
Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

10

Divider Title: _____

November 5, 1993

Ms. Terri A. Southwick
Attorney-Advisor
Office of Legislation and International Affairs
U.S. Patent and Trademark Office
Box 4
Washington, DC 20231

Dear Ms. Southwick:

This is to advise you that the National Association of Broadcasters would like to attend, and present oral testimony at, the hearing scheduled for November 18, 1993, concerning the development of proposals for protecting the copyrighted works disseminated through the National Information Infrastructure.

We propose to provide a two-part oral presentation. First, Dr. Richard Ducey, Senior Vice President, NAB Research and Information Group, will provide a synopsis of some of the challenges and opportunities broadcasters foresee will be provided by the advent of digital and compression technologies. I will then provide some of NAB's thoughts on the copyright issues relating to these developments. We anticipate our presentation will run approximately 20 minutes.

Attached is a summary of the points we plan to discuss in our testimony. We would like to reserve the right to file additional written comments on or before the December 10, 1993, deadline specified in the Notice of Hearing.

I will be out of the country until November 15, 1993. If, during my absence, you have any questions or concerns regarding NAB's testimony, please contact Jeff Baumann, NAB's Executive Vice President and General Counsel at (202) 429-5454.

Sincerely,

Benjamin F.P. Ivins

SUMMARY OF NAB's TESTIMONY
before
The Working Group on Intellectual Property
of The Information Policy Committee
of the National Information Infrastructure
Task Force
November 18, 1993

- I. Summary of the Testimony of Dr. Richard Ducey, NAB Senior Vice President, Research and Information Groups
 - A. The broadcasting industry operates under a policy model of universal service in the public interest, convenience and necessity which makes it distinct from other telecommunications and information media.
 - B. As part of the National Information Infrastructure, radio and television broadcast facilities serve essential public safety and emergency communication functions; and serve a broader social mission in informing and entertaining the public
 - C. Drawing upon advances in new technologies, radio and television broadcasters will be able to provide to the public not only their *traditional* package of universally available, commercially supported (i.e., free to the consumer) and wireless services, but also *new and advanced* services such as data communications, electronic mail, paging, signaling and telemetry services. Some of these services are already available through today's broadcast facilities.
 - D. To the extent the NII is truly *technology neutral* and therefore broadcasters are allowed to participate by using their technical facilities to offer innovative and improved services, these services would be offered *in addition* to traditional broadcast services.

II. Summary of the Testimony of Benjamin F.P. Ivins, NAB Assistant General Counsel

- A. NAB's members have a vital interest in the intellectual property ramifications surrounding the development of the National Information Infrastructure, both as prospective owners of information and entertainment products that will be disseminated through the Infrastructure pipeline, and as prospective users of such products. Accordingly, NAB anticipates playing an active role in the development of the legislative, legal, and regulatory environment to be created for the Infrastructure.
- B. The cornerstones of the American broadcasting system have been, and will continue to be, universal access, localism, and providing viewpoint diversity. These principles have served both broadcasting and the American public well through the years, and their preservation will be the basis upon which NAB develops its policies regarding the NII. To the extent the NII serves to advance these principles, NAB will lend support to its development. To the extent the NII appears to threaten these principles by, for example, creating a society divided into those who have the education and financial means to gain access to the NII, and those who do not, or by creating "info-monopolies" that can limit access and control viewpoint diversity, NAB will raise objections and concerns.
- C. Historically, significant changes in U.S. copyright law have resulted only through a process of negotiation, compromises, building a consensus where possible, and a balancing of interests among affected parties. There also has been a bias against such changes absent a significant showing of need by those proposing them. Finally, because copyright law has been viewed as a "seamless web" of compromises and interest balancing among many parties, revisions usually have been general and systematic, as opposed to piecemeal, to avoid upsetting the delicate balance of interests. The prime example of the application of these principles was the revision to the copyright law in 1976. While the advent of digital technology and the creation of the NII may well warrant changes in the copyright laws unparalleled since those made in 1976, and at a pace considerably more expedited than the 1976 revisions, NAB sees no need or justification for departing from the above-referenced time-tested approach to considering such revisions. We commend "The

National Information Infrastructure: Agenda for Action," for seeming to adopt this approach in recognizing the need simultaneously to consider the intellectual property concerns and interests of all parties that will be affected by the NII.

- D. While NAB recognizes that conversion to a digital world and implementation of the NII may require substantial revisions to intellectual property laws, we also see a danger in the attempt by some to use the specter of these futuristic developments to justify premature, overly-broad, and indiscriminate changes to such laws. There is nothing inherent in digital technology which necessarily demands an immediate radical departure from existing copyright principles. Rather, it is the way in which that technology might be deployed and ultimately used which may give rise to the need for changes in intellectual property law. Thus, for example, a broadcaster's conversion to a digital mode of transmission merely to enhance signal quality either over-the-air, or by wire, as part of a free ubiquitous service, would not, in and of itself, justify a change in current copyright law regarding performance rights in sound recordings, as applied to broadcasters. To the extent that digital technology or deployment of the NII facilitates unauthorized uses of a broadcaster's signal, such as copying of sound recordings or other portions of the signal for commercial gain, the remedies must be targeted at the unauthorized user.
- E. Broadcasters recognize that intellectual property principles which hold for traditional broadcast services (whether analog or digital in format) may differ from those that apply to *additional* services which can be offered through a more efficient use of spectrum by broadcasters.
- F. At this juncture NAB has no specific recommendations with respect to what, if any, statutory or regulatory changes might be required to accommodate the NII, or the licensing mechanisms that should be adopted in conjunction with its implementation. We would, however, offer the following general observations:
 - 1. Copyright owners should always retain the option of withholding any or all of their product from the NII, or any part thereof, especially if there are legitimate concerns that their unauthorized insertion into the NII would result in exploitation of their works by others for financial gain.

Broadcasters' experience with cable's use and exploitation of their signals leading to the adoption of retransmission consent underscores the need for this option. To the extent the NII anticipates the possibility of intercommunication, exchange, and the interoperability of different segments of the NII, mechanisms must be devised to create "firewalls" that preclude access to those segments of the NII that have not obtained authorization from a given copyright owner.

2. It would seem highly unlikely that any single licensing scheme could be devised that would cover all uses of all works available on the NII. From the copyright owners' standpoint, the decision to license at all and, if to license, what the terms, and conditions of that license would be, will depend at a minimum, on the intended use of the material by the licensee. As an example, the decision to allow a local school system or library to copy, store and subsequently perform a station's local newscast, and the terms of the license for permission to do so, might be considerably different from whether to allow an "infopreneur" to use the same newscast as part of a newly created derivative work which he or she intended to reinsert into the NII for profit. While it may be that, through time, standardized electronic licenses could be developed to cover certain uses by certain categories of users, the NII would always have to retain the flexibility to deal with the request for a nonstandard use by a unconventional user.
3. A major licensing problem that would exist with respect to the use of broadcasters' materials extracted from the NII is that such materials often consist of compilations and derivative works that include the copyrighted works of other parties. For example, a typical newscast may consist of copyrighted works of the station, the network with which it is affiliated, other stations, and other news organizations. While the station has obtained the rights from these other parties to use their materials as part of the newscast, the station probably is not in a position to convey any licenses to others to use these materials. Mechanisms will have to be developed to deal with identifying and obtaining the consent of the actual copyright owner in such situations, as well as with protecting the compilation interest of the broadcaster.

4. Perhaps the gravest copyright concern that broadcasters, and indeed probably most copyright owners, have with the NII is the ability to monitor and maintain control over secondary and tertiary uses of works disseminated through the NII. A major problem in this regard appears to be that once a user has obtained the right or ability to down-load a work in digitized form, there does not currently appear to be any reliable way to prevent them from making unauthorized uses of it by altering and/or reselling it or even of detecting that these activities are taking place.

- G. The "Notice of Hearing and Request for Public Comment on Intellectual Property Issues Involved In The National Information Infrastructure Initiative" notes that the commercial viability of the NII hinges, in part, upon "effectively promoting and encouraging use of the NII by all types of users." As providers of a ubiquitous service, broadcasters are in a unique position to educate the public about the NII and its potential benefits.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

11

Divider Title: _____

TESTIMONY OF JOHN MASTEN
EXECUTIVE VICE PRESIDENT, THE NEW YORK PUBLIC LIBRARY
BEFORE THE
WORKING GROUP ON INTELLECTUAL PROPERTY
OF THE NATIONAL INFRASTRUCTURE TASK FORCE

Mr. Chairman and members of the Working Group on Intellectual Property, thank you for the opportunity to testify on copyright and intellectual property issues and the National Information Infrastructure. I am John Masten, Executive Vice President of The New York Public Library. My comments today reflect the perspectives of this unique institution. The New York Public Library (NYPL) is a private, not-for-profit corporation with a public mission. Founded in 1895, it is a network of 86 libraries consisting of 4 world-renowned research centers and 82 branch circulating libraries in the neighborhoods of the Bronx, Manhattan, and Staten Island with 6 million users annually in The Branch Libraries and over 1 million in The Research Libraries.

Our Research Libraries, with holdings of more than 38 million items representing more than 3,000 languages, are the only comprehensive research facilities in the United States, other than the Library of Congress, that are freely accessible to the public. Through its current research centers: the Central Research Library at 42nd Street in Manhattan, the Library for the Performing Arts at Lincoln Center, the

Schomburg Center for Research in Black Culture in Harlem, and the Science, Industry and Business Library, to be housed in a new facility on Madison Avenue and 34th Street in 1995, NYPL provides unique collections and services supporting research in almost every discipline.

The founding of American public libraries arose from the same commitment to enlightenment, the broad dissemination of knowledge and the encouragement of learning and creativity that lies behind the concepts of copyright and patents. The U.S. Constitution gives the Congress the power "to promote the progress of science and the useful arts by securing for limited times to authors and inventors, the exclusive right to their *respective* writings and discoveries." This meant not only rewarding the creators, but also fostering and ensuring public access to their work. For example, the system of depository libraries for U.S. patents, of which The New York Public Library is one, is intended not only to inform the public which devices have the protection of patents, but to increase access to ideas and advances in technology and promote their development and contribution to the economic life of this country.

Public libraries and the free flow of information are, in fact, key contributors to creativity in America -- the creation of ideas and products. The New York Public Library has always embraced that role. The doors to our collections have been

open to all, regardless of the means or the affiliation of the user. Inside our doors countless great books and works of art have been researched. And in our reading rooms inventions from the Polaroid camera, Xerography to Soho Soda have been developed. In a more anonymous but equally important way, the small businesses that use our Science, Industry and Business Library daily find access to market information or technology updates that immediately benefit their operations and products. A letter from one of our users speaks clearly -

"Our success is directly related to the [Science, Industry and Business Library's] CD-ROM Center. It has given us the ability to find the right companies and their key personnel in an extremely efficient manner. And since our product increases the sales of our clients' products, the New York economy is helped two-fold."

The New York Public Library and other libraries have, in the past, been able to ensure public access simply by keeping their doors open. Access has meant on-site access to each institution's individual collections and, to a certain extent, through interlibrary loan, the collections of other institutions. In a predominately print environment, the "fair use" doctrine and other provisions of the copyright law pertaining specifically to certain copying exceptions for libraries have supported the public library's mission of open access to knowledge and information.

Now, like all libraries, The New York Public Library is coping with an avalanche of print material while planning for explosive growth in the digital, networked transmission of information. It is clear to all of us that in this new digital

environment, old concepts including "copying", "publication" and "distribution" lose their original meanings and must be reworked. But substantially revising a system of intellectual property rights opens up anew the critical question of balance. On the one hand, a system to manage intellectual property rights must foster creativity by helping to ensure that creativity will be rewarded. On the other hand, if property rights become too rigid, they can restrict public access to the ideas that spark creativity and growth. A system that does not accomplish both ends cannot "promote the progress of science and the useful arts."

I would like to make several suggestions about what is desirable in the revision of intellectual property law and practice, which are grounded in our experience at The New York Public Library. First, the fundamental public good of democratic access to information -- a foundation of our economic, political and cultural vigor -- must be at the center of that revision. It would be a terrible irony if, after having secured open access to the world of ideas through public libraries across America, this country could find no fair or reasonable way to secure that same access to information on the National Information Infrastructure. At The New York Public Library, much of the promise and public benefit of our expanded Science, Industry and Business Library that will open in 1995, will be at risk if the network cannot be used to extend off-site a wide range of our services and databases for small businesses and individuals.

Second, focusing directly on the importance of democratic access may be a better guide than trying to adapt the copyright concept of "fair use" to the networked environment. This is not to say that the doctrine of fair use has not played a critically important role in protecting the process of scholarship and learning through the nation's libraries. But the potential of network software to monitor and to record all uses of a proprietary database is very likely to lead, for example, to separate, individual contractual arrangements between owners and users that fall outside the copyright law entirely, and make an end run around the concept of fair use. And fair use, as free use, offers little practical guidance in those cases where network access is found to put potential markets for intellectual property at risk.

Third, as a single library, The New York Public Library has been able to secure for our users, on site, access to a wide variety of proprietary databases. The costs in site license fees are significant, but manageable. But the cost of compensating the owners of those databases, on the same basis, for opening them to access through a regional or national network would clearly be prohibitive for us as one institution. Unless some viable mechanism can be found --for example, the creation of a subsidy in aid of public access, or the building of a consortium of institutions to carry the cost -- it is precisely these proprietary databases, often in high demand because they are the most current and well-edited sources, that will not be

available via the network except to paying customers. Two classes of users would be created -- the information rich and the information poor. To put it in a more traditional context, it would be like saying that public libraries cannot offer free consultation of reference books unless they are out of date.

Finally, requiring or building into the network a single standard licensing system would be a mistake. It should certainly not be done just because it may be technically feasible. It is important to leave as much room as possible for individual owners of property rights on the one hand, and libraries or other users on the other, to negotiate arrangements that seem mutually beneficial. And it is important to recognize the wide variety of network environments in which these negotiations will occur, from statewide or regional networks to academic campuses, to low cost community networks or freenets. These environments are highly unlikely to share a single "best" solution. Moreover, experimentation is valuable. It can surprise us and teach us in which contexts there may be common interests uniting owners and users, or at least, where their interests are not opposed. A number of promising models for balancing the interest of creators with a concern for democratic access are, in fact, developing, including those which give differential treatment to the hierarchy of use from reviews of contents to transmission of full text. It would be a terrible waste of the ingenuity being

brought to bear on these issues across the country to impose a single government-approved form of licensing.

To return to where we began, adapting intellectual property rights to the network environment will continue to require a thoughtful balance in this new setting of two competing and familiar public policy concerns: rewarding the talent and effort that creates intellectual property and ensuring that it is accessible to all. Giving either concern short shrift will betray the promise of the NII and diminish the richness of the resources it can offer to all Americans.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

12

Divider Title: _____

InfoLogic

InfoLogic Software, Inc.

1223 Peoples Avenue
Suite 5405
Troy, NY 12180

TEL: (518) 276-4840
FAX: (518) 276-4841

November 2, 1993

Commissioner of Patents and Trademarks
U.S. Patent and Trademark Office
Box 4
Washington, DC 20231

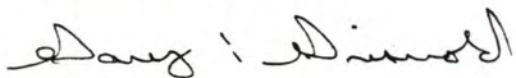
Dear Sir,

You have my respect and gratitude for the creation of a working group on intellectual property protection on the National Information Infrastructure. It is my pleasure and honor to present the attached report as written testimony before the working group for the November 18th meeting.

Technical solutions to this problem have been a primary concern of mine. The attached summarizes my thoughts and work to date. For your convenience, four copies have been included.

I will be in attendance at the meeting on the 18th, and am willing to give a verbal synopsis of this report, or answer any questions for the group.

Sincerely yours,



Gary N. Griswold

Methods of Copyright Protection for the National Information Infrastructure

Presented November 3rd, 1993
to the
Working Group on Intellectual Property
National Information Infrastructure Task Force
Patent and Trademark Office
Department of Commerce

Presented by

Gary N. Griswold
President

InfoLogic Software, Inc.
RPI Incubator Center
1223 Peoples Avenue
Troy, NY 12180

TEL: (518) 276-4840
FAX: (518) 276-4841

gary@infologic.com

Table of Contents

Motivation	3
Requirements	4
Publisher Concerns	4
Free Borrowing	4
Fair-use	5
Sharing	6
Alternatives	6
National Site License	6
Statistical Sampling	7
Advertising	8
No Protection	9
Centralized Control	10
Distributed Control	12
Proposal	14
Process	14
Benefits	16
Licensing Issues	16
Security Issues	17
Status	19
Recommendations	20

Motivation

Many celebrate the freer environment of electronic networks. The ease of data modification, copying, and multiple use usher in a relaxed attitude toward copyright. They believe that copyright holders must accept the less controlled environment of electronic networks. However, they are ignoring that these property rights are granted to authors and publishers in article 1, section 8, item 8 of the U.S. Constitution. The decision to place intellectual property on electronic networks is the prerogative of rights holders.

Because publishers do not share this relaxed vision of copyright, the current providers of electronic services are delivering information which does not require extraordinary protection, for example: open discussions, such as USENET; perishable information, such as news services; and government information, such as patent databases. However, any new system which wishes to leverage its content from the trillions of dollars in intellectual property already existing in the world, must address the property owner's concerns of property protection, or risk losing their cooperation.

Legally the problem must be solved. The HPCC Act of 1991 specifically requires that the NREN include a means to protect copyright.

(c) NETWORK CHARACTERISTICS.—The Network shall— ...

(5) be designed and operated so as to ensure the continued application of laws that provide network and information resources security measures, including those that protect copyright and other intellectual property rights, and those that control access to data bases and protect national security;

(6) have accounting mechanisms which allow users or groups of users to be charged for their usage of copyrighted materials available over the Network and, where appropriate and technically feasible, for their usage of the Network;¹

To date, no solution has been recognized. In his December 8th, 1992 presentation to Congress on the NREN, Dr. Allan Bromley, Director of the Office of Science and Technology Policy, had the following to say about the current status of copyright protection:

¹ High Performance Computing Act of 1991; Section 15 USC 55112 (c).

The technical mechanism appropriate to protect copyright of material distributed over the network is as yet unclear. ... Because consensus has not been reached in this complex area, implementation of technical measures on the Network has not yet been scheduled. ²

Requirements

Publisher Concerns

Mr. Timothy King, Vice President of Corporate Development at John Wiley and Sons has identified the following key concerns of publishers. They seek resolution of these questions before making their works available for network distribution.

Will the integrity of information be preserved? ... Will attribution for all information be ensured? ... Will the quality of the content and form of information be maintained? ... Will creators and copyright holders be able to control the use of their work and to receive compensation for that use? ... What mechanisms will be incorporated for the tracking of and payment for the use of information? ... What pricing models for the use of information will evolve? ... How easy and widespread will access be? ... Will there be long-term safeguards to ensure fair access to and use of the network by all? ... Who will pay for the network and the information provided on it? ³

Free Borrowing

Two hundred years ago, Benjamin Franklin established the first free borrowing library. His invention fostered a superior educational system in the United States, which produced a superior civilization. However, the digital world may be a threat to the free borrowing library. To date electronic information has been delivered on a fee, not free basis. Traditional libraries have begun providing their patrons access to electronic services.

² Dr. Bromley, Director of the Office of Science and Technology Policy; "The National Research and Education Network Program: A Report to Congress"; December 1992; Page 20.

³ Tim King; "Critical Issues for Providers of Network Accessible Information"; *EDUCOM*; Summer 1991; Page 82.

Since the libraries are unable to budget or control the use of these services, they have typically passed the costs along to patrons using the services.

If the electronic age eliminates free borrowing, then it may be a step backwards for democracy. Electronic or not, quality education is the highway of the American dream. A dream which has become faint for the inner city poor who find a quality education out of reach. Providing electronic highways to some, will only worsen these problems. We should not ignore truths that our ancestors held as self evident, but honor the equality of men as if our democracy depended upon it.

The free library contains purchased information which is later borrowed by others at no cost. Each borrower uses the information for a limited period of time. While an item is borrowed, it is not available for use by others. These procedures can be applied to an electronic free library. The key technical problem is to discontinue access to information after the borrowing period has expired. This must be done even though the information resides on the customer's computer outside the direct control of the electronic library.

Fair-use

Copyright law clearly allows 'fair-use' copying of information for scholarly and educational purposes. Although, current practices in the paper world offer little control to insure that all photocopying is 'fair-use'. Publishers and libraries are strongly divided over the meaning of 'fair-use'. Publishers seek a narrow definition to maximize their revenue, and libraries a liberal view in order to maximize their freedom of action. It is beyond the ability of this paper's author to suggest a resolution to this controversy, except to point out two key facts.

First, there must be a means for 'fair-use' copying to occur in the electronic environment. To satisfy the concerns of rightsholders there must be a clear way to differentiate between a document under copyright control and a fair-use copy of the same document. Second, when people perform fair-use photocopying today, they usually spend 10¢ per page. When electronic information becomes available for less than 10¢, the fair-use controversy will be over. Publisher's will be able to receive royalties due, while customers use more affordable forms of information. Low cost and high use digital information is a win-win objective.

Sharing

In paper publishing, it is the first sale of a copy that generates income for the publisher. Subsequent sales of the copy occur without royalty. In the electronic world, this part of copyright law is problematic because it is not possible to differentiate between a copy and a subsequent use of a previous copy. Each time information is moved from disk to memory, from memory to network, or memory to screen, a copy has been created. Does this mean that each of these is a new copy which requires remuneration to the rightsholders? Such a view could result in 'windfall' profit to publishers.

