (I) & (II) (West Supp. 1989).

standards for the contents of certain files on CD-ROM and other optical media. The work of this Committee builds on the extensive efforts made in recent years to prepare an international standard specifying the volume and file structure of CD-ROM for the interchange of information between users of information processing systems. Published in 1988, this standard is known as ISO 9660. [17]/ One task of Standards Committee TT is to specify data elements for the Copyright file that is specified in ISO 9660. The Committee will also be suggesting standard data elements and the formats for carrying those data elements on CD-ROM and other optical media for the Publisher, Data Preparer, Abstract, and Bibliographic files.

I mention this project because of the implications of decisions made in the optical media context for the development of transactional frameworks for the clearance of rights in a computer networking environment. It is evident that CD-ROM and other optical media may eventually serve as storage devices in an on-line environment. Remote access to material fixed on CD-ROM may be facilitated by the proper identification of proprietary claims in the contents, including any rights in computer programs embedded in a CD-ROM to facilitate access. It is no longer the case that claims are readily identified by a copyright notice.

Effective March 1, 1989, when the U.S. joined the Berne Convention for the Protection of Literary and Artistic Works, the

---

[17]/ Information processing -- Volume and file structure of CD-ROM for information interchange, ISO 9660: 1988(E).

copyright notice was eliminated as a condition of copyright in order to bring the U.S. copyright law into compliance with the Berne Convention. In taking this step, Congress softened the impact somewh t by adopting what is known as an "innocent infringer" provision. Under this provision, where a notice of copyright appears on published copies or phonorecords to which a person has access, a defense based on innocent infringement may not be asserted in mitigation of actual or statutory damages in an action for infringement (except as otherwise provided in the law for nonprofit educational institutions, libraries or archives, and public broadcasting entities). While the innocent infringer provision provides some incentive for including a copyright notice on published works, many producers may now cease using the notice, particularly for works that are not distributed internationally. The law does not provide for any notice on unpublished works that may be subject to copyright.

Owners of copyright might be heard to say that, where there is no notice of copyright, all works should be presumed to be protected. Such an interpretation may have unfortunate consequences. Where material accessible in a networking environment is in the public domain, a librarian or other user may be inhibited from using the information by the absence of a notice. While the subject was not taken up in the context of the Berne implementing legislation, there is a provision in the Berne Convention that does support the case for presumptions. Under Article 15 of the Convention, if the name of the author

(and, in certain countries such as the United Kingdom, the publisher) appears on a work "in the usual manner," there is a rebuttable presumption that, as specified in the domestic law of the member country, the person named is the owner of copyright and entitled to institute infringement proceedings. [18]/ In this post-notice world, it may be an opportune time to reconsider the significance of markings on works to indicate ownership of copyright, or at least the presumption of ownership.

In addition to the Copyright file, there are other files listed in ISO 9660 that may be relevant for copyright purposes. In reviewing this standard, the field in the Extended Attributes Record named "Permissions" is of particular interest. Transactional frameworks for clearance of rights on-line in a network environment may eventually be possible, and the portion of the CD-ROM dedicated to permissions may have some relevance in this context. While the ISO 9660 standard may now refer to permissions for security reasons, this file may also be useful for identifying permitted uses.

Generally, the bits in the Permissions file contain read and execute access control. When a CD-ROM is put on a network, the software used to control access looks in the Permissions file, compares the privilege bits in the Extended Attribute Record, and determines the degree of permitted access.

---

[18]/ For text of Berne Convention, see President's Message to Congress Transmitting Berne Convention for the Protection of Literary and Artistic Works (June 18, 1986), reprinted in S. Treaty Doc. 99-27, 99th Cong., 2d Sess. (1986).

For example, if a user tries to open a file, it calls the system server and the server checks the Permissions file to see whether the user is authorized to open the file. If the Permissions file gives read privileges to the World, the device driver will not limit access to anyone. If read privilege is denied, a person coming across a network would be denied access.

The degrees of access are usually grouped under four headings: World, System, Group, and Owner.

1. World: Everybody possible
2. System: System manager of a particular computer in a particular place, i.e., person in charge
3. Group: A set of individual users typically defined by the owner
4. Owner: Individual user

While there may be difficulties in using such an approach in connection with CD-ROM (since CD-ROMs are usually single user devices and access over networks is relatively slow at this time), the idea of embedding information on access in storage media merits further consideration.

Another approach that has been suggested is the use of card keys for access to a CD-ROM system to set levels of privileged access. It may be possible for access software embedded in a microchip on such cards to control access. This system would by-pass the Extended Attribute Record.

Since standards developed with respect to CD-ROM and other optical media may be useful for copyright purposes, it is advisable that such standards be coordinated with work under way

in the area of high-performance computer networks in order that any standards adopted be compatible. There is a need for deployment and experiment with technical controls in a network environment to support any contractual arrangements that are developed for the clearance of rights in the contents. While the database industry has grown considerably in recent years, we are still at a relatively early stage in the evolution of computer networks as an effective means of public access to information and knowledge.

For example, a system could be constructed where the owner of rights in information fixed on a CD-ROM would set basic terms and conditions of access in the Permissions file. When accessing the contents of a CD-ROM over a network, if a user wants to go beyond the standard access conditions, provision could be made for the network programs to interrogate the owner of rights on-line at the behest of a user in order to secure the necessary authorizations, and to arrange for payment of any royalties. Under this scenario, the system could check the Copyright file on the CD-ROM to determine the name of any copyright claimants in the contents, and their on-line addresses, for purposes of facilitating the clearance of rights in the contents. While there may be obvious loopholes in such a system, e.g., software could be written that would ignore the Permissions file and cause the controls to fail, I offer this hypothetical to illustrate how computer network systems and related storage devices could provide for data elements and other mechanisms that

may be adapted to the world of intellectual property. Such synergistic action between technical and legal controls would be helpful toward the development of advanced applications for computer networks.

5. **Digital Libraries**

The development of transactional frameworks for the clearance of rights in a networking environment should be facilitated by the proposals that have been advanced to develop and implement a distributed information system based on advanced computing and communications technology. For example, the Digital Library System ("DLS") proposed by the Corporation for National Research Initiatives will allow users to access information stored at various sites without the user being aware of the actual location or form in which the information is stored. [19]/ Unlike conventional databases, a user will not control directly how information is accessed by the DLS. At the risk of oversimplification, there will be a computer program barrier that separates the user from the supplier of information in the DLS.

From a proprietary rights perspective, the capability of the DLS to track and control access to objects in the system is an essential element. In the proposed system, it is possible to associate with each object an access control list. This feature would be used to check user authentication and other

---

[19]/ See The Digital Library Project, Volume 1: The World of Knowbots (Draft), Corporation for National Research Initiatives (March 1988).

profile data. User authentication may entail not just a password, but capabilities a user may have, e.g., a user is not permitted to access a specific class of objects.

Conclusion

The use of multi-access information systems over computer networks holds great promise. In order to realize this potential, the status of intellectual property rights requires further analysis and development. In this context, technology has an important role to play in providing adequate controls on access to protected information.

The task of creating an environment where publishers and other information suppliers look to computer information systems as a new and profitable market for their works, while providing access to users on agreed and reasonable terms, may be daunting, but it is certainly worth the effort. Proposals for high-performance computer networks now under development should go a long way toward facilitating this goal.