It may not be possible to move the 'first-sale' doctrine into the electronic world unchanged. Yet, how do we preserve its beneficial aspects? In paper media, people can freely share information without violating copyright. We should be able to share information in the electronic world as well. For example, a university may have a site license for a group of journals. Faculty and students need to be able to share information among themselves that they own in common. At the same time, it is necessary to prevent people who do not participate in the license from sharing the same information. In another case, there may be one copy of an article which people pass among themselves. That is, there must be a way for Alice to give a copy to Bob so that Alice no longer has a copy. Lastly, there must be a way for an owner of information to transfer their ownership without retaining the information.

The technical proposal in the later portions of this report addresses all of the requirements mentioned on these preceding pages.

Alternatives**National Site License**

Some have been trying to establish national site licenses for electronic journals. In this model, the publisher works backwards from an expected revenue and encourages each university library to pay their fair share in exchange for unrestricted distribution within the university. This approach may work well for the licensing of well established scholarly journals. However, our economy is a market system in which changes in customer demand result in the growth of new products and the decline of others. This occurs efficiently without central planning or egalitarian control. The

key problem to be solved for national licensing is: how will decisions be made about the introduction of new products and the reduction of ones no longer in demand?

Additionally, it may be tempting for the publishers holding national site licenses to ignore their 'cash cow' which brings in a consistent return each year, and turn their creative and marketing attentions to other avenues which offer them opportunities for growth in market size and marketshare. Also, national site licenses are apt to be not fully national; not every potential customer will participate. For example, a national site license plan involving university libraries, will not provide information to those who do not have access to those libraries. Hence, it will not provide universal access to information. Consequently, while the national site license approach may work for some kinds of information, it is clearly not the correct solution for all kinds of information.

Statistical Sampling

Statistical sampling can be used as a way to collect information on the use of copyrighted information. Sample measurement can then be used to charge customers and reimburse publishers. In the music industry, BMI monitors radio broadcasts and record sales. From this it projects the fractional percentage that each song is played. It then collects revenues from businesses which play recorded music publicly, giving them the right of public performance in exchange. The monies received are divided up among rightsholders according to the fractional percentage each song was played on the radio and in record sales. Some countries, such as Sweden, have a photocopy tax which is imposed on all persons and businesses in exchange for a right to photocopy. The monies collected by the government are paid to rightsholders.

Statistical sampling is feasible in the National Information Infrastructure. For example, information down-loaded from a server to a customer could be measured on a sample basis. The results could be extrapolated to proxy for all electronic information use. The monies received could be divided up among rightsholders according to the results of the sample. However, the more difficult question is how is revenue to be assessed and collected? The network could assess a fee from each network customer that would cover their information usage expense. This fee could be proportional to the time they spent accessing information on the network. In order for this to be fair to rightsholders, the measurement of network access by users

would have to be very inclusive and not permit the establishment of subnets which are outside the control of the measurement system. Otherwise, a simple work-around would be to down-load expensive information to private networks and use it extensively without additional cost.

An alternative which would eliminate this restriction would be to require that all users be charged an equal fee for unlimited information access. This could be imposed as a tax whose proceeds would be distributed to rightsholders. Using this alternative, the NII would become a heavily used information highway. A couple of hundred years ago a bridge builder considered how to pay for his bridge. He could charge a large fee and only a few would use it. Or he could charge a small fee and many more would use it. Since the bridge was not quickly worn down by use, the second seemed the better choice. Lastly, he could charge a tax on the bridge to everyone who lived nearby. This choice resulted in the greatest use of the bridge.

In addition to the political problem of assessing information taxes on the use of the network, this alternative also has problems with product pricing. In the music industry, the price of performance of most music is standardized. This makes it possible to divide up the revenue by usage. However, in the print industry, there is a tremendous variation in product pricing. This permits high quality and low quality products to co-exist. It also allows low demand products to exist by charging higher prices for those products. For the print word to move to this kind of statistical sampling, publishers would have to come to an agreement on standardized pricing. This may be possible for some kinds of information, but will not work for all kinds.

Advertising

Television has demonstrated that it is possible to fund the production of very expensive works, and deliver them free to the consumer by selling advertising space. Similar methods can be applied to the National Information Infrastructure. However, the downside is clearly the low quality exemplified by television production. Television has a greater capacity to educate than any prior media, but has not, largely because the economics of selling advertising is in control of content. Yet, considering the interactive television agenda of some large companies, if no other means to reimburse rightholder's appears, advertising might fill the void.

No Protection

In the early 1980's, the personal computer software industry used a variety of methods of copyright protection on diskettes they sold. These methods were inconvenient to customers who were unable to make backup copies of purchased software, or were required to insert diskettes into their drive at each use. Later, when market studies indicated that customers purchased much more unprotected than protected software, most software companies eliminated their protection schemes. Some have suggested that these same issues apply to information delivered on the National Information Infrastructure. However, such generalizations do not properly take into account the tremendous differences between software and other forms of information. Software piracy is the exchange of diskettes. This is more convenient and less expensive than piracy by photocopy. It is still cumbersome and expensive compared to the potential for piracy on a high-speed network. The lax controls that work in an environment of manual exchange of diskettes may have very little bearing upon the kinds of protection needed when piracy can occur at Gigabit speeds at the push of a button.

Software is difficult to evaluate for purchase, and more expensive in time to learn than its purchase price. Its complexity has created a need for local 'guru's who are able to advise others on the best software to purchase, and help customers learn how to use it. In order for such 'guru's to have experience in a wide variety of software it is usually necessary for them to be software pirates. In fact, a study of the personal computer software industry concluded that piracy played an essential role in the distribution of information about software products. Placing locks on software only meant the pirate might not have the software, thereby slowing down the free exchange of information about the software.

...piracy increases the total number of program users, since some who pirate would not buy, were protection strengthened. This increase in the user base becomes important when there exists a positive consumption or network externality which exists if consumer utility for a product increases with the number of other persons using it. ...the network externality will be strong under three conditions: if the program (1) is complicated and difficult to master, (2) allows or demands extensive user customization, via 'macro' programs or other means, or (3) is useful for multiple user data processing or

formal networking.⁴

To benefit from any written article we need only to read at the level it was written. To benefit from audio and video information even less skill is required. Clearly the complexity characteristics that make this 'network externality' so important for software do not exist for text, audio, and video information. However, some aspects of the software model may translate well. The software industry has been able to capture customers and make very good revenue by selling updates to customers on products they already own. It may be that information which needs to be updated frequently will benefit from the same model. News, for example, is very perishable. Very little protection may be required against downstream reuse of this kind of information. Instead, one must simply insure that only paid customers receive it in the first instance.

Centralized Control

On-line information services sell access to information in mainframe computers and control access to information with the user authorization and accounting capabilities of those computers. They do not control access to information after it has been distributed, instead they meter the customer's use of their facility and charge accordingly. Customers are able to download information to their own computers, alter it, pass it on, or both. The centralized system can charge for the time it takes the customer to locate the information they desire, and it can charge for the delivery of the information, but it does not monitor or charge for events off its own site.

Some believe that a similar approach will work on the National Information Infrastructure. However, this conclusion ignores the ease with which customers can make subsequent electronic copies on a high speed communications network. Current on-line services are not usually accessed over a network. They are accessed by point-to-point dial-up communications between the customer and the on-line database. These communications are very slow typically .0024 to .0096 Million bits per second (i.e. 2400 to 9600 baud). At these slow rates it takes minutes to receive information that would transmit in a fraction of a second on the National Information Infrastructure. For example, at 10 Million bits per second a 1 Million bit file could be transferred in close to 1/12th of a second. At 2400 baud

⁴ Kathleen R. Conner and Richard P. Rumelt, "Software Piracy: An Analysis of Protection Strategies", *Management Science*, Vol 37, No. 2, February 1991, Pages 125 to 139.

the same file would require 8 minutes. While the potential for piracy exists in both dialup and high speed networks, the awkwardness of piracy on dialups does not resemble the ease of piracy on high speed networks.

Networks control the delivery of information to a customer by address. Piracy could simply be forwarding received information to others by invoking an information delivery service, such as electronic mail or file transfer, and giving it the addresses of the recipients. In the current point-to-point dial-up on-line access, the pirate normally does not have similar facilities. Instead, piracy can be performed by placing the information on a diskette and exchanging it manually, or compiling information into another on-line service and providing a service to others, or moving the information to a network which includes an electronic mail service. None of these are nearly as convenient as the means of information sharing which could exist in the NII.

One of the objectives of the NII is to provide freer access to information to more people. In this regard the current on-line services are a poor model to emulate. They often charge \$50 to \$100/hour for accessing their services, with additional charges for the delivery of information. The market for these expensive services is information to support business and government decision making. Used for these purposes, such costs are often a bargain when compared to the alternative of making decisions without the information.

However, such expensive services have very little in common with the objectives of the National Information Infrastructure. Electronic information should be less expensive than its paper cousin. Electronic information does not need to be printed; only one copy needs be warehoused at any location and there are no returns. On the other hand, the on-line services fill their expensive computers full of desired information and charge for the use of their computers. They have replaced the savings of eliminated paper with the larger cost of computer usage. The benefit to the customer is speed of access, not cost of information.

In order to develop a national system of inexpensive information, we need to deliver the information with a minimal use of large, expensive computers and maximize the use of small, inexpensive computers that exist in most offices and homes and will soon exist in television sets. To do this, the information must be stored in distributed servers and delivered for use to customer's own machines. Only bibliographic services for

locating information should be centralized. By doing this and making maximum use of smaller computers, the costs of information can be kept to a minimum. In order to do this, we need a distributed means of information control.

Yet, centralized control will work for some applications. Some applications involve the delivery of so much information that the cost of capturing, storing, and forwarding the information is too expensive for pirates. For example, the regional Bells and others are planning the delivery of movies upon request. Even though a Megabit network would be fast enough to deliver such information, storage devices of sufficient size to capture an entire movie would be too expensive for consumers in the near future. Hence, those working on this technology are building cable interfaces which will store about 5 minutes of a movie at a time; the entire movie is to be transmitted from a central server to the customer, a few minutes at a time. Since any video pirate can rent a movie for \$2 and make a copy on a VCR in 2 hours, no one is likely to go to the expense of building an interface that would capture movies. However, the delivery of journals, journal articles, and books over the NII poses an entirely different problem. These forms of information are sufficiently small that they should be electronically delivered to reside on the machine of the customer. Once this is done, centralized control will not suffice, distributed control is needed.

Distributed Control

Digital signature use of public key encryption has been suggested as a means to protect copyright. A hashing algorithm is used to create a unique number from the content of a document. This number is encrypted with the private key of the originator. The receiver of such a document can obtain the public key of the assumed source of the document from a central key facility.⁵ While this important technology verifies the source and content of the document, it does nothing to prevent the creation or use of copies.

Public key encryption has also been suggested as a way to encrypt information. By using the public key of the receiver, only the receiver can decrypt it with their private key.⁵ While mathematically very secure, nothing prevents people from distributing encrypted information along with

⁵ Public-Key Cryptography Standards; RSA Data Security, Inc; June 1991.

their private keys. The elegant security of public key encryption prevents anyone from identifying the source of the offending private key and copyright infringement.

John H. Ryder and Susanna Smith describe a simple solution for the electronic dissemination of software. Before the customer receives the copyrighted software product in working form, the customer is presented with a number of screens of text which display a license agreement. The customer must follow certain steps on the keyboard to signify that they agree to the terms of the license agreement.⁶ However, while this method makes certain the customer understands their licensing rights, this method does nothing to insure that the customer lives up to those obligations.

Martin E. Hellman describes a means to limit access and bill usage of software, video games, video disks, and videotapes. This is accomplished via an encrypted authorization code, which contains information related to an identification of the computer, a product, a number of uses requested, and a random or non-repeating number. When entered into the customer's base unit, the authorization code permits use of the specified software product for the specified time.⁷ Victor H. Shear describes a system and method to usage meter distributed databases, such as CDROM. This method describes a hardware module which must be part of the computer used to access the distributed database. This module retains records of the intellectual property viewed. Once the module becomes full, it must be removed and delivered to someone who will charge for the usage and set the module back to zero usage.⁸ Both Hellman's and Shear's method requires a hardware module, which must be constructed into the customer's computer, in order to be able to control access. These methods will not be usable until there are a very large number of computers containing these modules. Hardware manufacturers will be hesitant to include these modules in the design of their computers until there is sufficient demand for these specific systems. Software implementations of these methods would not be secure, because a hacker could easily modify stored usage information.

⁶ John H. Ryder and Susanna R. Smith; "Self-verifying Receipt and Acceptance System for Electronically Delivered Data Objects"; *United States Patent 4,953,209*; August 28, 1990.

⁷ Martin E. Hellman; "Software Distribution System"; *United States Patent No. 4,658,093*; April 14, 1987.

⁸ Victor H. Shear; "Database Usage Metering and Protection System and Method"; *United States Patent 4,977,594*; December 11, 1990.

One approach suggested by Richard Linn of NIST, involves a system of cryptography methods to lock information in an envelope which cannot be opened by anyone except the person to whom it is licensed.⁹ In this solution, each protected document is encrypted and includes a data envelope which contains the identity and approved usage of the licensee. Using this information, software capable of unlocking the document first checks the license parameters before opening. If designed to adequately hide keys, this method would be reasonably secure and workable. However, it would be unable to license information for a period of time because users can so easily change their computer's clock. This would make it unusable for a free borrowing library. It could not be used to share information, because each information product is licensed to a user. The method could be enhanced to work for a group of users at a site, but it provides no way to share or transfer ownership.

Proposal

The solution presented is a distributed control software method, which uses the network to control access to information. A patent application has been filed on the pivotal aspects of this innovation.

Process

The approach is as follows: copyrighted information is transmitted in an encrypted form, and is transmitted in a software "envelope". The copyrighted information and the software envelope together comprise an executable program which is capable of decrypting the copyrighted information and presenting it to the user. The capabilities of the envelope intentionally limit the user's access to the copyrighted information to those capabilities which are appropriate under copyright law for the specific kind of copyrighted information contained. For database information, the software envelope should enable the user to search indexes and display text. For CAD information, the software envelope should permit the display of the information and permit the user to manipulate attributes of the display. For video information, the software envelope should display the video. For audio information, the software envelope should play the audio information. For text, the software envelope should display and turn pages. For hypertext

⁹ Richard J. Linn, "Copyright and Information Services in the Context of the NREN", Proceedings of the Joint Harvard MIT Workshop for Protecting Intellectual Property in the Networked Multimedia Environment", April 2, 1993.

information, the software envelope should allow the user to thread through the information. The above, mentions only some of the ways these software envelopes can control different kinds of copyrighted information. This list is hardly exhaustive.

Finally, the software envelope uses a method, to check for authorization to access, and to track the usage of the software envelope and copyrighted information over the same telecommunication network used to transmit them to the user. The tracking method works as follows: automatic messages are sent between the software envelope and a central authorizing site. Each time a customer starts to use a copyrighted work, a message is automatically sent from the work. Also, at a regular interval, additional messages are sent. By being sent at regular intervals, they are a measure of use. When the messages arrive at the central authorizing server they are verified. A reply is sent back, which is an authorization to continue or a denial of authorization. If no valid message returns, a denial is assumed by the software envelope. Whenever a denial is received or assumed, the use of the software or copyrighted information product is discontinued. The diagram in Figure 1 illustrates this method of tracking copyrighted information.

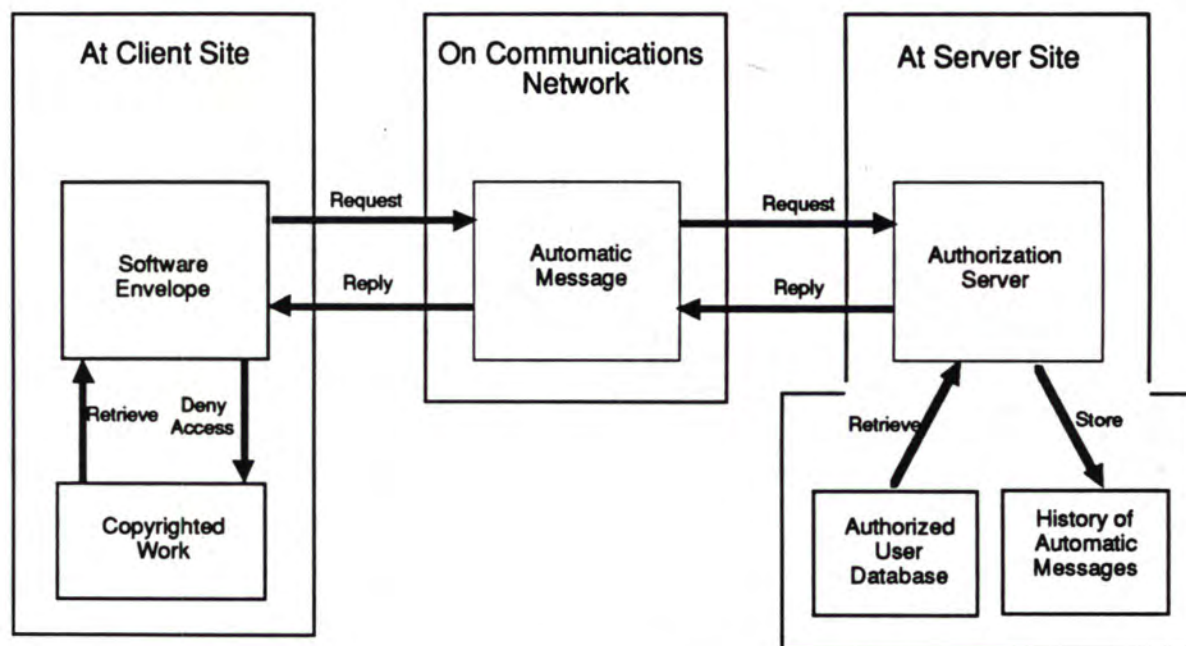


Figure 1 - Overview of Copyright Tracking Mechanism

Benefits

The authorization and usage measurement capabilities described above can be used to license information products in a variety of ways to suit a variety of information licensing policies. It can be used to enforce site licenses by preventing access off-site and limiting the number of concurrent uses. It can be used to limit duration of use, analogous to the returning of a book to a library, by disabling use of an information product after a period of time. It can be used to implement an electronic subscription by providing an unending duration of use of the product on one machine. It can also be used to meter and charge for each use of the information.

The software envelope would provide the user with the ability to view the information product, but it would not provide a way to edit or extract from it. This is needed, so that the displayed information is not used as a source from which to create a new copy, which is not subject to this copyright protection scheme. Second, it would insure the authenticity of the information products, by preventing the automatic creation of altered copies. Third, it would interfere with plagiarism, which has become an increasing problem because of the abundance of easily copyable electronic information. Fourth, it would prevent the automated generation of derivative works.

Licensing Issues

So far, we have only discussed controlling licenses for viewing information, but the same method can be used to control licensed printing. While the rightsholder may choose to give the customer a license to view and to print, they could require an additional expense for the action of printing. In this case, the authorization request would indicate that printing is requested and the reply would indicate whether the customer is licensed. The act of printing would be recorded for the purpose of charging. This system permits unlimited copying on the network, and yet limits the use of those copies to licensed customers. However, a customer may need to take an electronic copy of a document onto a machine which is not connected to the network. For machines which contain internally readable serial numbers or private keys in firmware, we can license and control the act of making copies. Each copy made will contain the internal identifiers of the machine on which it is to run. It will still be encrypted, and requires a similar software envelope for presentation. Instead of

checking for further authorization over the network, the software envelope checks that it is running on the machine to which it is licensed.

Security Issues

If protected information is decrypted into ASCII form, it is trivial to capture the unprotected text into a file while it is displayed or printed. (Not that ASCII was ever a desired form for published text. Publisher's wish to insure the quality of their presentation; that is not possible with ASCII files.) To thwart this simple attack and control the quality of output, it is necessary to generate bit-map output when decrypting information. It is still possible for the user to capture the display, but capture of a bit-map is more cumbersome. For example, only a few pages of such copies will fit on a diskette. This kind of copying should be possible to allow for the fair-use of protected information. Publisher's will have the assurance that copies created in this manner are immediately recognizable as copies.

If usage measurements are accumulated in software on the customer's machine, a hacker can easily find them by doing a bit-wise comparison of the software and datafiles at two distinct points of time. Once the storage location is found, it can be easily reset to zero by restoring the current to the initial state. To address this problem, the method presented stores usage information at a central trusted site, where a hacker will have great difficulty in viewing or altering the information. To be sure, the authorization site will be a target of hacker attacks, and B1 security procedures should be used to protect it. For similar reasons, the local clock of the customer's computer cannot be used to measure time. A clock at a trusted central location must be used.

Since authorization is communicated by datagrams from a central server to the client, creating false datagrams, or capturing and replaying datagrams are methods of attack. Both of these can be made ineffective by encrypting the datagrams, and storing in them information that can be used to verify their authenticity when received. Additionally, a hacker may seek to obtain authorization by changing their machine's address to that of a valid licensee. This kind of attack can be made unreliable by always using connectionless protocols when sending datagrams between client and authorization server. In this way, the approval authorization will be sent to the machine which legitimately owns the address, rather than the counterfeit which has just assumed to address.

Key handling is a central problem in the design of a distributed means of control. As already discussed, the standard use of public key encryption will not work, because the recipient is able to share their private key along with the decrypted information. This may lead some to suggest that the private key must be hidden in the software used to present the information. However, this solution is open to easy attack by a hacker who could find the hidden key by doing a bit-wise comparison of two copies of the same program. Even if the key is further obscured by hiding pieces in a variety of locations, the comparison would give the hacker a head-start on breaking the encryption. Not that having keys specific to each individual was ever a good idea; it interferes with the free sharing of information among valid licensees. Instead of using keys specific to each individual, keys specific to each document should be hidden within the documents. Since, each copy of a document would be identical, there is no way to locate the key by a bit-wise comparison of documents.

The actual key used for decryption should not be stored in its entirety, but generated from pieces hidden in the document. Not that it is impossible for a hacker to find the hidden key pieces or key generation logic. They could be located by reverse engineering the software used to display the information. An effort of this magnitude would be too time consuming for the average hacker. However, a commercially opportunistic hacker might decide to develop software which does not perform an authorization check before decryption. Such a program would be the economic equivalent of a cable unscrambler. To thwart this hacker, it will be necessary to constantly change the methods of decryption and key hiding used by the system. In this way, any hacker's successful reverse engineering project will only decrypt some documents, and the percentage of the total that it decrypts will decline as time passes. This will make selling unauthorized decryption programs financially unrewarding.

Many in the security field contend that methods of encryption should be documented and standardized; only keys should change. This belief leads the same people to conclude that hardware is more secure than software, because software solutions are open to reverse engineering attack by monitoring the instructions on the computer's 'bus'. I contend that these opinions ignore some important facts. Prior to World War II, encryption was performed on machines in which the key was set through switches and dials. When one of these machines was captured, an enemy with no cryptologic insight could simply try all combinations of the dials and switches until they deciphered a document. In the U.S., John Von Neuman decided

to put an end to this kind of attack by developing a machine which processed instructions and used the instructions to decipher and encipher information. Since, there were an infinite number of ways to combine these instructions, a machine captured by the enemy would not help them decipher messages. What John Von Neuman had invented was the distinction between software and hardware. Software which performs the task and hardware which processes the software. It is enlightening to recognize that he invented software for the purpose of making U.S. cryptology more secure. The key characteristic of software which makes it secure, is the ease of its revision.

Status

At this time, I have a demonstration version of the technology running on the Internet. The system includes a centralized database of information about rightsholder's, protected documents, customers, and licenses. There is a program for creating protected documents from ASCII, and registering them and their rightsholders in the centralized database. There is a 'software envelope' for checking the database for access authorization and presenting a protected document whenever authorization has been approved. The database and server portions reside on a SUN Sparcstation connected to the Internet in Albany, NY. The client programs have been demonstrated to work from machines connected to the Internet in Boston and Ann Arbor. This prototype lacks the user interface quality one would expect in a commercial product, and at present only runs on SUN Sparcstations. The prototype has a single server, but a production system will need to consist of multiple redundant servers. The Customer billing and publisher payment modules have not yet been written.

The next step will be to develop a full feature prototype, and implement it in pilot projects with a server of published information. We will be able to proceed with this step, when funding is available. This pilot system should limit the number of products and the number of customers in order to facilitate revision of the system as we learn from its use. However, this system should provide the full scope of functionality required in a commercial version. That is, it should manage licenses for viewing, printing and node locked copying, it should maintain a full database about its customers and publishers. The database should be used to bill customers and pay publishers. The system should provide a higher quality presentation program which is available on a wide variety of platforms. Finally, the license server must be redundantly deployed to guarantee 100% uptime.

Recommendations

In my opinion, the selection of any one method is premature at this time. Electronic copyright protection suffers from controversy and strongly held diverse opinions. Unfortunately precious little has yet been done to test any of these methods in the marketplace. What is needed at this time is pilot projects to test out some of these methods. My personal recommendations for further study include: national site licensing, statistical sampling, data envelopes, and software envelopes.

Despite the urgent need for a solution to this problem, I am not aware of any government funded research to help solve it. In the HPCC recommendations published by the Office of Science and Technology Policy, the National Library of Medicine was given responsibility for funding HPCC research in bibliographic information retrieval. Yet, I have been able to verify that no work in copyright protection has been funded there. In the HR 1757 National Information Infrastructure Act, the National Science Foundation was assigned funding responsibility for general issues including copyright protection. Even though the 1991 HPCC Act contained provision that the NREN shall have a means to protect copyright, a search of the NSF grants database turned up no research on this problem. The HR 1757 NII Act also assigns funding to NASA for work on Digital Libraries. Yet, NASA considers all of the information they produce as public domain, and not requiring copyright protection. Considering their policy of only funding research they expect to use, it seems unlikely they will fund work in copyright protection.

I respectfully suggest that everyone recognize the uniqueness of this problem and place the research funding responsibility under the Department of Commerce.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

13

Divider Title: _____

Corporation
for
National
Research
Initiatives

November 8, 1993



Research
and
Development
for
the
National
Information
Infrastructure

The Honorable Bruce A. Lehman
Commissioner of Patents & Trademarks
U.S. Patent & Trademark Office
Box 4
Washington, D.C. 20231

Dear Mr. Lehman:

I am submitting the attached document entitled "Deposit, Registration and Recordation in an Electronic Copyright Management System" as written comments that are related to testimony I am prepared to give at the hearing on November 18. In particular, I plan to focus my remarks on the following key points.

1. The system described in the written comments is applicable to electronic copyright management in a network environment; however, it may also be appropriate for many other purposes including, but not limited to, management of confidential or proprietary information not subject to copyright, negotiation of licensing arrangements and royalty payments.
2. A pilot project is being carried out by the Corporation for National Research Initiatives to test and evaluate these concepts in conjunction with several universities and the U.S. Government.
3. I view the NII as a set of common-user networks providing shared access facilities to a multiplicity of information resources. There is presently no system for electronic dissemination of protected works in the NII with any realistic measure of security (other than encryption) for people to plan for commercial transactions which require it. This limitation is particularly important for computer applications where access by programs to unencrypted data will be essential.

Suite 100
1895 Preston White Drive
Reston, VA 22091-5434

Tel: (703) 620-8990
Fax: (703) 620-0813
Internet: info@nri.reston.va.us

The Honorable Bruce A. Lehman
November 8, 1993
Page 2

4. The computer network environment will involve the use of computer programs of many different types into which may be incorporated other copyright works. The resulting computer programs may themselves be works protected by copyright. Protection of rights in these programs, beyond merely the right to reproduce, will be important. An example is the right to execute or otherwise perform the programs.
5. A number of technical areas are being explored and/or developed to deal with unauthorized access such as privacy enhanced mail based on digital signatures and public key encryption. Such techniques are sufficient to deal with unauthorized interception of communications, but do not address issues of further communication of computer program outputs or other digital information. In my view, it is too early to mandate controls at this point. Experience gained from early pilot projects, such as the one described in the written comments, will be helpful in providing guidance in the future.
6. Finally, in addition to the pilot projects, there is a considerable amount of work in the various standards bodies on standards for information exchange and software interoperability. What is yet unclear is the extent to which these efforts will adequately address the needs of copyright owners and other intellectual property rightsholders. This area requires considerable study and coordination to determine what additional standards, if any, may be required.

I would appreciate the opportunity to testify before your working group on these matters.

Sincerely,



Robert E. Kahn
President

Comments of Dr. Robert E. Kahn
President, Corporation for National Research Initiatives

NII Task Force - Information Policy Committee
Working Group on Intellectual Property

Washington, D.C.
18 November 1993

DEPOSIT, REGISTRATION AND RECORDATION
IN AN ELECTRONIC COPYRIGHT MANAGEMENT SYSTEM

by

Robert E. Kahn

Corporation for National Research Initiatives
Reston, Virginia

August 1992

Summary

This document proposes the development of a testbed for deposit, registration and recordation of copyright material in a computer network environment. The testbed will involve the Library of Congress and provide for electronic deposit of information in any of several standard formats, automated submission of claims to copyright, notification of registration and support for on-line clearance of rights in an interactive network. "Digital signatures" and "privacy enhanced mail" will be used for registration and transfer of exclusive rights and other copyright related documents. Electronic mail will be used for licensing of non-exclusive rights with or without recordation. Verification and authentication of deposits can be carried out within the testbed using the original digital signatures. A system of distributed redundant "Repositories" is assumed to hold user deposits of electronic information. The testbed provides an experimental platform for concept development and evaluation, a working prototype for system implementation and a basis for subsequent deployment, if desired.

1.0 Introduction and Background

Deposit, registration and recordation of copyright material and its associated claims to rights have generally been handled manually. Over the past two decades, the economics of information technology has enabled an electronic foundation for such material and claims. The key elements of this foundation are the personal computers, workstations, computer networks and peripheral devices such as scanners, printers and digital storage systems which have now become sufficiently powerful and cost effective to be put into widespread use. It is now essential that the underlying systems used to manage copyright be conformed to be compatible with the promise of this new computer networking environment. This paper addresses several essential steps that should now be taken to facilitate that process.

In the current manual system, claims to copyright are registered with the Copyright Office, Library of Congress. Deposits are accepted and stored in physical form including tapes and diskettes as well as paper and other substances. Notification of registration is also made in physical form. In addition, documents transferring copyright ownership and other documents pertaining to copyright may be submitted to the Copyright Office for recordation. While an on-line record of recent registrations and recordations may be accessed at the Copyright Office, there is only limited external dissemination of this information in

electronic form for access at remote sites.

This approach requires considerable physical storage at the Library of Congress for deposited materials which can only increase over time. Materials stored in physical form will slowly degrade unless deposited in digital media in which case the contents may be reproduced subsequently without loss of information but at some cost for duplication. Even if it is available digitally, much, if not most, of this material will not generally be accessible on-line from any source. Rights to use the information in a computer network environment cannot usually be acquired easily or quickly, even if the identity of the rightsholder is accurately known. Fortunately, these limitations can also be overcome with the use of information technology and only minor modification to the current manual system.

2.0 Components of the Proposed System

This document proposes building a testbed to develop and evaluate key elements of an electronic copyright management system. These elements include:

- a. Automated copyright registration and recordation
- b. Automated transactional framework for on-line clearance of rights
- c. Privacy enhanced mail and digital signatures to facilitate

on-line transactions

d. Methodology for deposit, registration, recordation and clearance

Current registration and recordation activities of the Library of Congress would be maintained and enhanced in the proposed testbed. It provides for repositories and recordation systems both within and without the Library of Congress, which would serve as agents for authors and other copyright owners which seek to register works with the library. In addition, the testbed provides for automated rights clearance, outside of but linked to the library, which would accelerate permissions and royalty transfers between users and rightsholders.

2.1 Electronic Copyright Management Testbed

A testbed is proposed to develop and evaluate these concepts and to obtain experience in the implementation and operation of an experimental system (see Figure 1). The proposed testbed consists of a Registration and Recording System (RRS), a Digital Library System (DLS) and a Rights Management System (RMS). The RRS will be operated by the Library of Congress and will permit automated registration of claims to copyright and recordation of transfer of ownership and other copyright related documents. The RRS would also provide evidence of "chain of title." The DLS will be a distributed system involving authors, publishers, database

providers, users, and numerous organizations both public and private. It will be a repository of network accessible digital information and contain a powerful network based method of deposit, search and retrieval. The RMS will be an interactive distributed system that grants certain rights on-line and permits the selective use of copyright material on the network.

Information may be stored in the DLS, located within the DLS and retrieved from the DLS using any of several mechanisms such as file transfer, electronic mail or agents such as Knowbot programs. Material may be imported into the DLS from other independent systems, from paper and other sources or exported from the DLS to other independent systems, to paper or to other materials such as CD-ROM, DAT, and microcassettes. The electronic copyright management system described in this document would be directly linked to the DLS.

The testbed would contain a digital storage system connected to an applications gateway (which is, in turn, connected to multiple communication systems including the Internet) to which documents would be submitted. The storage system would constitute an experimental repository for information. The applications gateway would be designed to support multiple access methods including direct login. The RRS and RMS would be servers connected to the Internet. Initially, they would be on a common machine, but they could later be easily separated. After development, the RRS would

be relocated to the Library of Congress or its designated agent prior to being placed in operation. After initial implementation, the repository and the RMS would be replicable at other sites.

2.2 Electronic Bibliographic Records

An electronic bibliographic record (EBR) is created by the user for each digital document submission and supplied with the document for registration. The EBR is also suitable for use in cataloging and retrieval. The EBR may be supplied to other systems without the actual document but with a pointer to it. The EBR must contain a unique name for the document per author. If a name is provided that has already been used by the same author, it will be rejected with an explanation. An acknowledgement of deposit will be returned to the user along with a unique numerical identifier and a retrieval pointer to the document, and, in the event of a claim to copyright, a certificate of registration from the RRS.

2.3 Claims Registration

When the EBR indicates a claim to copyright, the RRS will be supplied a copy of the EBR by the repository along with a digital signature (to be described shortly) that can be used to verify the accuracy of a deposit at a later time. The actual work would remain in the repository. The digital signature consists of a few

hundred bytes of data and is approximately the size of the EBR. It should allow the authenticity of the retrieved document to be formally established at any time for legal and other purposes.

2.4 Repositories

The RRS need not be colocated with a repository. It is expected that an operational RRS would be operated by the Library of Congress. The repositories would be operated by the Library of Congress as well as other organizations or individuals. Deposits in certain qualified repositories will constitute deposit for public record purposes. The Library of Congress will maintain its own repository of selected deposits.

Although a set of distributed repositories is envisioned for a widely deployed system, the proposed testbed will only have a single repository for experimentation. The repositories would be established in such a way as to insure the survival of the deposited information with perhaps different degrees of confidence (much like the treasury, banks and brokerage houses, for example). Certain information would probably not be deposited for purposes of registration and might be stored at the users local site or in a commercial repository. Highly valued information could be stored in rated repositories (5-star down to 1-star) with varying degrees of backup and corresponding costs. The most critical information, as determined by Copyright Office

regulations, might be stored at the Library of Congress or the National Archives as a safeguard. The structure of such a system of repositories should be developed as part of the project.

The advantages of a distributed repository system are:

1. Large amounts of physical storage is not required to be made available at the Library of Congress.
2. Access to the original documentation is guaranteed by the DLS to the confidence level selected by the user's choice of repository (again like the banks).
3. Repositories serve as interfaces to the users, thus offloading and insulating any central servers and systems such as the RRS from potentially large user loadings and specialized customer service requests.
4. Access to the RRS in transaction mode is available only to authorized repositories and RMSs that are qualified to use the RRS in that mode. An individual author, a collective licensing organization, a government or corporate entity or others may run an RMS. Authors and other copyright owners, as well as users may also connect directly to the RRS through a separate interactive user interface.

2.5 The Computer Network Environment

There are three specific actions of concern in a network environment. One is the movement of information already contained in a computer network environment thereby greatly facilitating the creation of multiple copies in multiple machines in fractions of a second. The second is the importation of external information, such as print material or isolated CD-ROM based material, which must first be scanned or read into the system before it can be used. The third is export of internal network based information to paper using digital printers or facsimile machines or copied to separable media such as tape or DAT for external transport to others. Some of these actions, such as local use on paper in very small quantities, may or may not be covered by fair use provisions. However, non fair use actions would require approval of rightsholders.

In addition to the above three actions, there is a fourth action that is facilitated by the computer network environment. Information in digital form has the property of being easily manipulated on a computer to produce derivative works. Such derivative works can also be easily moved about in a computer network environment and be subject to further manipulation by other parties. The technology makes it possible for parallel and concurrent manipulation of such information to result in an exponential proliferation of such derivative works.

2.6 Rights Management System

The four actions described above form a basis for a rights management system. In general, there will be many such systems operated by rightsholders or their agents for required permissions on either an exclusive or non-exclusive basis for a given type of action. To locate an RMS, a user requires the existence of a domain server that knows about the network names and addresses of all RMS servers. Transactions involving rights may be handled by direct exchange on-line between the user system and the corresponding RMS. Typically, this exchange would occur rapidly on-line, and we refer to this as the interactive clearance of rights. Privacy enhanced electronic mail would be available for exclusive licenses and other transfers of rights. Non-exclusive licenses might be handled by regular electronic mail.

Transfer of copyright ownership would usually involve recordation in the RRS and could conceivably be handled automatically by the RMS on behalf of the rightsholder and the user to facilitate matters. The confirmation from the RRS would also be passed back to the rightsholder and user directly or via the RMS using privacy enhanced mail. Various enabling mechanisms in the normal screen-based computer interface could be developed and invoked by a user to achieve rapid clearance. If included in the user

interface, this capability would have the effect of creating an instant electronic marketplace for such information.

Recordation is defined to mean the official keeping of records of transfers of copyright ownership and other documents pertaining to copyright by the Copyright Office, Library of Congress. For legal purposes, proof of official registration of claims and recordations will be provided by the Copyright Office (via the RRS). Other registrations (at repositories) and non-exclusive licenses (via RMSs) will be certified by privacy enhanced mail. It will be up to the parties to such registrations and recordations to maintain electronic records of their transactions. These could also be stored within the DLS.

2.7 Identification Systems

The electronic copyright management system actually requires several types of domain servers. First, documents can be easily retrieved via the DLS if the citation is accurately known or through one or more search and browsing processes otherwise. However, the mapping of a bibliographic pointer (to the designated repository) into its network name and address may require a separate server. Second, the above mentioned domain server for RMSs is needed. Third, the date and time that transactions have been requested and taken may need to be formally validated. An electronic notary and time server would

provide such a capability as part of the privacy enhanced mail system.

2.8 Retrieval, Appearance and Submission of Documents

Retrieval of documents from the DLS is generally a two-step process. The initial step is to identify the document and to retrieve its EBR. This record will also identify the rightsholder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permissions. Rules would have to be formulated and posted to inform clearly what obligations a user incurs when accessing the system. For example, it may be specified that a submitted request with a valid EBR will then be taken to mean acceptance of the terms and conditions, including any implementation and usage restrictions or payment requirements. The rightsholder may also wish to place restrictions on the appearance of documents for certain uses.

As part of the process of document submission, a valid EBR will have been produced which can be used in the author's system. Each author or other owner of copyright (or such owner's successor in title or duly authorized agent) will maintain his or her own collection of EBRs. Searches and requests will typically be made to the user's home system unless the rights have been transferred or delegated elsewhere (e.g. to a publisher, agent, or database provider). In applying for registration of claims to copyright at

the Copyright Office, a user could be required to certify that he or she has the rights to the material and sign the submission digitally.

3.0 Privacy and Authentication Technology

This section briefly describes several key technologies to handle privacy and authentication in the digital network environment. Four such technologies are described below, namely: 1) Public Key Cryptography, 2) Digital Signatures, 3) Privacy Enhanced Mail, and 4) Notarization.

3.1 Public Key Cryptography

In conventional cryptography, a mathematical function and a "secret key" are shared by parties who wish to communicate confidentially. Each message to be sent is "encrypted" using the function and key and the recipient(s) "decrypt" it using the same function and key. This may be thought of as sharing a locked box in which several individuals have the key and any of them can lock or unlock the box at will.

In the late 1970's, two Stanford University researchers, Martin Hellmann and Whitfield Diffie speculated that it might be possible to devise paired cryptographic functions which had the interesting property that one function would encrypt and the

other would decrypt. In fact, the concept was slightly more sophisticated in that any message encrypted with either one of the functions could only be decrypted by the other. In other words, having access to the function which did the encrypting does not help when it is time to decrypt. Using the box analogy, the public key cryptography system would be like having a box with a two-key lock. If one of the keys is used to lock the box, the other must be used to unlock it. A person holding a key used for locking could not use it for unlocking.

One of the biggest problems with conventional cryptography is that the keys must be kept secret and must be distributed by secure means. The notions of Hellman and Diffie opened up a new way of thinking about key management. One key could be made public (e.g. the one to be used for encryption) and the other kept private. Anyone knowing the public part of a pair of keys could use it to prepare a message which would remain confidential until the person knowing the private key used it to decrypt the message. The public keys could be listed in public directories without any special protection since knowing them did not help anyone decrypt messages encrypted using the public key. This feature makes it far simpler to manage key distribution since the public part need not be protected.

Three researchers at MIT, Rivest, Shamir and Adelman developed a pair of functions meeting the requirements specified by Diffie

and Hellman. These functions are now known as the RSA algorithms (from the last names of the inventors).

3.2 Digital Signatures

Since either key of a public key cryptography pair can be used to perform the initial encryption, an interesting effect can be achieved by using the secret key of the pair to encrypt messages to be sent. Anyone with access to the public key can decrypt the message and on doing so successfully, knows that the message must have been sent by the person holding the corresponding secret key. The use of the secret key acts like a "signature" since the decryption only works with the matching public key. Buyers could send digitally signed messages to sellers and the sellers could verify the identity of the sender by looking up the public key of the sender in a public directory and using it to verify the source of the message by successfully decrypting it.

3.3 Privacy-Enhanced Mail (PEM)

Public key cryptography can be combined with electronic mail to provide a flexible way to send confidential messages or digitally signed messages or both. In actual practice, a combination of public key, conventional secret key and another special function called cryptographic hashing is used to implement the features of privacy-enhanced mail. The public key algorithms require a

substantial amount of computing power compared to conventional secret key algorithms. The older secret key algorithms, such as the Data Encryption Standard (DES) developed by the National Institutes of Standards and Technology (NIST), are much more efficient. Consequently, confidential messages are typically encrypted using a conventional secret key which, itself, is sent, encrypted in the public key of the recipient. Thus, only the recipient can decrypt the conventional secret key and, eventually, decrypt the message.

To send digitally-signed messages, each message is run through a "hashing" algorithm which produces a compressed residue which is then encrypted in the private key of the sender. The message itself is left in plain text form. The recipient can apply the same hashing algorithm and compare the compressed residue against the one that was sent (after decrypting it with the sender's public key).

One of the basic problems with this application of public key cryptography is knowing whether the public key found in the directory for a given correspondent is really that correspondent's key or a bogus one inserted by a malicious person. The way this is dealt with in the Privacy-Enhanced Mail system is to create certificates containing the name of the owner of the public key and the public key itself, all of which are digitally signed by a well-known issuing authority. The public

key of the issuing authority is widely publicized so it is possible to determine whether a given certificate is valid. The actual system is more complex because it has a hierarchy of certificate issuers, but the principles remain the same.

3.4 Notarization

Using digital signatures, it is possible to establish an on-line notarization service which accepts messages, time-stamps them and digitally signs them, then returns them in that form. If the person desiring notarization digitally signs the message at the time it is sent to the notarizing service, then it will be possible, later, to establish that the person requesting the notarizing had the document/message in question at the time it was notarized. One can imagine that the originator of a message might have it notarized for the record and the recipient might independently do so. By this means, for instance, evidence of a contract's existence in the hands of each party at particular times might be established.

4.0 Verification, Authentication and Certification

The verification process uses stored digital signatures to ascertain whether a given copy is identical to the version which was originally deposited. If any portion of the copy differs from the original, the verification process will fail.

Authentication or formal certification of deposits may be provided to a requesting party in traditional ways or via electronic mail. Privacy enhanced mail would be used to certify the authenticity of a deposit, as well as to certify registration and recordation records, for legal purposes.

5.0 Conclusion

The deployment of an electronic deposit, registration and recordation capability for use in a computer network environment would greatly facilitate and accelerate the move to a network base for information creation and dissemination. The system would be compatible with the current manual system and would support the ability of the Library of Congress to provide automated registration and recordation services. It would provide a foundation for straightforward and easy expansion and evolution and provide a direct linkage for the Library of Congress to the DLS. It would provide a prime working example for all other kinds of activities where claims registration and rights management come into play. Verification and authentication of copies of deposits may be performed electronically using digital signatures. Formal certification of deposits, as well as registration and recordation records, using privacy enhanced mail may be provided for legal purposes. A testbed which demonstrates the relevant concepts and ideas can be implemented within a two to three year period with initial limited use within a year.

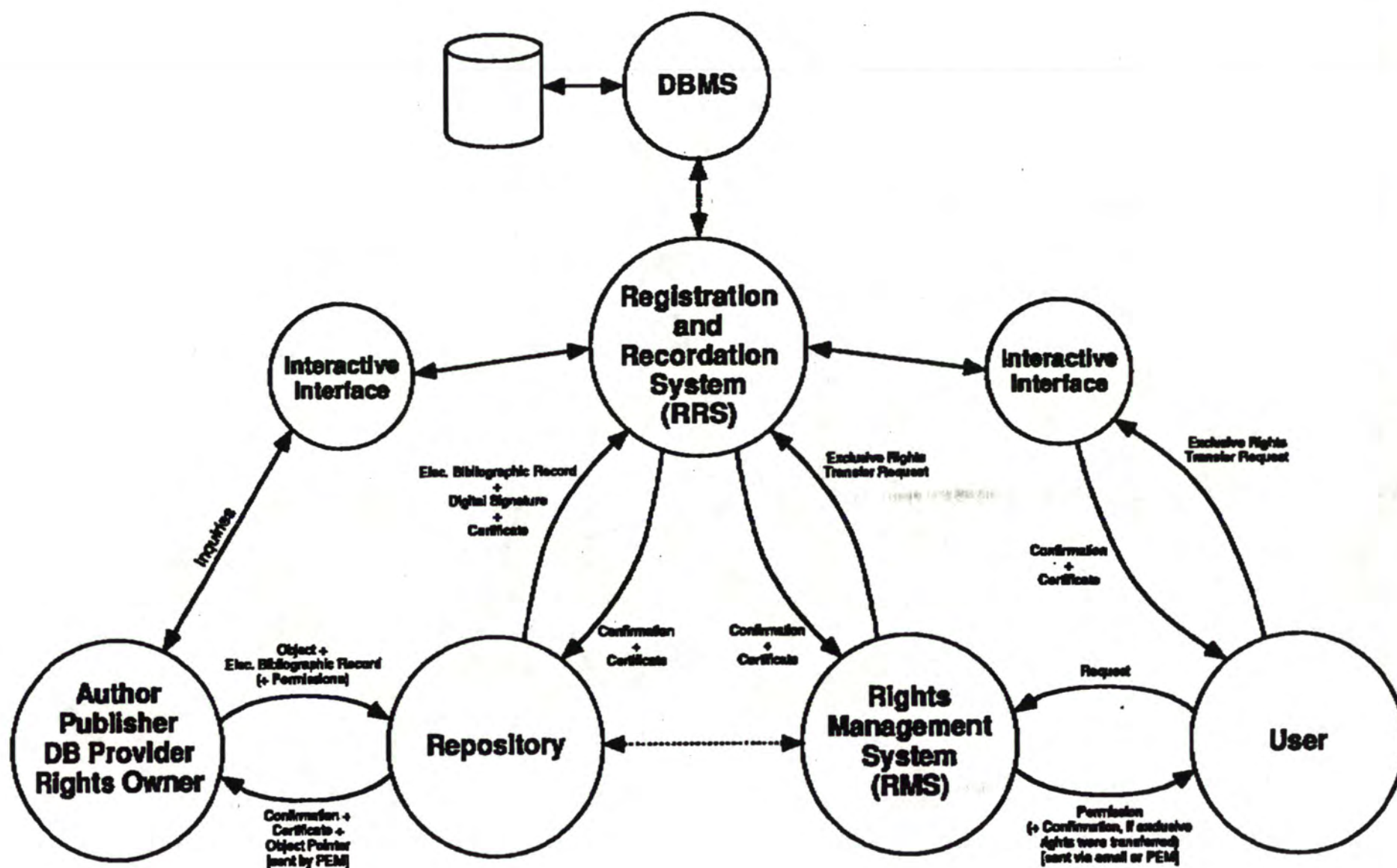


Figure 1. System Components and Information Flow.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

14

Divider Title: _____



Center for Electronic Markets

Brad J. Cox, Ph.D.

6603 Pelham Trace
Centreville VA 22020
703 968-8229 voice -8798 fax
bc Cox@gmu.edu

Commissioner of Patents and Trademarks
U.S. Patents and Trademarks Office, Box 4
Washington, DC 20231
Attn: Terri A. Southwick
Attorney-Advisor, Office of Legislation and International Affairs

Dear Ms. Soutwick:

This is in response to your request for written comments and oral testimony at your Nov 18 hearing.

I would like to testify regarding the prospect of technical solutions to the copyright issues your committee is considering.

I've enclosed the executive summary from the Coalition for Electronic Market's proposal to the Advanced Research Projects agency which outlines the approach we are considering.

Sincerely yours



Brad J. Cox, Ph.D.

ARPA Proposal

Pilot-Scale Deployment of a Multi-level Revenue Collection Mechanism for Computer-based Information Age Goods

Brad Cox; bcox@gmu.edu; 703 968 8229 Voice; 703 968 8798 Fax
George Mason University, Program on Social and Organizational Learning

Table of Contents

ARPA Proposal	1
Table of Contents	2
Executive Summary	1
Information Age Goods	1
Industry Needs a Solution	2
Invocation-based Revenue Collection	3
Pilot-scale Deployment	4
Coalition for Electronic Markets	5
Volume 1: Technical Proposal	1
1. Background	1
1.1 Software Reuse and Object-oriented Programming	2
1.2 Software Piracy	3
1.3 Information Superhighway Initiative	4
2. Our Approach	5
2.1 Overview	5
2.2 Technical Approach	8
2.3 Business Plan	10
2.4 Management Plan	11
3. Statement of Work	18
3.1 Phase Descriptions	18
3.2 Task and Element Descriptions	20
4. Selection Criteria Index	24
5. Bibliography	27

Executive Summary

A 21st century infrastructure would address many practical problems. For example, the government can serve as a catalyst for the private sector development of an advanced national communications network, which would help companies collaborate on research and design for advanced manufacturing; allow doctors across the country to access leading medical expertise; put immense educational resources at the fingertips of American teachers and students; open new avenues for disabled people to do things they can't do today; provide technical information to small businesses; and make telecommuting much easier. Such a network could do for the productivity of individuals at their places of work and learning what the interstate highway of the 1950s did for the productivity of the nation's travel and distribution system.

*A TECHNOLOGY POLICY FOR AMERICA Six Broad Initiatives
Bill Clinton; September, 1992*

President Clinton's enthusiasm for a high-tech information infrastructure is widely shared by the computer industry. This fragment of John Scully's speech to the newly-elected administration, in his role as Chief Executive Officer of Apple Computer, reflects a similar enthusiasm:

"We believe the creation of a national information infrastructure must be a national priority, and we are willing to work in partnership with the government to see that it gets done. The development of an information infrastructure will raise the standard of living for all Americans and enable our country to prosper in a competitive global economy."

This emphasis on infrastructure helps to surface a crucial paradox of the much-anticipated transition from a manufacturing age to an information age economy. Infrastructure means computers and networks. These are tangible goods that can be bought and sold by the unit just like traditional manufacturing age goods. But the goods that information age infrastructures convey are very different from the goods that traveled the highways and railroads of the manufacturing age. They are electronic properties such as computer applications, clip art, font libraries, electronic documents, reusable software components, and so forth; the intangible goods of the information age.

Information Age Goods

The computer industry's enthusiasm for infrastructure is perfectly understandable. They benefit directly by selling computers and networking hardware. However it is less obvious how users will "raise their standard of living and prosper in a competitive global economy". It is computer users, not computer vendors, who produce and consume the goods that this infrastructure conveys. It is unclear how users benefit because of an extremely fundamental problem. Information age goods can be copied and transported with almost no cost. This undercuts the traditional basis of commerce in which fees are exacted as each new copy is acquired by the customer. Thus precisely what it means to buy, to sell, and to own the goods of this increasingly dominant segment of the economy has become a tricky paradox; a formidable obstacle to the much-anticipated emergence of a information age economy.

- Software Piracy: How to control revenue losses from unauthorized copying of software, both within the U.S., but especially after it has been exported to countries where copying of software is not illegal, nor in some cases, even regarded as immoral?
- Dual-use Software: How to control how dual-use software is used after it has been exported, for example, during wartime?
- Software Crisis: Why has software productivity only grown arithmetically during the same period that hardware productivity has grown exponentially?
- Reusable Software Components: Why is nearly all computer software fabricated from first principles instead of being assembled from reusable software components?

- **Electronic Publishing:** How can book, magazine and newspaper publishers exploit electronic networks to reduce their present reliance on paper-based publishing, and the consequent degradation of the environment from deforestation, pollution from pulpwood processing, and trash disposal?
- **Mass market for computer hardware:** The quality and abundance of goods within existing information age infrastructures (Internet, Compuserve, Prodigy) is hardly sufficient to convince a potential mass market to buy home computers and networking infrastructure to access it. High quality content is more abundantly available in newsstands, bookstores and other non-electronic media. The market for computer hardware is not primarily limited by insufficient carrier but by insufficient content. Hardware, software, and networking markets are limited by the lack of an answer of how people can make money by providing information age content, as distinct from today's preoccupation with information age carrier.

This document proposes to build and deploy, on a pilot scale of limited but meaningful scope, a revenue collection mechanism for computer-based information age goods of any reasonable granularity. By 'granularity', we mean that the proposed system does not concentrate on any one of the items in the above list. It addresses each of them simultaneously by treating them all as examples of goods that enclose one another at various levels of granularity, just as automobiles enclose generators and spark plugs, and these in turn the goods of even lower levels of the automobile industry's structure of production – in bottom tier factories, refineries and mines.

This proposal's emphasis on a *uniform* revenue collection system that addresses *all* structure of production levels distinguishes it from the simpler but less capable mechanisms that are already available (dongles, shrinkwrap software, keyware, demoware, license servers, etc). These systems are certainly less ambitious but they are also far less capable in that they do not address the structure of production problem at all. They address revenue collection for a single granularity of goods such as computer applications. But they don't address the reusable software components from which the applications might be assembled. Nor do they address larger components within which the applications themselves are components. Electronic documents and network-based document repositories are examples.

The challenge of transitioning to an information age economy is similar to the challenge this nation surmounted two hundred years ago at the dawn of the manufacturing age. A similar opportunity is at hand with respect to the software industry at the emergence of the information age. A solution to the revenue collection issues discussed in this proposal is arguably the most crucial missing component that is needed to make the information age a reality. If there is to be a breakthrough in productivity in software engineering through the use of a robust market in off-the-shelf reusable components, a crucial first step is to deploy a revenue collection mechanism capable of supporting the evolution of a multi-level structure of production for computer-based information age goods.

Industry Needs a Solution

The Society of Information Management is the professional organization for more than 2,700 senior information technology executives around the world. Its 1992 member survey identified software licensing as a critical information technology issue. The following quotes are from the Software Licensing Position Statement of April 1993 in which this society summed up the view of software consumers within large corporations of means for resolving their difficulties with software licensing.

The ideal software vendor and customer partnership of the future will be based on an understanding of mutual issues, trust and the need to balance revenue stream generation for vendors with cost control for customers. As organizations move toward multi-vendor, multi-platform, open systems environments, the pricing models of today must give way to more flexible and equitable licensing models and allow for more regional and global focus on the part of customers.

The evolution toward rapid application development technology further adds to licensing fees. Licensing models have not kept pace with this evolution.

The evolution of desktop software towards the use of object-oriented technologies will transform the "Application-Centric" environment to one which is "Document-Centric." This will further add to pressures for licensing which addresses software integration trends.

Vendors must have the ability to monitor customer usage. Fair and equitable licensing models should ensure vendors' revenue streams are providing cost advantages to customers.

Their recommended approach is consistent with that of this proposal. The difference is that this proposal addresses this issue on an industry-wide basis and not exclusively from the perspective of a particular constituency. SIM's president, Steve Coppel, responded to our request for a statement to enclose with this proposal as follows: "The Society for Information Management (SIM) has addressed changes and issues regarding software technology and recognizes the software monitoring issue as one of the obstacles preventing this technology from moving forward. SIM is closely watching with interest the proposal put forth by the Coalition for Electronic Markets."

MountainNet is engaged in the AdaNET Research Project, funded by NASA, administered through the Johnson Space Center and the University of Houston - Clear Lake, under the Repository-Based Software Engineering (UHCL/RBSE) program. The purpose of the RBSE Program is to promote widespread adoption of modern software engineering, improve software quality, and reduce system life-cycle costs, across the public and private sectors of the economy. Bob Terry's responded to our request for a statement to enclose with this proposal as follows: "I spoke with my company's President (Mike Digman) and received his approval to endorse the approach the Coalition for Electronic Markets is proposing to ARPA. As I stated, we are currently attempting to monitor the access and usage of the objects in the AdaNET repository in order to provide feedback for authors, clients, and project management. We believe that your proposed work in these areas could provide us valuable technical assistance. We are interested in being involved with your proposed project in any possible manner."

Invocation-based Revenue Collection

The basis of our approach originates in the following observation. Receiving a copy of a tangible hardware device (for example, a memory chip or a computer), does not equip the customer to replicate another. Quite the opposite is the case for information age goods such as reusable software components and electronic documents, since such goods can be copied and transported at negligible cost. This difference undercuts the revenue collection mechanism of antiquity, which we call a *replication-based* mechanism since the traditional basis for commerce in tangible goods is exacting a fee when each replica is acquired by the customer.

This mechanism is robust for tangible hard-to-copy goods. It supports the broad and deep structure of production that is so characteristic of advanced engineering societies. Producers of goods at every level of the structure of production know that they will benefit whether their goods are consumed directly or indirectly. For example, a chip producer knows that revenue will accrue not only from those who use chips directly, but also indirectly as end users buy goods that use chips as internal components. But since no comparably robust revenue collection mechanism exists for easily-copied computer-based information age goods, a comparable structure of production has never emerged.

The approach proposed in this document is to directly leverage the crucial difference between manufacturing age and information age goods. Electronic objects differ from tangible objects by being fundamentally unable to monitor their copying but trivially able to monitor their use. For example, it is easy to make software count how many times it has been invoked, but hard to make it count how many times it has been copied. We call our approach an *invocation-based* market mechanism to contrast it with the *replication-based* mechanism upon which commerce in tangible goods is based. By basing revenue collection on invocation instead of replication, the easy-to-copy nature of

information age goods becomes the basis of a solution, as distinct from endlessly fighting it with technical, legal and moral restrictions.

Invocation-based charging does *not* mean that charges must be proportional to usage; often known as *pay-per-use* or *pay-per-view*. It only means that invocation records are the *basis* for whatever terms and conditions the vendor decides to provide. The vendor expresses its business conditions in a Terms and Conditions Algorithm (TCA). A billing agency uses this to convert invocation records into monetary amounts. These algorithms can easily support the familiar pay-to-own terms and conditions that dominate today's shrinkwrap market. But they can as easily support terms and conditions that are not viable options today. For example, pay-if-you-like-it involves an algorithm that simply delays the pay-to-own fee from the first to the n'th use. And of course radical incremental charging options such as pay-per-use, pay-per-minute, pay-per-keystroke can also be provided to those customers who prefer charges that are closely related to the software's measured utility to the user.

Although terms and conditions can remain the same or be radically different, software *distribution* becomes much simpler. Since revenue is now based on usage instead of on acquisition of replicas, there is no longer a need to restrict copying. With invocation-based charging, software vendors actually gain new paying customers regardless of how the copy was acquired.

Finally, although this was not anticipated as a benefit by the originators of this proposal, the ability to disable further access to software if account balances are not within threshold could also be used to disable further invocations of dual-use software on a client-specific or even geographic basis. This could be useful during wartime, for example.

Pilot-scale Deployment

Invocation-based revenue collection is a radically different approach to information economics, and as such raises a variety of serious questions. These range from the engineering challenges of building a complex system and making it secure from tampering, to the socioeconomic challenges of making it profitable, acceptable, protective of privacy, and attractive to customers.

We propose to test the concept of invocation-based revenue collection by deploying it on a pilot scale of limited but meaningful scope. The target market for this deployment is to Berkeley Productivity Group (BPG) as a software component producer, and to BPG's customers as software components consumers.

The software components addressed in this deployment is BPG's product, the *Blocks Library*. This is a library of object-oriented classes that helps factories model discrete assembly line operations. Therefore BPG's customers tend to be factories engaged in discrete assembly line operations. For example, Computer Associates is using the Blocks Library in their next generation real-time scheduling systems. We chose this domain for the deployment because the increased use of Electronic Data Interchange (EDI), object-oriented programming languages, and reusable software components within manufacturing is itself of substantial interest to ARPA, DOD and NIST; indeed most of the funding bodies for this proposal.

In the words of Christopher Lozinski, BPG's founder:

This metering per use idea makes a great deal of sense in a manufacturing environment. Charging by the CPU is extremely inefficient, and leads to curious behaviors on the part of the customers. Charging by the application makes people run their factories with only part of the functionality available. Charging by use makes more sense. It would be desirable to ship the same software, but charge the larger company more for its use than the smaller company. Since the software model knows the size of the factory it should derive the licensing fee. Let the customer with 100 machines pay more than the customer with 10 machines. Let the customer who runs many applications pay more than the customer who runs fewer. This will create a healthy tension where the users are trying to minimize the software use, and the developers are trying to tempt them with features they need. Every marginal user's needs will be met, because

the developers want to add them to the regular user base. I believe that this will lead to better service, and better products.

The goal of this project is to address the technical and socioeconomic issues of a pilot-scale deployment with a balanced combination of technical and social solutions. By a balanced approach, we mean that we do not require a purely technical solution; a solution that is impervious to tampering by an arbitrarily skilled and determined attacker. Purely technical solutions such as committing the entire metering infrastructure into tamper-resistant silicon (or using encryption to similar ends) are not cost effective options for this project, and might be unacceptably inefficient even if they were. Besides, everyday experience shows that technically impervious solutions are merely desirable, not essential. For example, robust markets exist within shopping malls where the technical barriers to shoplifting are almost as negligible as the barriers to software piracy in computers.

But the same observation argues that it would equally foolish to ignore tampering altogether. No one would trust a solution that anyone could subvert by simply turning off the computer in order to erase invocation-based data before it can be uploaded for billing purposes. Nor would people trust a system in which detailed records of their minute-by-minute computer usage were being transmitted over non-secure channels in an unencrypted form that anyone might read.

Therefore we seek to integrate technical solutions and socioeconomic solutions into a balanced and mutually-supporting whole. The technical solutions to be considered involve the use tamper-resistant packaging and silicon fabrication technology, supported by public and/or private key encryption. The socioeconomic solutions hinge upon having each party sign a contract specifying the obligations of each party to the others, the benefits to accrue if they fulfil them, and the sanctions to apply if they don't.

Coalition for Electronic Markets

The diverse technical, social, legal and business challenges of this project requires close cooperation among business, academia, and government. The Coalition for Electronic Markets (CEM) is a corporation that we've chartered as the vehicle for addressing the ownership and control issues that will emerge as this project unfolds, for raising follow-on capital, and for deploying this system as a commercially viable business.

However, for the purposes of the Statutory Program Requirements outlined in Appendix A of the Program Information Package, this project will be undertaken under section B1: *Defense Dual-Use Critical Technology Partnerships*. The prime contractor will be George Mason University as an institution of higher education in partnership with the Coalition for Electronic Markets and its members:

- Dallas Semiconductor Corporation (DSC) markets security-related products based on silicon technology and thus has extensive experience with silicon fabrication technology. Michael Bolan, a DSC founder and a member of its board of directors, will represent their interests to the coalition.
- Berkeley Productivity Group (BPG) markets software products based on object-oriented technology to factories engaged in discrete manufacturing. Christopher Lozinski is BPG's representative to the coalition.
- National Institutes of Standards and Technology: Two research groups, represented by Wayne McCoy and Miles Smid, provide world-class expertise in advanced communications and encryption technology. Wayne McCoy is NIST's representative to the coalition.
- George Mason University Foundation is also a coalition member. Since Dr. Brad Cox, CEM's president, is a GMU faculty member, Dr. Don Lavoie, the chairman of the Program on Social and Organizational Learning, will represent GMU's interests to the coalition. Scholars at the Program on Social & Organizational Learning, the Business School, the Law School and the Information and Software Systems Engineering (ISSE) Institute contribute well-rounded expertise

on the technical, legal, economic, cultural, and managerial issues involved in the creation of new market structures, the pricing of innovative products, and the careful analysis of market innovation experiments.

Intellectual property ownership and control issues will be formally addressed once this proposal is funded. We anticipate that ownership of group property will reside in CEM with shares held by coalition member companies in proportion to their contribution to this project. In the interim, ownership of intellectual property will reside within each member institution.

Many other companies have expressed interest in and support for the coalition's objectives. Its charter members were largely selected by the need to respond within the limited time available for preparing this proposal. We are especially grateful for the encouragement and support of the following individuals and institutions and look forward to their broader participation when time constraints are less pressing.

- Steve Koppel; Society for Information Management
- Bob Terry; NASA AdaNet Repository Project
- Raymond Yeh; International Software Systems Inc.
- Jim King; NCR Corporation
- Dave Roland; Roland Projects, Inc.
- John McGehee; Texas Instruments
- Les Yeager; Taligent
- Paul Mattson; IBM AS400 Division

We owe special debt of gratitude to Paul Kozemchak of the ARPA Policy Planning Office. Without the proactive encouragement and enthusiasm that he so generously provided, we'd have never undertaken this project.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

15

Divider Title: _____

WEIL, GOTSHAL & MANGES

A PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

SILICON VALLEY OFFICE
2882 SAND HILL ROAD, SUITE 280
MENLO PARK, CA 94015-7022
TEL: (415) 926-6200
FAX: (415) 854-3713

DALLAS
HOUSTON
MIAMI
NEW YORK
WASHINGTON D.C.

RONALD S. LAURIE
Direct Line: (415) 926-6210
Internet: rsl@applelink.apple.com

BRUSSELS
BUDAPEST
LONDON
PRAGUE
WARSAW

November 8, 1993

Via Facsimile
(703) 305-8865

Terri A. Southwick, Esq.
Attorney-Advisor
Office of Legislation and International Affairs
U.S. Patent & Trademark Office
Crystal Park Two, Suite 902
2121 Crystal Drive
Washington, D.C. 20231

re: Request for Comments --
*Intellectual Property Issues Involved in the
National Information Infrastructure Initiative*

Dear Ms. Southwick:

Pursuant to the above-referenced Request for Comments, as published in the Federal Register of October 19, 1993, I would like to present some brief oral remarks at the November 18, 1993 hearing to be held on this subject in Crystal City.

By way of introduction, I have worked in Silicon Valley for thirty three years, initially as a software engineer and later as an intellectual property lawyer specializing in computer law. I currently teach a course at Stanford Law School titled, "Intellectual Property Protection for Information Technologies."

I would like to suggest broadening the scope of the inquiry as follows. As formulated in the Request for Comments, the focus is on achieving the proper balance between the competing objectives of:

Terri A. Southwick, Esq.
November 8, 1993
Page 2

- providing effective intellectual property protection (primarily, via copyright) for the "electronic information and entertainment products" flowing through the NII system; and
- insuring maximum public access to the NII system and interoperability of system components, achieved, at least in part, through the use of standards and regulatory controls.

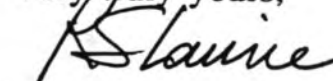
I believe that this process of balancing i.p. incentives against accessibility and connectivity should extend not only to the *content* flowing through the NII system, but also to the *delivery mechanisms* utilized in the system.

Let me illustrate my point with the following example. Two interrelated concerns of content owners are security and compensation. Delivery technology is now being developed to address both of these concerns. One such technology is that of "information metering systems" wherein the content, which is initially delivered to the end user in encrypted form, is decrypted at the user's terminal by secure hardware and software, on an as-needed basis, and "metered" as it is consumed. Compensation to individual content providers is achieved by secure software which periodically transmits usage data to a central accounting center via modem. Finally, the accounting center aggregates the usage data for all users subscribing to that center, bills the users on a monthly basis, and remits the proper amounts to the various information providers. The system operates as an "information utility" in much the same way as conventional electricity, gas and water distribution systems.

The implementation of this kind of technology presents significant policy questions involving the use of intellectual property protection (including both patents and copyrights) to promote the development of innovative information delivery mechanisms, without unduly prejudicing the interests of information consumers and developers of competitive systems.

I look forward to the opportunity of participating in the public debate on these issues.

Very truly yours,


Ronald S. Laurie

RONALD S. LAURIE

Ronald S. Laurie is a partner in the Trade Practices and Regulatory Law Department at Weil, Gotshal & Manges, a diversified commercial law firm of over six hundred fifty lawyers with six offices in the U.S. and five in Europe. He is a founding partner of the firm's Silicon Valley office located in Menlo Park, California where he heads the computer law group. Mr. Laurie also teaches computer law at Stanford Law School.

Mr. Laurie received an industrial engineering degree from the University of California at Berkeley in 1964 and worked for several years as a programmer and systems engineer in the aerospace industry before attending law school at the University of San Francisco. He has twenty five years of legal experience in the area of proprietary rights disputes involving computer technology, including hardware, software and semiconductor chip designs, with particular emphasis on compatibility and reverse engineering issues. He has assisted major American and Japanese computer and semiconductor companies in implementing reverse engineering and "clean room" design programs for compatible software and chip products in order to minimize legal exposure for copyright and mask work infringement. He is a registered patent attorney and a substantial part of his practice involves strategic planning, commercial exploitation and litigation of patents on cutting-edge software-based technologies such as artificial intelligence and multimedia systems.

Mr. Laurie represented Ashton Tate in its successful defense of the highly publicized software patent infringement suit filed by Refac Corporation against the six largest publishers of electronic spreadsheet software. He served as litigation counsel to Hewlett Packard in its defense of the "look and feel" copyright infringement suit filed by Apple Computer involving the Macintosh user interface. He has represented a number of major software publishers in copyright infringement suits against software pirates and has extensive experience in patent, trade secret and trademark litigation involving computer and semiconductor technologies.

Mr. Laurie has been an advisor to the U.S. Copyright Office, the Office of Technology Assessment of the U.S. Congress, the National Academy of Science and the World Intellectual Property Organization (WIPO), a United Nations agency based in Geneva. He is a Director of the Computer Law Association, and has served on the Executive Committees of the International Intellectual Property Association and the Intellectual Property Section of the State Bar of California. He is a member of the American Arbitration Association's Computer Dispute Resolution Panel. He is a contributing editor of *The Computer Lawyer* magazine and has published a series of articles on reverse engineering of software and chip designs. He is co-editor of the two volume treatise *International Intellectual Property* recently published by Prentice Hall Law & Business. He has lectured on computer law topics at conferences of lawyers, engineers, company executives and government officials in the United States, Japan, Europe, Australia and South America. He is one of two California intellectual property lawyers specializing in computer law to be listed in the 1991-92 and 1993-94 editions of *The Best Lawyers in America*.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

16

Divider Title: _____

villanova
university

VILLANOVA, PENNSYLVANIA 19085-1682

Henry H. Perritt, Jr.

Professor of Law

Direct Dial Number: (215) 519-7078

SCHOOL OF LAW

November 5, 1993

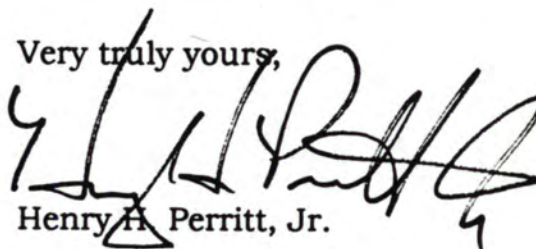
Commissioner of Patents and Trademarks
U.S. Patent and Trademark Office
Box 4
Washington, DC 20231

Attention: Terri A. Southwick, Esq., Attorney-Advisor
Office of Legislation and International Affairs
FAX (703) 305- 8885
voice (703) 305-9300

Dear Commissioner:

I request the opportunity to testify at the November 18, 1993
hearing on the protection of intellectual property in the National
Information Infrastructure. My statement is attached.

Very truly yours,



Henry H. Perritt, Jr.

Encl.

Statement of Henry H. Perritt, Jr. on Protection of Intellectual Property in the National Information Infrastructure

Introduction

In its October 19, 1993, Federal Register Notice, 58 Fed.Reg. 53917 (Oct. 19, 1993), the Working Group on Intellectual Property of the Information Policy Committee of the National Information Infrastructure (NII) Task Force requested comments on the intellectual property issues involved in the National Information Infrastructure initiative. This statement responds to that request. It argues that a commitment to high levels of encryption to protect intellectual property would negate many of the benefits of the NII and that combinations of lower levels of encryption, contracts formed electronically, and traditional intellectual property law are better ways to preserve both the incentives to create and the inherent advantages of new digital networking technologies. Entrepreneurial judgment and consumer preference, expressed in an electronic market, are better than government mandates for encryption.

I am a Professor of Law at Villanova University School of Law, and have written a number of books and articles on information technology and law. I was the principal consultant involved in formulating recommendations by the Administrative Conference of the United States on federal government electronic information policy, and currently chair the Committee on Regulatory Initiatives and Information Technology of the American Bar Association's Section on Administrative Law and Regulatory Practice. The views expressed here are personal and should not be attributed to any organization with which I am affiliated.

Wide area networks permit new kinds of electronic publishing, on demand. User needs are defined by the user, and satisfied by assembling information objects at the time of consumption from servers distributed across the network. This vision cannot be realized unless suppliers of desirable information objects can earn a return for making them available, by excluding consumers from their products until they pay. There are three ways to protect proprietary interests in distributed information objects: intellectual property, technology, and contract law.

There is broad agreement on the following propositions:

- some forms of intellectual property protection should continue

- protection by contract may be more important than protection through copyright and patent
- new technologies and architectures enable technological protection

Beyond those propositions, the prospect is murky, in part because the principal stakeholders come from different cultures. Broadcasters, entertainment producers, and cable carriers come from an environment in which encryption of satellite feeds to cable heads is routine and protected by federal law; an environment in which federal law prohibits the sale or importation of digital audio recording devices unless they reinforce encryption and technological copy control. Text publishers, librarians, government information enterprises, and Internet users come from a world in which traditional copyright protection is the main bulwark against pirates, reinforced by rudimentary password protection on computer networks. Personal computer hardware and software producers and users come from a world in which the failure of technological copy protection is a fresh memory.

In this clash of cultural traditions it is difficult to sketch the infrastructure that will serve all three groups and more. It is not altogether clear what the new architectures should look like in order for producers and consumers to enjoy the benefits of the new technology fully.

Three broad alternatives exist for protecting intellectual property in the NII: encryption, electronic contracting and intellectual property law. All have a role to play, but overemphasis on any one can blunt the benefits of the technological promise.

Technology's threat

The law recognizes intellectual property because information technology¹ permits one person to get a free ride on another person's investment in creating information value. New technologies increase the risk of free rides.

What is new with computer and wide area digital networking technology is the possibility of disaggregated value. One supplier can be a source of raw content value. Another supplier can add distribution value by providing a network that connects an ultimate consumer with a content source. Someone

¹ Information technology, as used in this sentence, includes primitive forms of technology, such as writing and copying.

else can provide an index by making pointers (like a Gopher or WAIS service) available on the network that permit a consumer to retrieve desired information directly from the content source. Creative works would reside on electronic publishing servers connected to wide area networks. Consumers of information products could access these objects, frequently combining them. Electronic publishing would be "publishing on demand" rather than the well known "publishing just in case," typified by guessing how many copies of a work will sell, printing and binding those in advance, and then putting them in inventory until someone wants them. This electronic infrastructure is a marketplace.

The concern is that it will be too easy to copy an entire work without detection and without paying for it. The new technologies make it difficult or impossible to distinguish between mere use and copying. Thus the seller cannot distinguish between an end user and a potential competitor. While intellectual property legal protection will not evaporate altogether, it will become less effective.

Technology's promise

But technology is capable of protecting investment in new ways as well as offering the potential for a free ride. Computer networks make it possible to restrict access and to determine when access occurs. Computer networks also make it possible to enter into contractual arrangements that protect intellectual property while facilitating publishing on demand. The new technologies also permit a much better audit trail, potentially producing better evidence for enforcement of both copyright and contractual rights. Depending on how new networks are designed, they may actually reduce free-ride potential.

Technology can protect intellectual property in two different ways. It can protect by denying access to the intellectual property until payment is made. This is a form of a priori protection. Encryption concentrates on this mode of protection. A second mode of protection is ex post, representing a sanction for violation of contractual terms. Under this second mode of protection, a user violating the terms of a contract for earlier use of intellectual property would be denied further access to a system prospectively.

Electronic contracting

In the traditional production process, the contracts for assigning and regulating proprietary rights from one stage to another were essentially bilateral and relational. In the new electronic publishing environment,

contracts are more likely to be multilateral and anonymous. Because of the multilateral and anonymous character of contracting in the new architecture, contracts must be standardized rather than negotiated de novo. Otherwise, transaction costs would be far too high for the market to work. Standardization in a computer environment means the development of data structures ("permissions headers") so that the exchange and contract formation process can be partially or fully automated.

Electronic contracting in an on-demand electronic publishing system invites comparison to Electronic Data Interchange ("EDI"). EDI is in wide use in American and foreign commerce, using industry-specific standards for discrete commercial documents like purchase orders, invoices, and payment orders, developed through the American National Standards Institute Accredited Standards Organization X12. EDI already has addressed many of the contract law and implementation questions that arise in technical systems for protecting intellectual property in the NII.

The starting point conceptually for identifying the elements of the permissions header are the rights exclusively reserved to a copyright owner by § 106 of the copyright statute.² The owner of an information object is free to impose contractual restrictions. The following kinds of privileges should be addressed in the permissions header:

- outright transfer of all rights
- use privilege, either unrestricted or subject to restrictions³
- copying, either unlimited or subject to restrictions like quantitative limits
- distribution, either unlimited or subject to restrictions, like geographic ones or limits on the markets to which distribution can occur
- preparation of derivative works.

Generalization of the permissions header concept beyond the level of an individual item of information content, to the level of network access, or access

² 17 U.S.C. § 106 (1988).

³ Display and presentation rights, separately identified in § 106, would be subsumed into the use element, because they are particular uses.

to a particular type of value like pointers in a Gopher server, requires adding the following privileges:

- access to the process to which the header is attached
- use restrictions, e.g. no redistribution, on material obtained through the process

Also, the data structure must allow for a specification of acceptable payment terms and have some kind of trigger for a payment approval procedure. For example, the permissions header might require presentation of a credit card number and then trigger a process that would communicate with the appropriate credit card database to obtain authorization.

There is a relationship between the permissions-header data structures and legal concepts. The query is a solicitation of offers. The permissions header is an offer. The matching of the two constitutes an acceptance.

These technological approaches provide new avenues, at lower cost, for traditional legal protections based on contract. But a threshold question for electronic contracting as a protection for intellectual property in the NII is whether the traditional formalities for making a contract are present when the contract is made through electronic means. The law does not enforce every promise. Instead, it focuses its power only on promises surrounded with certain formalities to make it likely that the person making the promise (the "promisor") and the person receiving the promise (the "promisee") understood that their communication had legal consequences. Traditional contract law requires "writings" and "signatures" for certain kinds of contracts - basically those contemplating performance extending beyond a period of one year.⁴

There is flexibility in the meaning of "writing" and "signature." They have two purposes: consciousness raising,⁵ and reliability of evidence.

The consciousness-raising purpose can be served by computerized contracting systems. This is so not so much because the computers are "aware" of the effect of their "conduct." Computers do not have consciousness. Rather,

⁴ In addition, the Copyright Act itself requires signed writings for transfers of copyright interests. 17 U.S.C. § 204(a). (1988).

⁵ See Michael S. Baum & Henry H. Perritt, Jr., ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW ch. 6 (1991) (contract, evidence and agency issues) [hereinafter "Baum & Perritt"].

it is true because the computers are agents of human principals. The programming of the computer to accept certain contract terms is the granting of authority to the computer agent to enter into a contract. The fact that a principal acts through an agent engaging in conduct at a later point and time never has been thought to defeat contract formation in the traditional evolution of agency and contract law. Nor should it when the agent is a computer.

Fulfillment of the evidentiary purpose depends on the reliability of the information retained by the electronic contracting systems. The ultimate question is trustworthiness, and if the computer methods are apparently reliable, the computerized contract should be valid unless the opponent can raise some reasonable factual question undercutting trustworthiness of the computerized record of the contract terms.⁶

Traditional evidence law permits computer records to be introduced in evidence when they satisfy the requirements of the business records exception: basically that they are made in the ordinary course of business, that they are relied on for the performance of regular business activities, and that there is no independent reason for questioning their reliability.⁷ The business records exception shares with the authentication concept, the statute of frauds, and the parol evidence rule a common concern with reliability.⁸ The same procedural guarantees and established practices that ensure reliability for hearsay purposes also ensure reliability for the other purposes. Any designer of an electronic contracting system for the NII can consult with counsel and design a system to meet the evidentiary requirements for a valid electronic contract.

In current EDI practice, contract interpretation and enforcement questions are eased by having parties who expect to have EDI transactions with each

⁶ See *United States v. Hutson*, 821 F.2d 1015, 1020 (5th Cir. 1987) (remanding embezzlement conviction, although computer records were admissible under business records exception, despite trustworthiness challenged based on fact that defendant embezzled by altering computer files; access to files offered in evidence was restricted by special code).

⁷ F.R.E. 803(6) (excluding business records from inadmissibility as hearsay); 28 U.S.C. § 1732 ("Business Records Act" permitting destruction of paper copies of government information reliably recorded by any means and allowing admission of remaining reliable record).

⁸ See Rudolph J. Peritz, *Computer Data And Reliability: A Call For Authentication Of Business Records Under The Federal Rules Of Evidence*, 80 Nw.U.L.Rev. 956, 978-80, 984-85 (1986) (noting body of commentator opinion saying that business records exception and authentication are parallel ways of establishing reliability).

other sign a paper trading partner agreement, in which the meaning of values or codes in the transaction sets is established.⁹ But requiring each pair of suppliers and users of information in the NII to have written contracts with each other in advance would defeat much of the utility of the NII. Thus the challenge is to establish some ground rules for the meaning of permissions header values to which all participants are bound. There are analogous situations. One is a standard credit card agreement that establishes contractual terms among credit card issuer, credit card subscriber, and merchant who accepts the credit card. The intermediary - the credit card company - unilaterally establishes contract terms to which the trading partners assent by using and accepting the credit card.¹⁰ Also, it is widely recognized that members of a private association can, through their constitution and bylaws, establish contractual relationships that bind all of the members in dealing with each other.¹¹ In the NII, similar legal arrangements can establish the standards by which electronic transactions between permissions header and user or intermediary requests will bind the transferor and the transferee of information.

Encryption

Encryption in the NII would relieve pressure on legal concepts because it substitutes technological for legal protection of the proprietary interests of suppliers.

It is important to distinguish among three uses for encryption, representing progressively higher levels of security and sophistication. First, is a simple payment authorization subsystem, similar to a credit card verification procedure, effectuated without human intervention. Encryption would be used in this subsystem to authenticate credit card numbers and approval codes and

⁹ See Baum & Perritt § 2.6; Note, *Legal Responses to Commercial Transactions Employing Novel Communications Media*, 90 Mich.L.Rev. 1145 (1992).

¹⁰ *Garber v. Harris Trust & Savings Bank*, 432 N.E.2d 1309, 1311-1312 (Ill. App. 1982) ("each use of the credit card constitutes a separate contract between the parties;" citing cases). It is not quite this simple, because both merchant and credit card customer have separate written contracts with the credit card issuer. But there is no reason that a supplier of information to a Digital Library System and all customers of that system might not have their own contracts with the Digital Library System in the same fashion.

¹¹ *Straub v. American Bowling Congress*, 353 N.W.2d 11 (Neb. 1984) (rule of judicial deference to private associations, and compliance with association requirements, counseled affirmance of summary judgment against member of bowling league who complained his achievements were not recognized).

to protect them from tampering or interception. No encryption would be used at the level of the permissions header or content.

Second, encryption associated with digital signature algorithms could be used to authenticate a header, contents and to detect if a header has been removed from contents with which it is associated. The contents themselves would not be encrypted.

In the third level, the contents as well as other attributes of the intellectual property protection system would be encrypted and decrypted only when permission is granted to a particular consumer.

It is well recognized that encryption provides higher levels of security than other approaches. But security through encryption comes at a price.

As the sophistication and degree of encryption increases, so also must the sophistication and universality of the infrastructure to support its use in an intellectual property protection system. An important infrastructure requirement for practicable public key cryptography is the establishment and maintenance of certifying entities that maintain the public keys and ensure that they are genuine ones rather than bogus ones inserted by forgers. A rough analogy can be drawn between the public key certifying entities and notaries public. Both kinds of institutions verify the authenticity of signatures. Both kinds require some level of licensing by governmental entities. Otherwise the word of the "electronic notary" (certifying entity) is no better than an uncertified, unencrypted signature. In a political and legal environment in which the limitations of regulatory programs have been recognized and have led to deregulation of major industries, it is not clear that a major new regulatory arrangement for public key encryption is practicable.

If one is skeptical about the likelihood of universal acceptance of content-encryption mechanisms because they get in the way of users, because the requisite standards cannot be agreed to, or because transaction costs are higher than the risk warrants, use of one of the lower levels of encryption may be more attractive.

Encrypted content affords greater security to the owner of copyrighted material, because someone who has not paid the price to the copyright owner must incur a much higher cost to steal the material. But the problem is everyone must pay a higher price to use the material. One of the dramatic lessons of the desktop computer revolution was the clear rejection of copyright protection in personal computer software. The reasons that copy protection did

not survive in the marketplace militate against embracing encryption for content. Encryption interferes with the realization of electronic markets, because producer and consumer must have the same encryption and decryption protocols. Encryption burdens the processing of electronic information objects because it adds another layer. Some specific implementations of encryption require additional hardware at appreciable costs.

Law and technology as barriers

A number of the issues posed in the Department's October 19, 1993, Federal Register Notice, 58 Fed.Reg. 53917 (Oct. 19, 1993) suggested that legal duties to adhere to some particular approaches for protecting intellectual property might be imposed.¹² For example, "should standards or other *requirements* be adopted for the labeling or encoding of works available via the NII "Should standards be established to encourage or *require* the intercommunication or exchange of information and the interoperability of the different types of computer software" "Are there technical means for preventing unauthorized reproduction or other unauthorized uses of copyrighted works that should be *mandated or required* to comply with certain standards"

It would be most unwise to adopt legal requirements for technologies, especially encryption technologies, for protecting intellectual property. Such an approach freezes technology. It blocks access to the National Information Infrastructure by those unwilling or unable to adhere to particular technologies, and if some kind of pre-approval or licensing approach were used as the enforcement mechanism, it actually would erect a bureaucratic impediment to participation that now is routine in the existing electronic infrastructure represented by the Internet.

On the other hand, if the enforcement mechanism were entirely post hoc, the approach would either clog the courts or require the establishment of a kind of intellectual property police force to detect and punish violations.

¹² The intercommunication and interoperability questions posed in the fourth issue statement are matters of broader significance to the national information infrastructure and more appropriately would be addressed in connection with the reinvention or reconceptualization of the common carrier idea by the Telecommunications Policy Committee of the Information Infrastructure Task Force, perhaps with input from the working group on intellectual property rights.

The full potential of the NII cannot be realized until consumers perceive that the benefits of electronic formats outweigh the costs, compared to paper formats. Legally mandated encryption interferes with electronic formats' traditional advantages of density, reusability, editability, and computer search ability and also, by impairing open architectures may perpetuate some of papers' advantages.

Law and technology as complements

While high levels of encryption could make legal protection almost unnecessary, the factors discussed in the preceding sections militate against adopting the highest levels of encryption. This suggests examining the efficacy of legal protection, based on contract and on copyright and patent.

Different levels of security can be achieved through any of the three methods, electronic contracting, encryption and intellectual property law, depending on the sophistication of the system used. There is no such thing as a free lunch, however. Higher levels of security come at a price -- the price of higher transaction costs.

Realizing the potential of electronic publishing in distributed information networks requires sensitivity to the transaction costs of too much security. Conventional publishing markets and technologies are appropriately sensitive. With traditional technology, if an author and publisher are worried about unauthorized photocopying of a book, they *could* insist that each purchaser of the book also be accompanied by an armed guard whenever the book is used. The presence of the armed guard surely would reduce the likelihood of unauthorized copying. On the other hand, the disproportionality of cost to risk and the inconvenience to the user would be so great that real world consumers and producers never gave the idea serious thought.

Despite the theoretical need for standardization of exchange and contracting in the NII, nothing in the history of standard setting for computer software suggests any reason for optimism that universal nonproprietary standards will be agreed to in time to be useful. The reality will be that a variety of institutional mechanisms will co-exist in order to protect intellectual property. In designing these institutional arrangements, it is important to observe two criteria:

1. the institutional arrangement for protection should be proportional to the risk, and

2. the institutional arrangement should not frustrate the inherent benefits of the architecture.

Realizing the potential of digital networks as electronic publishing environments requires that law and technology work together to minimize the risks of free riding on the intellectual contributions of authors and publishers. While high levels of encryption can virtually eliminate the need for contract and copyright legal protections, the advantages of electronic publishing on demand in wide area networks can be realized better through a combination of modest levels of encryption, contract protection and copyright and patent. Contract-law and evidence-law doctrines are adequate to protect contributors in well-designed digital library systems, but there is a risk that relying on encryption and other sophisticated technological means to protect intellectual property in content will frustrate the vision of an open architecture for electronic publishing because they impose transaction costs disproportionate to the risk. A better solution is to rely on technical control of access to networks and value added processes, backed up by contract, trade secret and patent law.

Whatever the role of encryption and electronic contracting, copyright will retain three important functions, under present interpretations of the Copyright Act. First, it would protect against wholesale misappropriation of content.¹³ Second, it would protect the computer programs through which much value in the NII is produced. Third it would protect encryption schemes.

Patent and trade secret protection is also appropriate for process innovations, and trademark concepts will protect against misrepresentation of origin.

Conclusion

Realization of decentralized, on demand, electronic publishing in the NII requires a method for collecting money and granting permission to use works protected by intellectual property. Standards for the data structures involved must be agreed to, and systems must be designed to satisfy legal formalities aimed at ensuring awareness of the legal significance of transactions and reliable proof of the terms of the transactions.

¹³ Under *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991), of course, copyright cannot play this role with respect to content that is in the public domain, like the text of federal statutes, and factual information. For these kinds of content, however, incentives in the form of protections against free riding are not necessary. Taxpayers pay the cost of production.

There is much enthusiasm for public key encryption. Yet the vulnerability of public key encryption systems is in the integrity of the key authority. In traditional legal protections, the third party custodians or authenticating agents like notaries public and registrars of deeds receive state sanction and approval, and in the case of registrars of deeds, public funding. We must be clearer as to whether a similar infrastructure must be developed to make encryption a feasible approach to protecting intellectual property. The cost of enforcement infrastructure for encryption must be weighed against the risks of free riding with other techniques of protection.

We must be thoughtful about what legal obligations, imposed on whom, are appropriate. Burdening intermediaries to police intellectual property rights is a bad idea. Such burdens discourage the construction of electronic publishing systems utilizing distributed information. They also look like King James I's restrictive licensing of printing presses to control the flow of information, the genesis of legal copyright.

The NII should be an environment in which vigorous competition among producers and product concepts can take place. In that environment, some of today's questions about the relative transaction costs of encryption versus electronic contracting, the institutional overhead required for reliable public key encryption, the performance penalties associated with encryption, and the magnitude of the risk of piracy will be answered. Picking particular technologies should wait for more experience. Imposing new legal obligations on information producers should wait even longer.

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

17

Divider Title: _____



November 8, 1993

Ms. Terri A. Southwick
U.S. Patent and Trademark Office
P.O. Box 4
Washington, D.C. 20231

RE: Request for Comments on the Intellectual Property Issues
Involved in the National Information Infrastructure Initiative, 58
Fed. Reg. 53917 (Oct. 19, 1993)

Dear Ms. Southwick:

Enclosed are an original and five (5) copies of ITAA's comments in the above-referenced proceeding. This is also a request for an opportunity to testify at the public hearing scheduled for November 18, 1993, and otherwise to attend the hearing.

If you have any questions about ITAA's comments or this request, please contact me directly at (703) 284-5349.

Sincerely,

Ronald J. Palenski
Senior Vice President and General Counsel

Information Technology Association of America



November 8, 1993

The Honorable Bruce A. Lehman
Assistant Secretary of Commerce and Commissioner
of Patents and Trademarks
U.S. Patent and Trademark Office
Box 4
Washington, D.C. 20231

RE: Request for Comments on the Intellectual Property Issues
Involved in the National Information Infrastructure Initiative, 58
Fed. Reg. 53917 (Oct. 19, 1993)

Dear Assistant Secretary Lehman:

What follows are the comments of the Information Technology Association of America, Inc. (ITAA) in the above-referenced proceeding. ITAA is the principal trade association of this nation's information technology industry. Its more than 2400 direct and affiliated corporate members provide the public and private sectors with the computer-related products and services that make possible the useful application of information technology. These products and services include: applications and systems software for mainframe, mid-range, and personal computers; custom and contract programming services; information systems integration services; and information processing services. ITAA's members and industry have a significant stake in the National Information Infrastructure (NII) initiative and in the issues raised in this proceeding.

General Comments

Given the very early stage of development, it is difficult to foresee with certainty the precise issues that will emerge concerning intellectual property protection for works made available by way of an enhanced NII. However over the years, copyright has proved itself to be a flexible system of protection, capable of adapting to new technologies, and ITAA expects that the copyright system will meet whatever challenges the NII presents.

Regardless of how the NII initiative develops, ITAA strongly believes that the existing rights of computer program copyright owners, particularly the rights to control reproduction, adaptation, and distribution, should not be lessened. The success of an enhanced NII will depend directly on the willingness of software and other authors to make their digital works available by way of an information superhighway – a willingness which will be predicated on their expectation of adequate but effective protection for their high-value but easily misappropriated digital works.

Information Technology Association of America

1. Is the existing copyright law adequate to protect the rights of those who will make their works available via the NII? What statutory or regulatory changes, if any, should be made?

Given that the architecture of an enhanced NII is presently uncertain, it is not clear to ITAA that the U.S. Copyright Act needs major adjustment at this time. The foreseeable challenge to copyright owners will be effective enforcement of existing substantive rights rather than their creation.

Computer program authors are almost certain, however, to rely heavily upon technical copy protection or encryption methods to protect their works on the NII. Currently, circumvention of technical copy protection or encryption systems is not unlawful unless it is found to constitute contributory copyright infringement.¹ Given the high value of digital works, including computer software, and the ease and perfection with which they may be misappropriated, ITAA believes that the U.S. Copyright Act should be amended specifically to make unlawful the importation, manufacture, or distribution of any device or the offering of any system or service the primary purpose of which is to circumvent the technical copy protection or encryption systems implemented by software copyright owners to prevent the unauthorized copying of their works. Similar provisions were enacted recently with respect to digital audio recording devices and are addressed with regard to encrypted satellite signals in the North American Free Trade Agreement.² Otherwise, specific statutory changes should be made only as the NII develops and specific need arises.

2. Do existing fair use provisions of the copyright law adequately accommodate the interests of users of the works available via the NII? What statutory or regulatory changes, if any, should be made?

It should be noted that "fair use" is a defense to a finding of infringement, rather than a substantive right. Fair use designed to avoid rigid application of the copyright law in circumstances when to do so would stifle the very creativity the copyright system was designed to foster.³ The fair use doctrine is but another mechanism designed to balance the interests of copyright holders and the public. Thus, the more appropriate question is whether the fair use provisions of the U.S. Copyright Act will continue to balance the interests of copyright owners and the public in a digital era – a question which ITAA would strongly answer affirmatively.

As noted above, the copyright system has demonstrated amazing adaptability in the face of new technologies, a characteristic shared by the fair use doctrine. ITAA thus sees no present need to alter the statutory embodiment of this judicially created rule of reason. As the NII develops, however, it may be helpful if digital authors and the users of their works agreed on guidelines for appropriate use of digital works, as was done in connection with the 1976 Copyright Act revision for educational materials.⁴

3. Should standards or other requirements be adopted for the labeling or encoding of works available via the NII so that copyright owners and users can identify copyrighted works and the conditions for their use?

¹ See generally, 3 Nimmer on Copyright, § 12.04[A][2] and [3] (1993).

² See, Audio Home Recording Act, 17 U.S.C. § 1002 (1992). See also, North American Free Trade Agreement, Part 6, Art. 1707.

³ 3 Nimmer on Copyright, § 13.05 (1993).

⁴ See, House Report on the Copyright Act of 1976, H. Rep. 94-1476, 94th Cong., 2d Sess., 67-75 (1976).

ITAA notes that a labelling requirement may have implications with respect to Article 5(2) of the Berne Convention for the Protection of Literary and Artistic Works (1971) which prohibits formalities as a precondition for the enjoyment and exercise of copyright rights. Moreover, the NII is likely to become part of an international network of networks in which the lack of formalities will be the norm. Accordingly, ITAA believes that all digital works made available by way of the NII should be presumed to be protected by copyright unless the contrary is indicated. In addition, ITAA believes that technical standards, such as those that would be necessary to implement a labelling or encoding scheme, as well as business standards, should emerge from voluntary, industry-led, consensus processes, with government participation and support.⁵

4. Should standards be established to encourage or require the intercommunication or exchange of information and the interoperability of the different types of computer software and systems supporting or utilizing the NII?

As stated in its July 1993 Issues Paper, "National Information Infrastructure: Industry and Government Roles," ITAA believes that:

[t]he NII, and in particular the movement towards joint government-industry work in application development, deeply implicates standards in two overlapping but somewhat distinct ways. The first applies to technical standards in the traditional sense. While these sometimes take a simple *physical* form, as in plug connections, IT industry standards are apt to be *logical*, as in interfaces. Interconnection and interoperability standards for all NII components, including equipment, networks, services and applications – as well as agreed upon interfaces – are essential if the United States is to enjoy the benefits of a 'network of networks.' " (Emphasis in original.)

At the same time, however, ITAA strongly believes that the content of standards, including interconnection and interoperability standards, should emerge from *voluntary, industry-led*, consensus processes, but with government participation and support to ensure uniformity in connection with public and private transactions. Moreover, where proprietary technology is incorporated into national and international standards, ITAA favors the evolving industry practice of nonexclusive licensing on reasonable terms.⁶

5. Should a licensing system be developed for certain uses of any or all works available via the NII? If so, should there be a single type of licensing or should the NII support a multiplicity of licensing systems?

ITAA does not presently favor a licensing/collection system for computer software made available by way of the NII. A rich variety of software applications has already been made available to the American people, and the U.S. software industry has prospered under a system of private contract. There are no indications that this system will not work well into the coming digital era. To the extent, however, that a standardized licensing system may become necessary, it should be voluntary, nondiscriminatory, and come into being primarily because of commercial concerns.

6. Are there technical means for preventing unauthorized reproduction or other unauthorized uses of copyrighted works that should be mandated or required to comply with certain standards (similar to the serial copying controls required in digital audio recording devices and digital audio interface

⁵ See, ITAA, "National Information Infrastructure: Industry and Government Roles," § 3.0 (1993).

⁶ *Id.* at §3.1.

devices under the Audio Home Recording Act of 1992)?

As stated before, computer software authors will likely resort to technical copy protection or encryption systems to safeguard their intellectual property rights. ITAA believes very strongly that any standards in this regard should be voluntary, and adopted pursuant to an industry-led, consensus-finding process in which government plays a part. Indeed, it is likely that new technical copy protection and encryption systems will emerge as an enhanced NII develops, so that it would be premature for anyone, government or industry, to promote standards at this time.

7. What types of educational programs might be developed to increase public awareness of intellectual property laws, their importance to the economy, and their application to works available via the NII?

Since 1983, ITAA has been a leader in efforts to educate the public regarding the benefits of strong intellectual property protection and the need to respect copyright. In addition to pursuing legislative, technical, and litigation efforts, ITAA has aggressively pursued public education, targeting attractive brochures about the need for software copyright protection to the business and academic communities. The prospect of an enhanced NII offers additional opportunities to educate the software-using public about the benefits of and need for intellectual property protection, employing the very computer and communications technologies made available by the NII. Imagine, for example, the powerful message that could be conveyed using emerging multimedia technologies or consider the possibilities of digital PSA's, or public service announcements, broadcast over the NII. The possibilities are many and limited only by imagination. Again, however, it should be up to the private sector to use its considerable creative resources to convey the message.

Conclusion

ITAA appreciates this opportunity to present its preliminary views to the Administration regarding intellectual property protection and the National Information Infrastructure. In the coming days and weeks, ITAA will be devoting additional resources to this and the other major policy questions arising from the proposal to create an enhanced NII. ITAA intends to provide the Administration with additional information and offers any assistance it can provide on this matter.

Sincerely,



Ronald J. Palenski
Senior Vice President and General Counsel

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

18

Divider Title: _____

Software Publishers Association



November 9, 1993

Commissioner of Patents and Trademarks
U.S. Patent and Trademark Office
Box 4
Washington, D.C. 20231

Attn.: Terri A. Southwick, Attorney-Advisor

**Re: Comments on Intellectual Property Issues Involved
in the National Information Infrastructure**

1730 M Street
Northwest
Suite 700
Washington, DC
20036-4510

Telephone
(202) 452-1600

Fax
(202) 223-8756

Dear Mr. Commissioner:

The Software Publishers Association (SPA) wishes to comment on the intellectual property issues involved in the National Information Infrastructure (NII), as requested by the Working Group on Intellectual Property Rights of the Information Infrastructure Task Force (IITF).

SPA is the principal trade association of the personal computer software industry. Its more than 1,000 members range from well-known companies, such as Adobe, Apple, Computer Associates, Novell, IBM, and Symantec, to hundreds of smaller companies, all of which develop and market business, consumer, and education software. SPA members sold more than \$30 billion of packaged software in 1992, accounting for more than half of total worldwide sales.¹

Since it was founded in 1984, SPA has been a leader in advancing the interests of its members through copyright law. In 1989, SPA testified before Congress in support of the Computer Software Rental Amendment Act, and in 1992 was closely involved in making copying computer programs a felony under some circumstances. This year, SPA testified before House and Senate judiciary subcommittees to support the Copyright Reform Act of 1993 (H.R. 897 and S. 373), which would advance equal access to the courts for every copyright owner and contribute to the war on software piracy.

¹ For world market estimates, see U.S. Dept. of Commerce, *U.S. Industrial Outlook, 1993*, at 26-34 (Table 7).

Software Publishers Association

SPA wishes to inform the Working Group of its concerns for protecting intellectual property in works available on the NII and other electronic networks, such as the Internet. These hearings are very timely because hardly a day passes without news of another corporate merger or technological development that heralds the birth of the "information superhighway."

Yet, in other respects, the inquiries made by the Working Group may be premature because the shape of the NII is still largely unknown. For example, the intelligent software capable of taking advantage of the wealth of information on the NII has not yet been developed.² It is also unknown whether the NII will be a directly interactive network, a "world of interconnected, wide-area networks, which allow[s] a publisher access to virtually unlimited markets for their information."³ On the other hand, the NII could develop as a mediated distribution system provided by a single carrier, such as a local telephone or cable television company. Thus, the Task Force may need to revisit these issues as the NII comes closer to being a reality. In the meantime, SPA wishes to make the following comments in response to the Working Group's inquiries:

- **Is the existing copyright law adequate to protect the rights of those who will make their works available via the NII? What statutory or regulatory changes, if any, should be made?**

The Copyright Act of 1976, as amended, appears at present to be adequate to protect the rights of those who make their works available via the NII. Like the shape of the NII itself, however, the way in which copyrighted works will be used, once available on the NII, is largely unknown. As these practices develop, and potential abuses arise, the courts should have the first opportunity to apply the copyright law. If shortcomings become evident, then the copyright law should be revisited and, if necessary, modified to preserve the rights of copyright owners to control their works.

The outlines of some copyright issues are now visible, however, and SPA urges the Working Group:

² Vizard, "Software May Clear Some Hurdles on Data Highway," Computerworld (Oct. 25, 1993), p.45.

³ WAIS Inc. Questions and Answers (March 1993), at 1.

Software Publishers Association

- (1) To make clear that the exclusive rights provided to copyright owners, as well as other intellectual property rights, must be respected on the NII;
- (2) Ensure that the scope of the exclusive rights of public performance and display of copyrighted works on the NII and other telecommunications networks is adequate to preserve their economic potential, and is not undermined by exempted uses that supplant demand for copies;
- (3) Make illegal as contributory infringement the manufacture, importation, or sale of technical devices or computer software products designed to circumvent copy protection or network security; and make illegal as copyright infringement their use.
- (4) Support U.S. ratification of multilateral agreements, like GATT-TRIPS, NAFTA, and the Berne Protocol, that will protect dissemination of copyrighted works on telecommunications networks; and
- (5) Clarify contract law as needed to enable copyright owners to transact licenses and other contracts in an interactive telecommunications network.

These points are discussed below.

First, SPA strongly rejects the position of some that copyright and other intellectual property rights, such as trade secrets, are somehow lost when works are made available on electronic networks.⁴ Rather, copyright and other intellectual property rights must be respected, regardless of the technological means by which they are presented or disseminated, for rights holders to make their works available at all.

Software piracy, which SPA estimates cost software developers over \$3 billion in lost revenues in the U.S. alone during 1990 and 1991, could be much higher if software is illegally posted and copied from telecommunications networks. For example, large numbers of copyrighted works are now available on bulletin board services (BBS), and the number is growing daily. The number of legitimate BBS systems, estimated at over 50,000 in the U.S. today, is mirrored by that of pirate BBS systems dedicated to software piracy. Pirate

⁴ See Rose, "Is Copyright Dead on the Net," Wired 1.5 (Nov. 1993), at p. 112.

Software Publishers Association

BBS systems comprise 17 percent of all BBS systems, and SPA monitors nearly 2,000 such bulletin boards for piracy. Besides piracy, the prospect looms that large numbers of works, including digitized photographs and other images, could be infringed by unauthorized adaptation. While questions of fair use will arise, copyright owners will be reluctant to make their works available on telecommunications networks unless they have assurances that their legal rights will be respected, and that they have the means to enforce those rights.

Second, the rights of public performance and public display of literary and audio-visual works, which are provided by Sections 106(4) and (5) of the Copyright Act, will be increasingly important to protect copyrighted works on the NII. Once many works are accessible on demand through the NII and other networks, users may choose to display or perform these works without purchasing a copy. Because these uses may well substitute for the need to purchase or download copies, and thus diminish the market for them, the display and performance rights should provide copyright owners with the means, such as on-line and access fees, to realize the commercial potential of their works.

Congress anticipated the dissemination of copyrighted works via telecommunications networks in 1976 when in a House report it stated that "performances and displays are continuing to supplant markets for printed copies . . ." ⁵ The legislative history explains that while "the showing of images on a screen or tube would not be a violation of [the reproduction right], it might come within the scope of [the public display right] ⁶. Therefore,

⁵ H.R. Rep. No. 94-1476, 94th Cong., 2d Sess. 63 (1976); S. Rep. No. 94-473, 94th Cong., 1st Sess. (1975), *hereinafter cited collectively as* "H.R. Rep."

⁶ H.R. Rep., at 62. As the House Report explained:

"The definition of 'transmit' -- to communicate a performance or display 'by an device or process whereby images or sound are received beyond the place from which they are sent' -- is broad enough to include all conceivable forms and combinations of wired or wireless communications media, including but by no means limited to radio and television broadcasting as we know them. Each and every method by which the images or sounds comprising a performance or display are picked up and conveyed is a 'transmission,' and if the transmission reaches the public in any form, the case comes within the scope of clauses (4) and (5) of section 106

Moreover, the legislative history also makes clear that transmission over networks may also constitute a "public" performance or display that requires authorization from the copyright owner. In particular

Software Publishers Association

the Working Group should ensure that the rights of public performance and public display of copyrighted works on the NII are adequate to preserve their economic potential, and are not undermined by exempted uses that supplant demand for copies and diminish the market for copyrighted works. The Working Group should also consider whether these rights should be supplemented by an exclusive right of digital transmission, or digital delivery, that would enable copyright owners to maintain control of works that are disseminated over networks, but not necessarily reproduced in copies.

Third, because hardware and software locks will be an important means of controlling access to copyrighted materials, the Working Group should recommend that the manufacture, importation, or sale of technical devices or computer software products designed to circumvent network security is made illegal as contributory infringement. Serious attention should be given to the possibility that unauthorized copying will become a widespread practice. At present, it is not infringement to manufacture, distribute or sell means to circumvent safeguards preventing unauthorized copying. SPA urges the Working Group to make these activities illegal as contributory infringement. The Working Group also should recommend that gaining unauthorized access to these works by using these devices or other means to break or override hardware and software locks constitutes copyright infringement.

The need for such steps has become urgent in the five years since Cornell graduate student Robert Morris unleashed his computer virus on the Internet. Last year, nearly 800 security breaches were reported on the Internet, and the Computer Emergency Response Team expects to see over 1000 in 1993.⁷ That amounts to several every day. Once these computer "crackers" penetrate a network operating system, they disseminate their techniques in publications and BBS systems, thus proliferating the unauthorized use of copyrighted works and the disclosure of both valuable trade secrets and confidential personal information.

Fourth, the Working Group should support ratification of multilateral agreements, like GATT-TRIPS and NAFTA, and ongoing negotiations for the proposed Berne Protocol.

[A] performance made available by transmission to the public at large is 'public' * * * whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times."

⁷Sandberg, "Computer 'Cracking' Is Seen on the Rise," The Wall Street Journal (Nov. 1, 1993).

Software Publishers Association

These are essential because works available on networks in the U.S. will be available to network users in many other countries and vice versa. For example, when SPA member Novell, Inc. released its NETWARE 4.0 software in Europe, it was illegally copied from an electronic bulletin board in the U.S. just one week later. These agreements will further cement the minimum standards required to protect computer software as a literary work, and provide copyright owners with the legal means to enforce their rights in many countries around the world.

Fifth, the Working Group should clarify contract law as needed to enable copyright owners to transact licenses in an interactive telecommunications network. Subscription agreements and "pay per use" transactions should be enforceable against the network user who pledges payment, such as by credit card or on-line service account, and agrees to abide by restrictions on use of the work. Only by clarifying contract law in this regard will copyright owners be confident that they will receive payment for works accessed through the NII, and that the use will not result in pirated copies, unauthorized adaptations, and unauthorized disclosure of trade secrets.

- **Do the existing fair use provisions of the copyright law adequately accommodate the interests of users of the works available via the NII?**

The provisions of Section 107 of the Copyright Act appear to provide courts with adequate guidance in deciding questions of fair use, while preserving the flexibility of the doctrine's common law origin. For now, Section 107 should be applied by the courts in its present form in disputes over their use of works available on the NII. If judicial development cannot preserve the balance between copyright owners and users, then Congress has shown itself willing to modify the law when necessary.

- **Should standards be established to encourage or require the intercommunication or exchange of information and the interoperability of the different types of computer software and systems supporting or utilizing the NII?**

Standards for intercommunication are necessary for information to be exchanged in telecommunications networks, such as the NII. The private sector has responded to this

Software Publishers Association

need by developing standard file formats to facilitate intercommunication. Customarily, standard file formats are developed by ad hoc private sector groups who recognize the need for users to exchange information, and then cooperate in developing and publishing the standard. The standard file formats are then tested in the marketplace by software producers and users, who have the final word on whether they will prevail or be replaced by superior formats. This ad hoc private sector process has resulted in such enduring standard file formats as ASCII, which permits textual information to be exchanged, and EPS, which permits graphic information to be exchanged.

The success of standard file formats provides the model to develop intercommunication standards for the NII as needed by the private sector. As noted by the IITF, "[t]he United States has long relied on a consensus-based, voluntary standards-setting process in communications."⁸ While SPA welcomes the IITF's willingness to "participate more actively in private-sector standards-writing bodies,"⁹ standards should not be imposed by the government because they promise to be outpaced by the rapid technological change now prevalent in the software and computer industries. Rather, intercommunications standards for the NII should be voluntary, developed by the private sector, and tested by the market.

- **Should standards or other requirements be adopted for the labeling or encoding of works available via the NII so that copyright owners and users can identify copyrighted works and the conditions for their use?**

SPA members believe that it would be helpful to develop a means for labeling or encoding works available via the NII so copyright owners and users can identify works and the conditions for their use. As with intercommunications standards, labeling or encoding works should be voluntary, and if necessary done according to standards developed by the private sector and tested by the market.

- **Should a licensing system be developed for certain uses of any or all works available via the NII? If so, should there be a single type of licensing or should the NII support a multiplicity of licensing systems?**

⁸ Information Infrastructure Task Force, The National Information Infrastructure: Agenda for Action (Sept. 15, 1993), at 9

⁹ Id.

Software Publishers Association

SPA at this time steadfastly opposes the use of compulsory licenses for software available via the NII. Copyright owners should retain full control of their works, and thus be free to authorize or prohibit their use by others, and set the conditions and cost of their use in the marketplace. The IITF and the NII should not be involved in setting the terms of such licenses, but rather in maintaining the environment in which copyright owners are free to offer their works for authorized use.

As discussed earlier, the Working Group should clarify contract law to make network transactions fully enforceable. Because access to many copyrighted materials will be authorized using electronic commands, the Working Group can assist the development of licensing by insuring that contracts made via the NII, as well as contracts involving the use of materials available on the NII, are fully enforceable. Particularly if the NII develops along the lines of the Internet model, a variety of systems will arise to permit users to obtain authorization to reproduce and display copyrighted works, especially with the development of technical means to meter their use. For example, WAIS Inc. (Wide Area Information Servers) foresees that information will reside in a single place, close to the publisher. In this system, publishers can restrict access to the information sources, and establish their own relationships with their audiences.¹⁰

Such a vision may not arise, however, if the NII is developed to resemble the cable television model, in which access to users is mediated by distributors offering the only service to a geographical area or subset of users, or if significant vertical integration occurs between content providers and distributors. While government should remain vigilant against marketplace domination and unfair trade practices, for now the marketplace should be free to experiment with these alternatives, and to deploy new technological means to facilitate these transactions as they develop.

- **Are there technical means for preventing unauthorized reproduction or other unauthorized uses of copyrighted works that should be mandated or required to comply with certain standards (similar to the serial copying controls required in digital audio recording devices and digital audio interface devices under the Audio Home Recording Act of 1992)?**

¹⁰ WAIS Inc. Questions and Answers (March 1993), at 1.

Software Publishers Association

The technical means for preventing unauthorized reproduction or use of copyrighted works should not be mandated, nor should they be required to comply with certain standards. Copyright owners should be free to decide whether access to their copyrighted works on the NII should be restricted and, if so, to choose the means that best fits their need for security and marketing.

Network management systems that control access to specific applications is a growing area for many SPA members. These programs, such as Norton's Administrator for Networks from Symantec Corporation, permit software use to be distributed from a central file and "metered" to authorized users on the network, while denying access to unauthorized users. These systems are applicable to networks in which users have accounts with networks, such as America On-Line and Lexis/Nexis services. For networks that do not restrict access to account holders, prototype systems are being developed to identify record users, copyrighted works used, and compensation. Network management systems thus promise to provide the technical means to prevent unauthorized reproduction or use of copyrighted works available on telecommunications networks.

The technical means for preventing unauthorized reproduction or other unauthorized uses of copyrighted works should not, however, be mandated or required to comply with certain standards. Network security is often vulnerable to breach or override by unauthorized users, and a single mandated standard would simply lay all the information riches of the entire NII open to illegal copying and tampering by ingenious and persistent trespassers. These breaches could be better contained if copyright proprietors and distributors on the NII were free to use a variety of proprietary network management systems to protect specific applications. Thus, by permitting diverse technical systems for network management, the IITF can actually encourage greater security for copyrighted works available on telecommunications networks.

- **What types of educational programs might be developed to increase public awareness of intellectual property laws, their importance to the economy, and their application to works available via the NII?**

In its campaign against software piracy, SPA has learned that educational programs are very effective in deterring unauthorized reproduction and use of copyrighted works. As a result, the most important step in protecting copyrighted works on the NII may be to dispel

Software Publishers Association

mistaken notions about reproducing copyrighted works by educating users to respect the intellectual property rights of others.

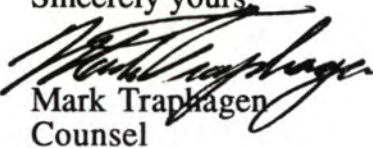
For example, SPA staff regularly speaks to business, education, legal, and computer user groups about how to comply with copyright law while making use of software products. SPA produces a software management guide, brochures, computer programs for auditing software use, and videotapes in several languages. SPA also advertises in trade magazines and on television to get the word out that software piracy is a crime. The Working Group should consider a similar effort to educate the public on how to respect copyrights on the NII. If the Working Group or the IITF decide to go forward, SPA would be pleased to cooperate with this educational effort.

Conclusion

SPA's member companies are poised to provide the software necessary to operate the NII and make its content available to network users. To encourage these copyright owners to make their works available for use on the NII and other telecommunications networks, the Working Group must ensure that their copyright and other intellectual property rights will be respected, regardless of the technological means by which they are presented and disseminated. SPA stands ready to assist in this effort.

SPA is grateful for the opportunity to present the Working Group with these comments on the intellectual property issues involved in the National Information Infrastructure (NII), and looks forward to the Working Group's report to the IITF. In the meantime, SPA would be pleased to provide additional information or assistance to the Working Group's effort, as needed.

Sincerely yours,



Mark Traphagen
Counsel

Clinton Presidential Records Digital Records Marker

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a tabbed divider. Given our digitization capabilities, we are sometimes unable to adequately scan such dividers. The title from the original document is indicated below.

19

Divider Title: _____

JOINT STATEMENT OF
THE BUSINESS SOFTWARE ALLIANCE AND
THE ALLIANCE TO PROMOTE SOFTWARE INNOVATION

Before the Working Group on Intellectual Property
of the Information Policy Committee
of the National Information Infrastructure Task Force

November 18, 1993

I. Introduction

Mr. Secretary:

My name is Tom Lemberg. I am the General Counsel of Lotus Development Corporation of Cambridge Massachusetts. I am appearing today on behalf of the Business Software Alliance ("BSA") and the Alliance to Promote Software Innovation ("APSI"). On behalf of the BSA and APSI I would like to thank you for convening this hearing and opening the dialogue between government and the private sector on the intellectual property and other critical issues raised by the National Information Infrastructure ("NII"). We appreciate having the opportunity to participate in this process.

The member companies of the BSA and/or APSI include: Adobe Systems, Inc., Aldus Corporation, Apple Computer, Inc., Autodesk, Inc., Borland International, Inc., Computer Associates, Inc., Digital Equipment Corporation, GO Corporation, Intel Corporation, International Business Machines Corporation, Lotus Development Corporation, Microsoft Corporation, Novell, Inc., UNIX Systems Laboratories, Inc., and WordPerfect Corporation.

II. The Software Industry's Contribution to the U.S. Economy

In the last five years, every governmental, academic and industry study of technologies that are key to America's future has identified the vital role to be played by the software industry. Software is characterized by both rapid technological innovation and widespread use in downstream markets. Software innovation improves the competitiveness of other industries which utilize software products to make themselves more innovative and competitive. The benefits of continuous software innovation permeate much of the American economy.

In March of this year, the BSA released a study prepared by Economists, Inc. entitled The U.S. Software Industry: Economic Contribution in the U.S. and World Markets.¹ Based on government and industry information, the study reviewed the economic contribution made to the American economy by the U.S. "core" software industry: prepackaged software; custom computer programming services; and computer integrated design.

The Economists, Inc. study found that the "core" software industry:

- (1) Is the fastest growing industry in the United States;
- (2) Is now larger than all but five manufacturing industries;
- (3) Is contributing to the economy of virtually every state in the nation; and
- (4) Is achieving tremendous success in the international marketplace.

Notwithstanding this impressive record, the software industry's role in the growth of the nation's economy will be even more critical in the future as new and more advanced technologies such as the NII continue to evolve.

¹ Stephen E. Siwek, Harold W. Furchtgott-Roth, Economists Inc., The U.S. Software Industry: Economic Contribution in the U.S. and World Markets (March 1993). We have submitted a copy of this study along with this statement.

III. The Software Industry's Vision of and Role in the Development of the NII

The digital information revolution is underway. The digital revolution will enable everyone to be plugged into, and interactive with, everyone else. Because of the ease, speed, versatility and reliability of creating and transmitting digital information, it will be the preferred pathway for business and commerce and the desired highway for personal and cultural communications.

It is not surprising, then, that the private sector is already well underway in developing and deploying the infrastructure that will be necessary to support the digital revolution. We have witnessed the birth of a broad array of new enterprises, joint ventures and business alliances as companies get ready for the digital future. We expect this trend is likely to accelerate in the months and years ahead.

The United States will need an advanced NII that will be able to accommodate and facilitate the expanding use of digital information. The NII must include high capacity interoperable networks capable of moving tremendous amounts of information almost instantaneously. Just as the interstate highway system once marked a historical turning point in our national economy, the NII and its ability to move text, data, and images around the country and the world efficiently will be a key component of the future of America's economic strength.

The NII offers us many new opportunities. First, the NII will generate demand for a wide array of new products and services which will rely on advanced computers and sophisticated software. This will create new opportunities for expanding America's technology manufacturing base, thus creating new high paying, high skill jobs.

Second, new applications of digitized information will offer all Americans, regardless of their location or economic position, access to the latest information in such areas as health care, education, and manufacturing, and improved access to government information and libraries. The NII will therefore be able to serve as an enhanced and efficient provider of social services. To quote the Administration's recently released report, The National Information Infrastructure: Agenda for Action: "The NII can transform the constraints of geography, disability, and economic status... giving all Americans a fair opportunity to go as far as their talents and ambitions will take them."²

However, in order to be able to fully realize these benefits, the NII must have a number of essential characteristics.

First, it must be capable of affording access to all potential users, whether they be private citizens, hospitals, businesses, schools, libraries, government agencies, or research organizations.

Second, there must be compatibility between the sources of information and the means of access. Users must be able to use and access information through a variety of machines and to transmit the information between different types and sizes of machines everywhere.

While much of the talk about the NII revolves around hardware, it is essential to understand that what makes the whole system work is software. Fiber optic networks and digital information hardware without software are incapable of responding to even the simplest command or forwarding the simplest message. The hardware may serve as the "muscle" but it is software that will operate as the "brains" of the NII. Software transforms

² Information Infrastructure Task Force, The National Information Infrastructure: Agenda for Action at 4 (September 15, 1993).

the raw power of high capacity networks and computers into information systems that help people at work, school and at home.

Software does this in two ways. First, it helps the user navigate oceans of digital information to locate or create that which is useful or desired. Second, once a decision is made to send or receive information, it is the software that actually "pulls" the information through the computer switches and wires that are the physical network. As communications and computer technologies become more powerful and less expensive, we will expect them to do more for us and software will be the key to making it happen. For example, continuing new and creative software solutions are required to handle network scalability, that is, the problems which result from the exponential rate of attachment of new users and networks to backbones, such as the Internet.

IV. The NII and the Vital Role of Copyright Protection

The protection of intellectual property through copyright is an essential element of the successful development and deployment of the NII. Clear and appropriate legal protection of proprietary rights is needed to provide the necessary incentive for the development of the software, hardware and elements of content which will make the NII attractive to users. Such protection is also necessary to instill confidence in the owners of software and other works that their products will not be subject to piracy and unauthorized use on the NII.

Copyright owners will be hesitant to develop new works, or make their works available via the NII, unless they can be assured they will be protected. Notwithstanding the tremendous success of the software industry to date, piracy - unauthorized duplication and/or distribution of software - remains a major, continuing threat to the industry. Worldwide, we

estimate that the industry loses about \$12 billion annually - \$1.9 billion in the U.S. - due to software piracy.

The digital information revolution presents unique challenges to protecting the rights of copyright owners. First, digitization offers an easy and inexpensive method to create an unlimited number of perfect copies. Second, digitized information can be instantaneously uploaded and downloaded by an unlimited number of users. Third, information in disparate media can be converted into a single digital stream and can easily be manipulated to create a variety of new works. While many of these challenges are not new to software publishers, they are revolutionary for many other copyright owners whose works have not historically been available in digital form.

Since 1790 when Congress passed the first copyright act, U.S. copyright law has demonstrated the amazing ability to adapt to whatever new challenges have been presented by technological advances. Indeed, the tremendous success of the software industry would not have been achievable without the evolution of strong copyright protection for software. The continued growth of the software industry and other information technology related industries and the successful development of the NII will depend on the continuing ability of the copyright law to adapt to these challenges. Moreover, as the NII evolves, it will be critical that aggressive and effective enforcement of the copyright laws be a top government priority.

A. Possible Amendments to Copyright Law

It is stating the obvious to say that the NII is evolving rapidly. Our industry is still in the early stages of devising business strategies and developing new products and services to take advantage of the many opportunities offered by the NII. We do not yet know the NII's full implications for our industry.

Our copyright law, as history has shown, is a flexible law which can be adapted, with only minor modifications, to technological change. Our industry is an excellent example. In 1980, the Copyright Act was amended explicitly to protect computer programs. This was accomplished through the addition of just a handful of new provisions to the law. In addition, the copyright law provides a rich source of precedent and experience through which to tackle new issues. While it is likely that some changes in law and policy will be needed for the efficient development of the NII, it is our current judgment that what will be needed is adjustment at the margin, and not wholesale change. In any case, we need more practical experience with the NII and its operation before proceeding with changes in law.

Having said all this, we do see some areas in the law where change may be appropriate. We would support the suggestion you have made, Mr. Secretary, of exploring possible amendments that would make it a criminal and civil offense to manufacture, import, sale, lease, use or possess a technical device or computer program product, the purpose of which is to circumvent either the security of the NII or any other security measures included in the NII, or in copyrighted works themselves, to safeguard the integrity of works.³

As for other proposed changes to current copyright law, at this time we believe it would be premature to make any other recommendations. With additional experience and further development of the NII, we will be better positioned to suggest other statutory or regulatory changes, if such changes become necessary. Some of the copyright issues that will need particular examination as the NII evolves include scope of protection for derivative

³ Article 1707 of the North American Free Trade Agreement provides similar protection for encrypted program-carrying satellite signals.

works, rights of reproduction and distribution, display and performance rights, fair use and licensing.

B. Copyright Licensing Systems

We believe that we lack the necessary experience with the NII to make recommendations with regard to any proposed copyright licensing system(s) for works made available via the NII. The history of our industry, and that of other copyright based industries, is that efficient licensing and distribution systems have evolved over time in response to consumers' needs and market forces. Our experience to date has been with individual transactions governed by contracts. We have had very little experience with collective administration of rights. Thus, we are not in a position to judge their applicability in the NII context. We are certain, however, that compulsory licensing of copyrighted works would not be appropriate. This is particularly true of works of high value, such as computer programs.

IV. The Role of Standards in the Development of the NII

Mr. Secretary, you have raised the issue of requiring or establishing standards in the context of the development of the NII on several fronts: (1) standards for labeling copyrighted works; (2) standards to ensure the interconnectivity and interoperability of hardware and software systems supporting or utilizing the NII; and (3) standards for technical means to prevent the unauthorized reproduction or use of copyrighted works.

The technology in the computer and software industries is changing at an unprecedented rate. The precise contours of the future of the NII are still vague and uncertain at this time. No one individual, company or even industry can be sure how the many technological and economic choices are going to be determined. The challenge to both

the government and private sector in the successful development and deployment of the NII is that nothing be done, particularly in the context of the requirement or establishment of standards, that might accidentally "fossilize" technology at yesterday's levels or prejudice the rights of intellectual property owners.

A. Standards for Labeling Copyrighted Works

The use of "standardized" electronic headers, labels and other signature techniques to enable the identification of ownership and determination of the terms and conditions of permitted uses of copyrighted works moving through the NII may in time prove to be appropriate. As the NII evolves, we believe the private sector should be allowed to determine whether labeling requirements or standards are appropriate and, if so, to develop such standards voluntarily over time.

B. Standards to Require Interconnectivity and Interoperability

The elimination of incompatibilities is in everyone's best interests. However, it would be antithetical to the fast moving technology characteristic of the digital information revolution to suggest that standards be imposed from above. Instead, we believe the way solutions to the connectivity problem have developed to date is instructive.

Today, there are an estimated 5 million people worldwide connected through several thousand interlocking networks which comprise the Internet. Indeed, some analysts believe the Internet traffic rate is growing at rates as high as 15% per month. As you know, the federal government created the backbone of this network by financing the construction of links between universities, research laboratories, and military installations. But increasingly, individuals and businesses are using the network to communicate and provide information services. Importantly, it has been the private sector that has been able to keep up with

technological developments and establish protocols and procedures for linking disparate networks into a larger whole. Moreover, we would note that there is a high degree of compatibility between hardware and software that is commercially available today that has been allowed to evolve over time with the development of technology.

We believe taking a similar approach to the development of the NII would be equally effective.

C. **Standards for Technical Means to Prevent Unauthorized Reproduction or Other Unauthorized Uses of Copyrighted Works**

Again, without being sure where digital information technology is headed, we believe it would be premature to suggest any technical requirements or standards in this area at this time, though we believe that the encryption of information made available on the NII should be permitted. Obviously, because of the non-physical nature of the electronic computer medium, "traditional" methods of protecting information and ensuring its authenticity, such as sealing and signing a letter, are of no use in the context of the NII. One strong option for protecting copyrighted works is to provide protection and authentication as part of the information itself -- by means of encrypting the data, scrambling it using mathematical techniques so that it is extremely difficult for anyone other than authorized recipients to decrypt it.

In computer generated encryption, the strength of an encryption program depends on: (1) the integrity of the mathematical formulas used such that they are not subject to sophisticated mathematical attack (i.e., no "backdoors"); and (2) the length of the encryption formula (the "key") that encodes the message. The key is measured in terms of "bits," or the number of digits, with longer keys corresponding to stronger encryption schemes.

In this context, cryptographic strength measures how long it would take someone with a computer to identify the key by randomly trying all combinations -- a so-called "brute force attack." It becomes exponentially more difficult to randomly crack an encryption formula as more digits or bits are used.

Encryption can be done either through computer software or hardware. Thus, an encryption program can be imbedded on a magnetic medium, e.g., floppy disc or hard drive; burnt into a microchip (microcircuit) that is part of the computer; or placed on a accessory device, e.g., a PCMCIA card. Regardless of the medium used, the encryption program gives a series of instructions to the computer to perform the mathematical calculations necessary to encrypt or decrypt the information.

The BSA recently asked Stanford University Professor Martin E. Hellman to consider the implications of encryption policy on the NII.⁴ Professor Hellman's report warns that information moving through the NII will be extremely vulnerable to electronic eavesdropping and tampering unless it is encrypted. While commending the Administration for recognizing the critical importance of the NII, Professor Hellman cautions that "unless the Clinton Administration reverses existing national policy which discourages the use of encryption, it will get an insecure NII."⁵ Professor Hellman describes how an insecure NII poses, in his words, "three possible embarrassments:"

⁴ Martin E. Hellman, a Professor of Electrical Engineering at Stanford University, has worked in cryptography for over twenty years. As a result of his work, he has received a number of honors from the Institute of Electrical and Electronic Engineers, the primary professional electrical engineering society.

⁵ Martin E. Hellman, Implications of Encryption Policy on the National Information Infrastructure at 3 (1993).

●**A White Elephant:** Just as people do not use post cards for most of their mail, prudent users will refuse to trust most information to an insecure NII.

●**A Disaster:** Careless or ignorant users who trust confidential or valuable information to an insecure NII will be easy prey to hackers, thieves, spies, or others who violate the system.

●**Foreign Dominance:** Foreign companies, operating from countries which do not discourage encryption, could offer a competing, secure service and put the NII out of business.⁶

In short, assuring the security and integrity of information will be essential to the successful development of the NII. The availability of strong encryption can provide this assurance. For these reasons, we ask the Administration to reverse its policies which discourage strong commercial and private encryption and strongly urge the Administration to immediately change its export controls on software to permit the export of generally available software with encryption capabilities employing the DES algorithm or other algorithms such as RC2/RC4 at comparable strengths (56-bits).⁷

⁶ Id. at 3.

⁷ We have submitted a copy of Professor Hellman's report along with our statement.

V. **Educational Programs to Increase Public Awareness of Copyright Protection**

We strongly support the development of public awareness campaigns and educational curricula for schools about the role of copyright in sustaining the creative process and its contribution to America's technological and economic growth. In this regard, we support your suggestion, Mr. Secretary, of exploring the development of a national educational curriculum, in cooperation with the Department of Education, on the role of copyright and other intellectual property rights in electronic information systems.

Our experience over the last five years has demonstrated the critical importance of increasing public awareness of the legal protection afforded software through copyright. Indeed, when founded five years ago, one of BSA's primary tasks was the development of worldwide educational programs to increase public awareness of the legal protection afforded software.

When we began in 1988, we developed a model anti-piracy campaign combining public policy initiatives to strengthen copyright laws, investigative efforts to increase the pace of enforcement, and marketing programs to educate the public about copyright law protection for software. Now active in more than 50 countries, our educational efforts are specifically designed to increase public awareness of software copyright laws. By forging alliances with national software alliances throughout the world, we develop and distribute information to software users and retailers about managing the acquisition and use of software in compliance with copyright law. The BSA works closely with its members and other software publishers worldwide to implement local

education programs specifically tailored for each market. Since 1988, we have distributed more than 100,000 Guides to Software Management in eight different languages.

In addition to the possible development of a national educational curriculum and public awareness campaigns, we suggest that stringent enforcement of the existing criminal statutory provisions for copyright infringement of software and other copyrighted works would also serve as a valuable "educational" tool. Last year, Congress made copyright infringement of software in certain instances a felony.⁸ Willful infringement of software and other copyrighted works for purposes of commercial advantage or private financial gain is a felony if it consists of the unauthorized reproduction or distribution, during any 180-day period, of 10 or more copies of one or more copyrighted works, with a retail value of more than \$2,500. The criminal penalties provided include imprisonment of up to five years, fines up to \$250,000 or both. Thus, anyone who makes multiple copies or distributes software or other copyrighted works over the NII without authorization for the purpose of commercial advantage or private gain could be charged with a felony. The aggressive enforcement of this particular criminal statute by federal prosecutors would serve as a valuable tool in "educating" the public of the seriousness of violating the copyright law and the integrity of the NII.

⁸ Pub. L. No. 102-561, 106 Stat. 4233 (codified at 18 U.S.C. § 2319(b)(Supp. 1993)).

VI. Conclusion

Again, Mr. Secretary, we would like to thank you for providing us with the opportunity to present this statement and for opening the dialogue between government and the private sector. As the NII continues to evolve, we look forward to having the opportunity to work with you and others in the Administration in addressing the many issues that have been raised here today.

Implications of Encryption Policy on the National Information Infrastructure

Martin E. Hellman¹

Electronic information processing is replacing paper in a number of applications. Ten years ago, fax was used primarily by large law offices and a few other professionals; today, most businesses could not compete without it.

Electronic mail is rapidly moving from a curiosity of the academic community to a mainstream business application. Widespread electronic document distribution, including multimedia messages, is on the near horizon. Figure 1 on the next page illustrates the rapid growth of information flowing over the Internet computer-communications network and shows that, today, it carries approximately thirty-five *billion* packets per month.

Electronic communication has a number of advantages which are fueling this rapid switch from paper-based communications.

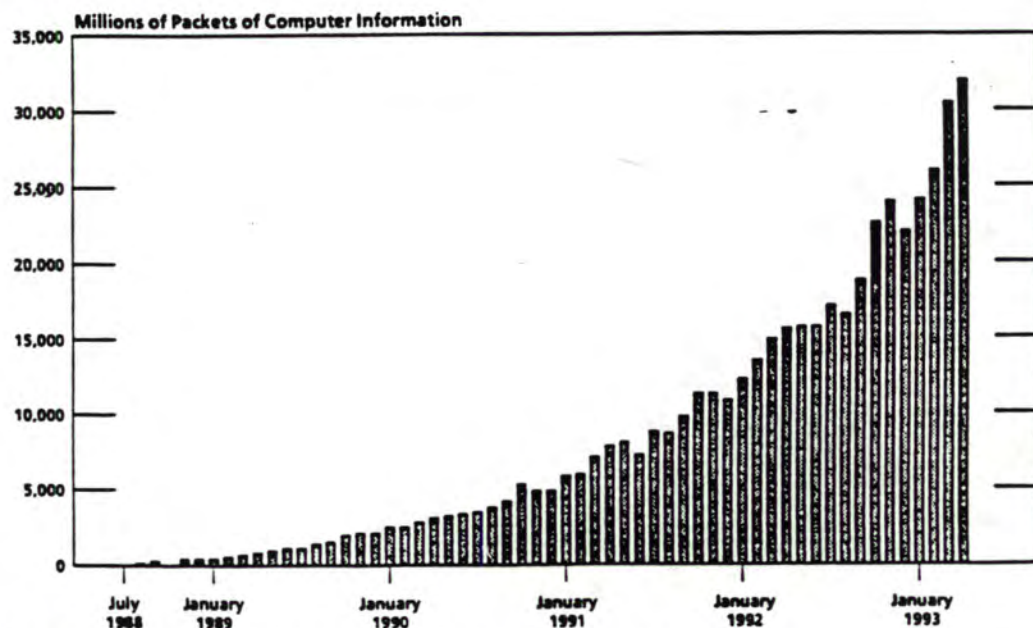
- **Speed:** electronic messages move at the speed of light. Paper moves at the speed of the Postal Service, or if premium prices are acceptable, overnight.
- **Cost:** Faxing a single page across the country costs as much as a first class stamp. E-mail can send on the order of 100 pages for the same amount.
- **Storage:** An 8 mm tape cartridge that sells for \$10 and is the size of an

¹Martin E. Hellman, Professor of Electrical Engineering at Stanford University, has worked in cryptography for over twenty years. His contributions, notably his invention with Whit Diffie and Ralph Merkle of "public key" cryptography has received a number of honors from the IEEE (Institute of Electrical and Electronics Engineers, the primary Electrical Engineering professional society): He was elected a Fellow of the IEEE "for contributions to cryptography;" received two IEEE awards for outstanding papers, and was awarded an IEEE Centennial Medal. The California State Psychological Association also honored him with its first Award for Distinguished Contributions to Consumer Protection. Before joining Stanford's faculty in 1971, Prof. Hellman was on the faculty at MIT (1969-71) and the research staff at IBM (1968-69). Preparation of this report was supported by the Business Software Alliance.

audio cassette can store 10 Gbytes of data, equivalent to 10,000,000 pages of text, or a thousand file drawers, each stuffed to the gills.

- **Access:** Electronic files can be accessed more rapidly and more conveniently than paper. When a copy is brought “on-screen,” the original resides safely on disk, whereas a paper copy that is accessed is vulnerable to loss or misfiling when returned to storage.
- **Content-Based Access :** Access based on content (e.g., “Find all documents containing the words *National Information Infrastructure*.”) is not economically feasible with paper documents, but can be accomplished inexpensively with computer-readable information.
- **Reproducibility:** Each copy of a paper document is degraded somewhat, while a tenth-generation copy of a digital document is indistinguishable from the original.

Summary Figure 1.
History of Internet Traffic, 1988-1993



SOURCE: Congressional Budget Office from data provided by Merit/NSFNET, Ann Arbor, Michigan.

Figure 1. History of Internet Traffic, 1988-1993. [Source: Congressional Budget Office from data provided by Merit/NSFNET, Ann Arbor, MI.]

Recognizing these advantages and their importance in maintaining America's competitiveness, the Clinton Administration has proposed the development of a National Information Infrastructure (NII), sometimes referred to as an electronic counterpart to the Interstate Highway System. This initiative is to be commended. But, unless the Clinton Administration reverses existing national policy which discourages the use of encryption (scrambling to protect information), it will get an insecure NII and three possible embarrassments:

- **A White Elephant:** Just as people do not use post cards for most of their mail, prudent users will refuse to trust most information to an insecure NII.
- **A Disaster:** Careless or ignorant users who trust confidential or valuable information to an insecure NII will be easy prey to hackers, thieves, spies, or others who violate the system.
- **Foreign Dominance:** Foreign companies, operating from countries which do not discourage encryption, could offer a competing, secure service and put the NII out of business.

An insecure NII is extremely dangerous because the advantages of electronic communication listed above are even more valuable to illegitimate users ("spies") than to authorized users. Once an electronic message has been intercepted, a spy can send an exact replica of the original, rapidly and inexpensively, to his headquarters. There it can be stored inexpensively and accessed conveniently. Fast, inexpensive access based on message content is indispensable to spies because they must sort through millions of irrelevant messages to find one of interest (e.g., any message containing the words *Clinton*, *reelection*, *California*, and *strategy*). Approximately ten billion words of computer-readable messages, such as e-mail, can be scanned for a dollar, so even if only one message in a million is of interest, \$1 worth of scanning produces

10,000 interesting words!²

Even though scanning is surprisingly cheap, we still would be safe if it were expensive or difficult for a spy to intercept our message stream. Unfortunately, interception is also extremely cost-effective in many instances. The increasing use of wireless and other shared communication channels (e.g., Local Area Networks or LAN's) increases the vulnerability of electronic communications by making large amounts of information available to unintended users without wiretaps or other risky operations.

Communications carried by satellite can be picked up by inexpensive "dishes" hundreds of miles from the intended recipient and give the spy access to literally billions of words per day. Cellular telephone conversations are vulnerable, as Princess Di and Governor Wilder now realize. Local area networks are, in reality, spy networks in which each node watches all the information flowing over the shared cable and picks out only those messages with its address. It would take only minor modifications to create phantom nodes that watch all information flowing over the cable and pick out only those intended for someone else on the network (e.g., I could intercept all messages intended for the president of Stanford University). Because such phantom nodes look like normal nodes, it would be hard to detect their existence. The same is true for interception of satellite and cellular telephone messages. Spying is a passive activity, and therefore hard to detect.

More ominously the Internet, on which the NII is likely to be modeled, uses distributed communication and switching. In this approach, the computer at Stanford which holds my e-mail is also used as a switch, for example taking

² In a timed experiment, my NeXT workstation searched approximately a million characters per second. This is equivalent to 100 billion characters per day, or 200 trillion characters over its approximately five year expected life. At six characters per average word, this \$3,000 machine can search 30 trillion words over its life, resulting in the 10 billion words per dollar quoted above. Because these are only approximate numbers intended to give ball park figures, only one decimal place of accuracy has been maintained (i.e., they are accurate to "one significant figure").

messages from the University of Washington, 800 miles north of us, and relaying them to UCLA, 400 miles to the south. This provides fault tolerance (if Stanford's node goes down, any other "gateway" south of the University of Washington can be used as the relay) and cost savings (e-mail from the University of Washington to UCLA can make use of unused capacity in Stanford's communication lines and does not need a separate, dedicated link). But, while the University of Washington's messages are being relayed by these other machines, they are vulnerable to search for key words that sort out "interesting" messages. Any Stanford "super-user" – and there are a number of them – can listen in on all the traffic passing through Stanford.

If the NII is developed under current policy, using it will be worse than writing all paper-based communications on post cards because a spy need not be physically present in the "Post Office" to intercept your "post cards." The NII will therefore be a tempting target for foreign intelligence organizations, organized crime (for blackmail, insider information, and sale of strategic business information), competing companies, and so-called "hackers." NSA (the National Security Agency) is well aware of the dangers inherent in electronic mail and prohibits its own confidential information from being sent over the Internet. Instead, the Agency uses its own secure e-mail network and is extremely careful to prevent any connection between the two.

While NSA has generally resisted the spread of commercial and private encryption, it has made an exception with respect to the communications of DoD contractors and other private-sector communications deemed of national security concern. NSA has warned a number of such concerns to encrypt or otherwise protect their communications that were being spied upon by NSA's foreign counterparts. While the Soviet Union and its satellites used to be NSA's prime concern, the French government is a major threat today, gleaning economic and

technological intelligence from American companies and passing this information on to their French competitors.

If all messages flowing through the NII are encrypted then the insecurity currently present in the Internet would disappear. The Administration recently released a report entitled *The National Information Infrastructure: Agenda For Action* which acknowledges this need: "The trustworthiness and security of communications channels and networks are essential to the success of the NII." But when the report calls for "review of encryption technology," it merely says that "In April, the President announced a thorough review of Federal policies on encryption technology." While there may be other April Administration actions that are referred to, the only one of which I am aware (the "Clipper chip" announcement) *discouraged* private-sector encryption by adding a new encryption system (the Clipper chip) which is incompatible with existing systems based on the Data Encryption Standard or DES. This action will likely retard the growth of encryption as companies and individuals delay purchase, waiting to see which of these mutually incompatible systems will dominate. The Clipper system also has a major drawback when applied to securing the Internet or NII: Clipper is a secret algorithm, available only in silicon, and cannot be implemented in software. Yet software encryption is most easily, cheaply, and rapidly implemented on such networks, requiring only an update to software releases. If encryption hardware must be installed at every node, security is likely to be delayed for years, and may never become widespread.

If the Administration decides to reverse current government policy which discourages encryption, then the required technology is in hand. While popular accounts of encryption often give the impression first popularized by Edgar Allen Poe that "human ingenuity cannot concoct a cipher which human ingenuity cannot resolve," Poe was wrong. Encryption is a special form of computation and has

benefitted every bit as much as word processing from the rapid decrease in the cost of computation. Ciphers that cannot be broken with any foreseeable technology can be implemented inexpensively today. When implemented in software, encryption is an almost-free add-on to a backup utility, telecommunications package, or similar program.

The former high cost of key distribution, in which couriers had to communicate the secret keys used to encrypt and decrypt message (analogous to "combinations" used to "lock" and "unlock" messages), can be eliminated by public key systems. In a public key system, two users communicating across an insecure channel *without any prearrangement* are able to agree on a secret key that an eavesdropper is unable to determine. This seemingly impossible feat is accomplished by allowing the eavesdropper to recover the key in theory, but preventing him from doing so in practice by making the cost of recovery prohibitive – for example, more than the entire country's GNP.³

Public key systems also allow digital signatures, numbers appended to digital messages which can easily be checked by anyone as authenticating that the message originated from its claimed source, but which can be easily generated only by the legitimate signer. Digital signatures are tied to message content, so that the recipient of an electronic bank draft cannot change the amount or any other part of the check.

Digital signatures are generated with a user-specific, secret key. They are validated with a related, public key. While, in theory, the secret signing key can be derived from the public validating key, again that can be prevented in practice by making the derivation ridiculously expensive. Digital signatures promise to

³ For example, the RSA public key system depends on the difficulty of factoring large integers. If I ask you to multiply 13 times 29, it takes only a short time to find the product: $13 \times 29 = 377$. But it takes much longer if I give you 377 and ask you to find its two factors, 13 and 29. Similarly, a computer can multiply two 100-digit numbers in a matter of milliseconds, but would take over a million years to factor the 200-digit product.

revolutionize business by allowing electronic contracts, tax returns, etc. In some ways, digital signatures are more secure than written signatures: Because written signatures are not message dependent, one signed paper document allows unlimited imitations by a skilled forger. Digital signatures do not suffer from this problem.

At this point it might be asked why, if cryptography is so needed, it is not more evident in our lives. The answer is two-fold. First, cryptography is more widespread than we realize since it is often done automatically, in which case it is invisible to the user. Anyone who has used Lotus' *Notes*TM has used encryption, but probably has not known it. Second, national security concerns have caused NSA to resist the spread of commercial and private encryption. NSA fears that strong, publicly available encryption will hinder its international intelligence gathering operations.

NSA has slowed the spread of encryption through its effective control of export licenses for encryption products.⁴ While there are some exceptions, in general NSA refuses to grant licenses for strong encryption. For example, NSA allows mass market software with encryption capabilities to be exported under a blanket license, but only if the key size is 40 bits or less. This is akin to allowing combination locks to be exported, but only if they have 20 or fewer possible combinations. It falls far short of the current Federal Data Encryption Standard (DES) which employs 56-bit keys. A 40-bit key can be searched 65,000 times faster than one that is 56-bits long.

Export controls limit domestic as well as foreign entities. Along with the shift to a global economy, communications are becoming increasingly international in nature. Just as few people would buy a new telephone that could

⁴ While export licenses are granted by the State Department, it is generally recognized that State defers to NSA's expertise in this area.

only be used domestically, market acceptance is limited for secure communications services and products that can only be used for communicating within the United States. American manufacturers are also loath to build high security devices for the domestic market for fear of drawing attention to the poor security of the export version and to avoid duplicate marketing efforts. Foreign software and hardware manufacturers which operate from nations with less onerous export controls therefore have a competitive advantage not only in their home country, but also in the US market. The U.S. Government limits the export, but not the import, of cryptographic products.

An unavoidable tradeoff must be faced: If the Clinton Administration continues the policies of the past by discouraging strong commercial and private encryption, it aids American intelligence agencies in an important task: reading international message traffic to glean information of value to the American Government. But that policy also allows foreign intelligence agencies to read that same traffic and glean information of value to foreign governments – much of it involving confidential information of American citizens and corporations. This tradeoff needs to be carefully examined by those proposing the NII because, as noted earlier, without strong encryption there are three possibilities which could prove extremely embarrassing to the Clinton Administration:

- creating a white elephant that no one will use;
- creating a disaster if an insecure NII is used; or
- foreign dominance by a competing, secure III (International Information Infrastructure).